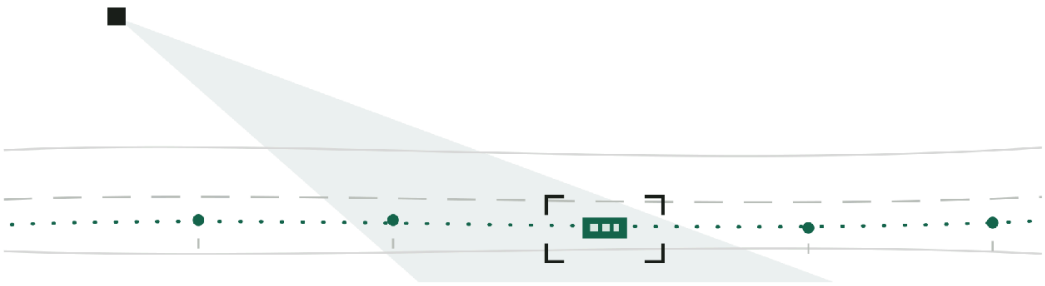
ALPRs and the Principles of Democratic Public Safety

A Framework for Governance

How automatic license plate readers can save lives, solve serious crimes, and improve investigative precision while remaining faithful to the values of fairness, restraint, transparency, accountability, and respect for civil liberties.



Brandon del Pozo, PhD

July 2026

Contents

Preface **4**
Abstract **5**
Executive Summary **6**
ALPRs and the Principles of Democratic Public Safety **8**
Public safety in a democracy 8
Principles guiding ALPR acquisition and deployment 9
The legal bases of ALPRs 10
The escalating uses of ALPR data 11
The Function of ALPRs in Policing: Strengths and Concerns **13**
ALPR use cases 13
Confederated ALPR searches 13
The array of concerns about ALPRs 14
Misuse of ALPR data for non-police purposes 15
ALPRs amid the continuum of data collection 15
The emerging history of ALPR use 17
ALPRs and the democratic principle of restraint 18
ALPRs and the reduction of the police dragnet 18
ALPR placement and democratic fairness 19
Measuring the effectiveness of ALPR programs 21
Cost effectiveness, critical incidents, and ALPRs 22
The Democratic Regulation of ALPRs **25**
Role-based access and the principle of least privilege 27
Judicial process and ALPR searches 30
Retention periods 30
Elements of an agency ALPR policy 34
Core themes and content of ALPR legislation 35
ALPRs and public trust 35
Conclusion **37**
Essential Elements of an ALPR Policy **38**
Elements of ALPR legislation 39
ALPR Governance Workbook **41**
Part 1. Policy self-assessment checklist 41
Part 2. Five decisions every jurisdiction must make 42
References **45**

Funding/Conflict of Interest Disclosure: Dr. del Pozo received funding from Flock Safety to write this white paper. Flock had no role in the writing of this report. Written assurances of the author's editorial independence and peer review of the paper prior to release were conditions of the project.

Preface

Brandon del Pozo spent twenty-three years in American policing - 19 with the New York City Police Department and four as chief of police of Burlington, Vermont - before turning to research full time. He holds a PhD in philosophy from the CUNY Graduate Center and studies policing, public health, and the governance of public safety at Brown University. His work is motivated by the belief that the effective exercise of police power and its careful regulation are joint requirements of democratic government.

This paper reflects both halves of that career. The cases described in these pages - vehicles traced across state lines, victims quickly located, suspects cleared by exculpatory evidence - are drawn from the practice of policing, including incidents the author oversaw as a chief of police. The framework offered for governing ALPR technology is drawn from the scholarship of democratic policing. The aim is to move a polarized debate onto more productive ground: not whether license plate readers should exist in our communities, but how a self-governing community should direct, constrain, and audit their use.

Abstract

Automatic License Plate Readers (ALPRs) have become one of the most debated public safety technologies in America, a debate most often cast as a binary choice between protecting communities and protecting privacy. This paper argues that this is a false dichotomy. Drawing on democratic principles of public safety, constitutional law, police practice, and evidence-based governance, it offers a framework for how ALPRs can be used to save lives, solve serious crimes, and improve investigative precision while remaining faithful to the values of fairness, restraint, transparency, accountability, and respect for civil liberties. Rather than asking whether ALPRs should exist in the first place, this paper focuses on how the ALPR technology in place today can be successfully used and governed in a democratic society.

Executive Summary

This paper presents a framework for using Automatic License Plate Readers (ALPRs) to improve public safety while remaining faithful to the democratic principles of fairness, restraint, transparency, accountability, and respect for civil liberties. The question it takes up is not whether ALPRs should be used, but how they should be governed so that they maximize public safety while effectively minimizing risks to privacy and liberty.

The potential for ALPRs to enhance public safety is significant. They provide accurate, often time-sensitive information about a vehicle's identity and location that helps police recover stolen vehicles, locate missing and abducted persons, apprehend dangerous offenders, and strengthen complex criminal investigations. Their greatest contribution is not as a standalone source of evidence, but the speed, precision, and quality they bring to investigations overall. The data they collect is correspondingly limited: a license plate number, a time, a location, sometimes a direction of travel, and a description of the vehicle itself - its make, color, and any prominently distinguishing features. ALPRs do not identify drivers or independently reveal their behavior, intentions, or destinations; the data they supply is primarily inferential, and requires corroboration with other evidence to establish criminal activity.

Reflecting these limits, existing case law recognizes that a car's license plate must be displayed whenever it is on a public road, this display carries no reasonable expectation of privacy, and that collecting ALPR data in public is therefore not a Fourth Amendment search. Privacy concerns arise primarily when large volumes of data are aggregated over time and combined with other information to reveal detailed patterns of an individual's life that could not be inferred by simply viewing their car's license plate at a given location in public.

Used well, ALPRs can advance democratic policing. By narrowing suspect pools, corroborating witness accounts, directing investigative resources more efficiently, and providing exculpatory evidence that clears innocent people, they allow police to pursue public safety objectives by less intrusive means. Deployed impartially and according to a community's demonstrated needs, they distribute public safety fairly while reducing unnecessary police contacts and limiting investigative bias.

The legitimate concerns raised by ALPRs, including long-term retention of vehicle location data, information sharing with agencies whose enforcement agendas a community does not share, potential misuse by police employees, and the possibility that widespread deployment could enable mass surveillance, should be addressed through clear and effective governance rather than by abandoning a valuable public safety tool.

Effective governance operates through three complementary mechanisms: (1) legislation that establishes legal authority and accountability, (2) agency policy that governs

operational use and (3) technical system design that embeds safeguards directly into everyday operation, among them role-based controls that grant access to the fewest number of people necessary, automated audit logs, geofencing around sensitive locations, restrictions on confederated searches, and carefully controlled data sharing.

Among these safeguards, the retention period for ALPR data deserves particular attention. Historical ALPR data should be retained only as long as empirical evidence demonstrates meaningful investigative value, a duration that should be established by research into the arc of successful criminal investigations rather than by arbitrary statutory limits, and ALPR programs should be evaluated by operational outcomes such as stolen vehicles recovered, time to locate victims and suspects, case solvability, and improvements in investigative quality.

Governed this way, ALPRs are best understood as one component of a broader public safety system rather than as a standalone technology: one that can improve public safety, promote more precise and restrained policing, respect civil liberties, and strengthen a community's trust in their police.

PART I

ALPRs and the Principles of Democratic Public Safety

Public safety in a democracy

It is a fundamental duty of a democratic government to create, improve, and sustain public safety in several ways, two of which are especially relevant to ALPR data collection. One is the apprehension of people suspected of crimes in order to limit the danger they pose to the community and bring them to justice. The other is direct intervention on crimes in progress and other critical incidents, to protect and rescue people in physical danger. In each case, police are the government actors who execute these duties in service to the public by collecting, interpreting, and acting on reliable evidence about what a person has done, what they are doing or are about to do, and where they can be found. In achieving these goals, the government has a duty to support and utilize technologies that provide this evidence in a timely and effective way. Publicly observable information about the vehicle a person is driving and where it was seen is an important piece of information in these public safety efforts, and automatic license plate readers (ALPRs) can accurately provide it.

> **CASE - SAN DIEGO, CALIFORNIA - JUNE 2026.**
> A witness provided police with a license plate number after seeing a woman escape from a vehicle before a man forcibly dragged her back inside and drove off. Within minutes, police used an ALPR system to locate the vehicle, stop it, and secure the release of the victim. Detectives later determined the suspect had allegedly abducted the woman from her home, and he was arrested on charges including kidnapping, false imprisonment, residential burglary, assault with a deadly weapon, evading police, and driving under the influence.[1]

> **CASE - PAGOSA SPRINGS, COLORADO - MARCH 2026.**
> A 22-year-old man was arrested on three counts of homicide after allegedly shooting an elderly woman in Lyman, Utah, stealing her car, then driving to Torrey, Utah, killing two hikers, and fleeing in their vehicle. Using its license plate, ALPRs located the hikers' vehicle as it traveled through southern Utah and northern Arizona into Colorado, where pursuing officers were able to locate the suspect and take him into custody.[2]

As a basic right of every person in a democracy, public safety must be created and distributed according to key democratic principles. One is impartiality: people should enjoy the safety provided by their government as demonstrated by their need for it, regardless of their class, race, religion, political affiliation, other aspects of their identity, or their ability to pay. Likewise, insofar as policing places burdens on the average person in terms of fines, fees, police encounters, and exposure to the enforcement of low-level and administrative

violations, those burdens should be both based on objective personal behavior and not distributed inequitably among certain groups and communities due to an allocation of police attention that is beyond a person's control. Deploying ALPR technology must adhere to these principles to meet basic conditions of justice and fairness.

Principles guiding ALPR acquisition and deployment

What ALPRs do. ALPRs collect a narrow range of data: the location of a vehicle at a given time, and when deployed at a stationary location on a roadway, its direction of travel. They do not capture who is driving, the destination of the car, or the behavior of the driver. It is important to note that vendors may bundle ALPR technology with an evolving range of other features, such as the live recording of people, facial recognition, AI-driven human behavior recognition, moving violation traffic enforcement (such as speed and red light cameras), and gunshot detection technology.[3] **The analysis here only examines the use of ALPRs. These other features should be subject to thorough analyses of their own.**

The limits of ALPR data. The information attached to a license plate in government databases can convey a car owner's active warrants, suspended license, or that the vehicle itself is stolen or suspected to have been involved in a crime. Beyond this, nothing about the data collected by ALPRs indicates a behavior in and of itself without additional information and context. In that way, ALPR data is inferential in nature: apart from objective facts about a vehicle's location and its direction of travel, anything else this data suggests can only be substantiated by other independent sources of knowledge. This limits the ability of ALPR data alone to reveal a person's patterns of behavior in a meaningful way (except when the goal is to locate and apprehend a person thought to be in a particular vehicle). Rather, ALPR data yields probative leads, important context, and opportunities to corroborate suspicion or provide exculpatory evidence. In sum, apart from ALPR alerts for vehicles sought in the immediate aftermath of violent crimes, abductions, etc., the primary enforcement use of ALPR data is to provide critical contextual information that adds to the quality and solvability of an investigation. A continuum of examples that require increased levels of independent knowledge illustrate this point.

1. A car has been reported stolen. An ALPR alert locates the car parked at the roadside, and police recover it.

2. A person has just committed a violent crime and fled to an interstate highway. Witnesses provide police with the vehicle's license plate number, and may use ALPR reads to determine the vehicle's direction of travel, close in on it, and arrest the driver.

3. A pedestrian is struck and killed by a motorist who flees the scene. Witnesses can only provide a general description of the vehicle: e.g., a green Chevrolet sedan. ALPR data shows three cars matching that description passed a nearby camera on the roadway around that time. Detectives visit the registered owners and observe one of them has a green sedan in

the driveway with front end damage. Officers secure the scene, obtain a search warrant, and lift the victim's DNA from the car. The owner confesses.

4. Over the course of several weeks, a neighborhood suffers a string of burglaries. Witnesses report a black pickup truck leaving their block as they returned home. Detectives use ALPR records to determine a particular black pickup truck was recorded in the community on the night of the burglaries. The registered owner lives with a brother who was recently released from prison on a similar crime. Detectives visit pawn shops near his home and determine the brother has pawned stolen property. They obtain a search warrant, recover additional property stolen during the burglaries, and arrest the brother.

5. An interstate human trafficking ring brings its victims to and from motels in three different cities using a fleet of rental cars. In building a case, police use ALPR data as corroborating evidence to show the ring has been operating this way for months, switching vehicles to avoid suspicion, and moving their victims between cities in the early morning hours.

Five uses of ALPR data, in order of the increasing independent knowledge each requires.

The legal bases of ALPRs

It is established law that operating a vehicle on a public road in the United States requires displaying a unique registration plate, and that this plate must be open to public view. This display comes with no expectation of privacy. The characters on the plate can therefore be recorded by any observer, along with any other information that could be observed in a public place by the naked eye.[4]

> **"Courts have consistently held that the collection of ALPR data in a public place is not a search or seizure requiring judicial process."**

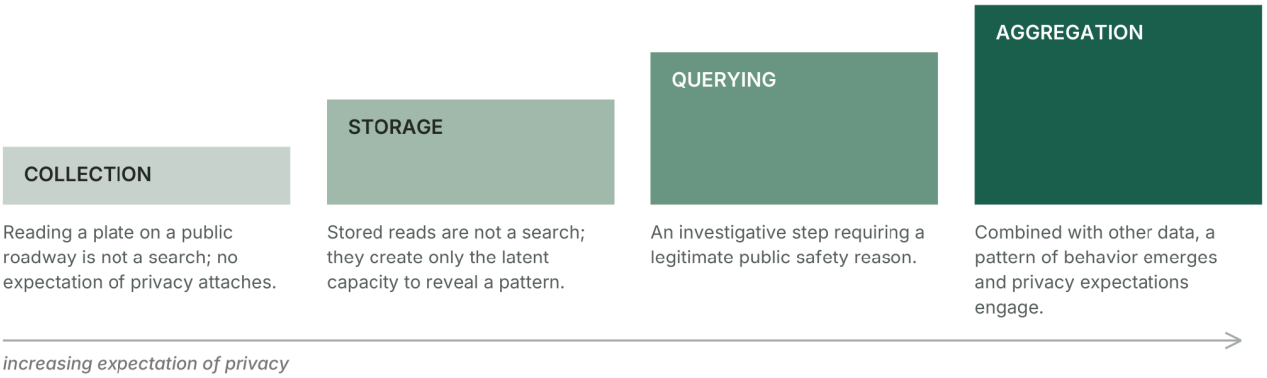
Case law supports this construal; courts have consistently held that the collection of ALPR data in a public place is not a search or seizure requiring judicial process, with the one trial-court ruling to the contrary since rejected by Virginia's appellate courts.[5] One ruling has opined that there may come a point where a sufficiently large volume of ALPR data collected in a jurisdiction may trigger a privacy protection, because it reveals a detailed pattern of behavior over space and time that cannot be discerned from more traditional observations made in public. For that reason, the ruling held, citizens would have a reasonable expectation of privacy regarding their behavior.[6] Nonetheless, the ruling did not specify what volume, over what length of time, would trigger this expectation, and found that there is nothing inherent in the deployment of ALPRs that invokes a Fourth Amendment concern on its own.

The escalating uses of ALPR data

This understanding allows us to present the escalating uses of ALPR data in terms of a person's expectation of privacy, which comes into play only after ALPR data is combined with other data sources that move beyond inference to clearly reveal a pattern of behavior:

THE ESCALATION LADDER

Four uses of ALPR data, and where privacy expectations engage



COLLECTION. The collection of raw ALPR data on a public roadway is not a search under the law, and people do not have an expectation of privacy regarding their license plates.

STORAGE. The electronic storage of ALPR data collected over time is not a search, nor does the simple storage of the data on a server constitute the construction of a pattern of behavior associated with a particular vehicle. It does, however, create the latent capacity to infer or reveal a pattern of behavior, which some may view as a latent threat to privacy.

QUERYING. Querying an ALPR system to create a report that collects historical data and presents it as a partial or inferred pattern of behavior is an investigative step by police that requires a legitimate public safety reason. Nonetheless, the resulting pattern arises from a series of observations made in public, each without a corresponding expectation of privacy. Any pattern that goes beyond describing trends in time, location, and direction of travel is limited to inference without incorporating additional types of data. While some people feel querying this data collected in public violates their privacy, to date courts have not ruled that aggregating these data points into a partial pattern triggers a Fourth Amendment concern.[19]

AGGREGATION. Combining ALPR data with other data about personal behavior, such as financial transactions, CCTV footage, cell phone location data, web surfing history, an ALPR read at or near a sensitive location, and direct eyes-on surveillance, can collectively yield a detailed and extensive pattern of life. That pattern moves beyond inference toward strong evidence of behavior by a person that could not be construed by public observation. This aggregation triggers an expectation of privacy, as reflected by the need for subpoenas and other legal process to obtain the most detailed data used in this type of aggregation.[7]

PART II

The Function of ALPRs in Policing: Strengths and Concerns

ALPR use cases

ALPR data has value any time the identity, location, and/or direction of travel of a vehicle can be combined with other reliable knowledge. It can help locate a victim, identify a criminal suspect, apprehend them, provide corroborating evidence about their unlawful behavior, or exonerate uninvolved people by providing exculpatory evidence or confirming an alibi. In practice, this translates into a range of recurring use cases for ALPR data:

01 Recovery of stolen vehicles

02 Locating the victim of an abduction

03 Apprehension of persons wanted for past crimes

04 Identifying a previously unknown suspect

05 Narrowing the scope of an investigation

06 Location of persons in the midst or immediate aftermath of a crime

07 Locating a person reported missing

08 Developing probable cause to arrest a known suspect

09 Contributing to the depth and quality of an investigation

10 More efficiently directing investigative resources

Confederated ALPR searches

Conducting ALPR searches across jurisdictions using a network that automatically queries all participating agencies' databases (rather than searching them one by one or pooling their records in a single repository) offers discrete public safety benefits for investigative purposes. Criminal suspects often flee the jurisdiction of occurrence to escape the investigative reach of the agency responsible for apprehending them. In the case of abductions, they will also flee to places where the victim is less likely to be recognized as a missing person through news coverage and community ties. ALPR data aggregated across jurisdictions provide the means to ascertain if a suspect has fled, their direction of travel, and possible destinations. This allows the investigating agency to efficiently reallocate resources, better focus their efforts, and to request the assistance of other jurisdictions.

CASE - BURLINGTON, VERMONT - 2016.

Amos Beede, a transgender person from Burlington, Vermont, was beaten to death at a homeless encampment by four suspects who fled the city by car. Over the course of several days, Burlington police used confederated ALPR searches and location data obtained by warrant to trace the car's movement west, to southern California. Coordination with the San Diego Police led to their arrest a few hours after reaching the city. All four were extradited to Vermont and convicted of charges ranging from second degree murder to aggravated assault.[8]

Audits will indicate police across the country have queried the ALPR data of distant cities hundreds of thousands of times.[9] This is because opting into a confederated database means queries may automatically be run in all participating jurisdictions to provide the most accurate results possible, not that agencies engage in frivolous queries of distant cities. The scope of these confederated searches reflects the automation of the process rather than the intentions of the agencies involved: a single investigator's query can result in a search of every member's database by design. Agencies should carefully restrict data sharing to ensure other participating jurisdictions cannot use ALPR data for purposes beyond those authorized by the contributing agency's criminal laws, such as civil immigration enforcement or investigations related to reproductive healthcare.[10] It is critical that agencies limit access accordingly, and work with ALPR firms to develop business processes that facilitate these restrictions and ensure they are effective.

Compelled disclosure of ALPR data. One risk agencies face is the possibility that despite declining to share their ALPR data with specified agencies through restrictive policies and technical safeguards, those agencies can nonetheless compel disclosure of the data through a court order or subpoena. While this has yet to occur,[11] it is conceivable that federal agencies, for example, can attempt to compel individual police departments to provide their ALPR records through legal process. That process is likely to be onerous and inefficient, however. Local municipalities can attempt to quash a subpoena or seek to limit its scope, which would require the requesting agency to respond before a judge. The agency seeking to compel disclosure would have to subpoena each record-holding agency individually, and engage in an adversarial legal process with most or all of them. A habitually contested legal process is likely to provide a strong disincentive to routinely attempting to compel disclosure of ALPR data. In assessing this issue, communities should weigh their ability to improve public safety using ALPR data against the risks of interference by outside law enforcement agencies.

The array of concerns about ALPRs

ALPRs can generate privacy and civil liberty concerns because they collect and store large amounts of public location data about individuals who are not suspected of wrongdoing. By capturing license plates, timestamps, and locations, ALPRs can create detailed records of a

vehicle's travel activities over time, leaving drivers open to inferences about their behavior. With enough ALPR cameras collecting enough data, critics worry ALPRs will provide more than a series of point-in-time locations of a person, and conglomerate into a discernable pattern of a person's life and activities without the need for additional contextual data from sources that require legal process to obtain. They argue that widespread ALPR deployment therefore creates a mass surveillance dragnet, allowing governments or private entities to infer sensitive information about individuals, such as their political activities, religious practices, medical visits, or personal associations. Additional concerns include data retention periods beyond their usefulness in investigations, extensive information sharing among agencies that may use the data in ways the collecting community does not consent to, inadequate administrative oversight, and the potential for misuse of ALPR data by police.

Misuse of ALPR data for non-police purposes

Sensitive data maintained by the government has been misused by public officials for personal or commercial reasons. Officers can run criminal background checks on exes, romantic adversaries, or the rivals of an associate's business. They can access Department of Motor Vehicle data to learn the name, address, and cars owned by a driver, and search agency records to see if individuals are victims or suspects of criminal investigations or have reported crimes to the police.[12] These violations of public trust require effectively regulating the use of government-held data; they should motivate police to limit access to officers serving in relevant roles, to conduct frequent audits of data use, and to treat violations as serious matters requiring discipline, termination, and arrest where appropriate. They have not, however, been viewed as a reason not to collect the data in the first place, since the public safety benefits of doing so considerably outweigh these risks.

There is nothing inherent to ALPR data that places it in a different regulatory category than these other government-maintained data sources. In many respects, knowing the time, place and location of a person's vehicle in public poses fewer privacy risks than a person's criminal history, status as a crime victim or suspect, or home address. Legitimate concerns about the misuse of ALPR data should therefore take place in the larger context of longstanding efforts to combat the misuse of sensitive government data generally, and incorporate the same types of safeguards effectively used in other cases. In that regard, the potential for misuse falls into a set of scenarios that an agency can anticipate and prevent with safeguards and disincentives, as well as detect and address with the appropriate audits, investigations, and discipline.

ALPRs amid the continuum of data collection

In its dependence on contextual information from other sources to form a bigger picture, ALPR data is among the least intrusive type of information collected about people in terms of what it reveals about their private lives, which, along with the fact that it is data observed

in a public place, is one of the reasons courts have not required a subpoena or search warrant to collect and analyze it. Internet searches, web browsing history, credit card use, online and in-store purchases, banking history, texts and calls made by mobile phone, and the location of a mobile phone determined by the towers it connects to are data that provide a detailed and specific portrait of a person's actions, networks, associates, and movements. Generally, people assent to the corporate and government collection of this private data because it smooths daily transactions in their lives and is associated with goods and services they value. Likewise, ALPR data contributes to a vital government function, although its value arises when public safety is at risk, rather than the routine commercial and social transactions of daily life.

FIGURE 1

Data sources' ability to establish a pattern of life

	Identity	Location †	Speech, interests & plans	Purchases	Health	Beliefs & assoc.	Pattern score
Browsing & search history all searches and browsing from an IP address	✓	●	✓	✓	✓	✓	92%
Cell phone data carried everywhere, always on	✓	✓	✓	●	●	✓	83%
Credit cards & banking every electronic transaction	✓	●	✗	✓	●	●	58%
Medical records narrow in scope but extremely sensitive	✓	✗	✗	✗	✓	✗	33%
ALPR records a plate, a time, a place, a direction	●*	●	✗	✗	✗	✗	17%

✓ reveals a pattern factor (1 point) ● limited or partial reveal (½ point) ✗ not captured (0 points)

Each factor was weighted evenly to compute a cumulative pattern-of-life score, from 1 out of 6 (17%) to 6 out of 6 (100%). A limited or partial reveal of a pattern was scored as ½ (8.3%).

* A plate resolves to a registered owner only through a separate records check — it does not identify the driver at the time the data were captured.

† Location differs by source: cell phones provide a continuous track, financial transactions provide extensive location data, and ALPR provides location only at intermittent points in time, on public roads.

A pattern of life emerges only when ALPR data is accessed and searched, and the results are combined with the other data sources above — which is why effective safeguards target how the data is searched and used, not the fact of collection alone.

The emerging history of ALPR use

Despite a notable increase in its use by police in recent years, ALPR technology has been in use in several major US jurisdictions for about two decades. This extended period provides an opportunity to consider what privacy and liberty concerns have actually arisen in these jurisdictions, and how many cases of misuse by officers have been detected relative to the scale and duration of ALPR deployment. For example, the New York City Police Department has employed ALPR technology since about 2008, and presently utilizes it citywide, collecting hundreds of millions of license plate reads a year. While it is beyond the scope of this paper to make an empirical assessment about the NYPD, there is no indication in the public record of a history of tracking religious or political activity using ALPR data, or the recurring use of the data for unauthorized, non-police (i.e., personal or commercial) purposes. As ALPR use grows across the nation, we will be better able to assess the extent to which the most serious concerns about ALPRs actually materialize, or remain hypothetical. In the case of the nation's largest municipal police department, the risks appear to remain unrealized after nearly two decades of expanding use of the technology.

ALPRs and the democratic principle of restraint

The use of ALPRs allows for more tightly-focused enforcement across the spectrum of policing and criminal investigations. From proactive enforcement to responding to past crimes, knowledge of the specific times and locations of vehicles of interest allows police to cast narrower, more specific nets, locate suspects with greater precision, and build more accurate, higher quality cases against individuals accused of serious crimes. In this way, ALPR data can reduce the number of mis-identified suspects, police encounters with people ultimately uninvolved in a crime, and combat the biases that may occur when witness statements and identifications are not supported by more objective empirical evidence. Just as importantly, ALPR data can provide innocent people with a compelling alibi, or corroborate or bolster the account that vindicates them. A democracy that emphasizes personal liberty values restraint in its use of law enforcement, and ALPRs are a key contributor to more restrained police work. By this view, ALPR data collection does not target motorists for enforcement by police, but rather helps police identify the most important targets for investigation from among a pool of motorists in a community, allowing them to conduct enforcement with greater precision.

Restraint and data volume. When a type of data offers the potential to make policing more restrained, this potential can be positively correlated with the overall volume of data collected. This is based on the premise that the more thorough ALPR data collection is, the more likely it is to 1) provide probative evidence of a suspect's involvement in a crime, 2) reduce the chances that a probative data point went uncollected, and 3) increase the likelihood that ALPR records contain data that excludes innocent motorists from suspicion by providing or corroborating evidence of innocence. This is not meant to suggest agencies

should pursue a form of omnisurveillance in the collection of ALPR data, which runs the risk of revealing private behaviors by its nature. It does suggest, however, that thorough ALPR coverage in a community can increase restraint by increasing the probability of more focused and precise police work. Communities should deliberate about the best balance.

ALPRs and the reduction of the police dragnet

> **"The thorough collection of ALPR data can reduce the size of the police dragnet experienced by a community."**

The critique that ALPRs create a mass surveillance dragnet of innocent people presumes that the initial collection of data constitutes the dragnet itself. This is akin to saying the simple existence of credit card records or cell phone tower data create an unjustified surveillance dragnet of all Americans. The principles put forth in this paper instead suggest the size of the "dragnet" arising from a type of data collection should be measured by the number of people the data draws into suspicion, leading to criminal investigations and encounters with police. That number is countered by the number of people the data excludes from suspicion and subsequent police contacts. ALPRs capture a large volume of public data upstream, prior to police contact with citizens, to reduce the size of the actual dragnet used in their subsequent work. Rather than a wide search for a "black Ford truck," or a frantic, large-scale search for a specific license plate that spans several jurisdictions, ALPR data allow police to look for specific vehicles (and people) in specific places, while excluding large numbers of motorists from suspicion and police involvement. In doing so, the thorough collection of ALPR data can reduce the size of the police dragnet experienced by a community.

CASE - BURLINGTON, VERMONT - DECEMBER 2015.

Obafemi Adedapo, 28, was shot and killed on the sidewalk outside a nightclub in Burlington, Vermont. The ALPR on a sheriff deputy's car responding to the scene from outside the city recorded the suspect's vehicle headed toward the interstate. With the knowledge that the suspect was no longer in Burlington, local police reallocated resources from a widespread search for him in Burlington to interviewing witnesses and collecting evidence. Using ALPR data from cameras on the highway, they traced the suspect's car as it fled south. He was arrested in West Springfield, Massachusetts, and returned to Vermont to face a murder charge.[13]

ALPR placement and democratic fairness

Given their potential to improve the public safety of a community, the placement of ALPR cameras operated with public funds (as opposed to privately procured systems) can be

analyzed as the distribution of a public resource. The principles guiding ALPR placement across a given jurisdiction where cost is a limiting factor should therefore be guided by a commitment to the fair distribution of this resource. This suggests:

1. Priority placement in a) the communities that have the greatest comparative deficit in public safety that could be improved by ALPR use cases, and b) inherently critical locations (e.g. Times Square, Wall Street, Bourbon Street, etc.), followed by

2. Placement in key public places that benefit the entire community (e.g., throughout a jurisdiction-wide highway network or widely used public spaces), followed by

3. Placement in neighborhoods that already benefit from a comparatively high level of public safety.

Following this priority order ensures the neighborhoods with greatest need for improved public safety, and then the community at large, benefit from the placement of ALPR cameras before neighborhoods that already enjoy comparatively high levels of public safety. Deployment decisions can therefore be made by analyzing the incidence of the most serious, reliably reported crimes that underlie ALPR use cases.

Honoring the commitment to restraint. A fairness concern, however, is that ALPRs are not an unalloyed good: if used beyond the expectations of a community, they can expose people to the enforcement of a vast array of minor crimes and vehicle regulatory violations that would not have been detected but for the placement of ALPR devices. These include expired registrations, inspections, and insurance, as well as arrest on warrants for nonviolent misdemeanors, or for unpaid fines and fees. This would expose certain neighborhoods to disproportionate levels of enforcement for the minor violations detectable by ALPRs and the underlying records attached to a car's registered owner. While these enforcement actions might have a small positive effect on public safety, they could have serious consequences for an individual's finances or low-level arrest history. This invokes a concern about the fairness of ALPR-generated enforcement, especially when the neighborhood distribution of serious crime in a city falls along the lines of economic opportunity, which in the United States consistently invokes race, with minority communities exposed to greater enforcement of minor violations. Addressing this concern gives rise to an additional principle of fairness in ALPR placement:

> When distributing ALPR technology across communities, its subsequent use must be restricted to the cases that were analyzed to specify the distribution, as well as the additional range of serious but low-incidence use cases (e.g., abductions, fleeing felons, etc.). The analysis, the offenses it considers, and its results should be made public for inspection.

These principles therefore do not mean that democratic fairness requires distributing ALPRs equally across a jurisdiction. Rather, they require that any differences in distribution benefit

the neighborhoods that are the least well off in terms of public safety, followed by everyone, before they can be used to benefit the people who are already safer than their neighbors. Finally, democratic fairness requires that ALPRs are not used beyond the ways an agency publicly declares they will be, that the agency's analysis is based on these use cases, and that the criteria and results are transparent and verifiable.

The distraction of policing minor incidents. Beyond concerns about fairness, there is also the possibility that using ALPRs to enforce a wide range of minor offenses and vehicle status violations could be a net detriment to public safety. It is possible that handling an increased volume of minor incidents could translate into more time spent off patrol for officers, increased response times to more serious calls for service, and less effective proactive policing and investigation of serious crimes. This is an empirical question that may vary from agency to agency, but it leaves open the possibility that using ALPRs to enforce minor incidents could undermine not only an agency's commitment to fairness and restraint, but public safety in the communities that need it most.

Measuring the effectiveness of ALPR programs

One of the recurring challenges in assessing the effectiveness of ALPRs is attempting to determine their marginal value in some discrete, measurable way, as an individual unit of analysis. The belief that this is either necessary or possible may be based on an underestimation of the range and complexity of the police role. Granted, there are clear cases in which ALPRs make a decisive difference during a critical incident: for example, quickly locating a moving vehicle involved in an abduction, a mass casualty incident, or the shooting of a police officer.

Otherwise, ALPR data are a part of a larger system that detects crime, identifies and apprehends suspects, contributes to the legal adjudication of their actions, and deters and prevents future criminal incidents. As a part of this system, they can contribute to the overall quality of an investigation without being the standalone reason why a case was solved. Fingerprint evidence and the forensic analysis of shell casings and bullets are valued in criminal investigations even though they are understood to be parts of a much bigger process. In the same way, ALPR data contributes to public safety in ways that are not always simple to isolate and measure using experimental or quasi-experimental designs.[14] However, we can better understand the value of ALPR data by the role it plays in its most important use cases by using the following suggested measures:

TABLE 1

Measuring ALPR effectiveness by use case

USE CASE	SUGGESTED MEASURES
Recovery of stolen vehicles	Number, rate, and time to recovery
Location of persons in the midst or immediate aftermath of a crime	Number of apprehensions, time to apprehension
Locating the victim of an abduction	Number of investigative leads, time to reunion
Locating a person reported missing	Number of investigative leads, time to reunion
Apprehension of persons wanted for past crimes	Number of apprehensions, time to apprehension
Developing probable cause to arrest a known suspect	Number of cases solved, time to solution
Identifying a previously unknown suspect	Number of suspects named, time to identification
Contributing to the depth and quality of an investigation	Number of cases in which data is used as evidence
Narrowing the scope of an investigation	Number of cases in which suspects or investigative steps are eliminated
More efficiently directing investigative resources	Reducing investigative steps and focusing effort more precisely

In endeavoring to measure these outcomes, agencies can deliberately configure their records management and dispatch systems to automatically capture the data required, or to prompt officers to enter it during the completion of reports and records. Complemented by specific data fields that capture ALPR queries and their results, and the linkage of records across platforms, it is likely that the advent of large language models and AI-generated analyses will allow agencies to measure the outcomes above by determining at what point ALPR-related evidence was utilized, if it had an effect on the outcome of the incident, and how that compares to cases where ALPR data did not play a role in a case.

Cost effectiveness, critical incidents, and ALPRs

Police are tasked with responding to high-stakes incidents that are infrequent but require extraordinary effort and extensive resources when they do occur. This unique role makes assessing the cost effectiveness of the resources necessary for such a response much different than a traditional balance sheet approach would suggest. For the same reason, assessing the return on investment in preparing for these incidents goes beyond a simple

monetary calculation when the goal is to ensure a government is capable of discharging its duty to deliver effective public safety when citizens need it most.

> **“Police are justifiably expected to expend extraordinary resources in the search for an abducted child, a fleeing rapist, or a missing disabled person.”**

In other words, evaluating the government's preparation for low-frequency but critical public safety incidents is based on whether its preparation will allow it to effectively serve its most vulnerable victims, not on whether they are a comparatively cost-effective use of funds. By the nature of critical incident response, they rarely would be. For example, police are justifiably expected to expend extraordinary resources in the search for an abducted child, a fleeing rapist, or a missing disabled person, regardless of whether a more restrained response with fewer tools and resources would have been more cost effective for society or a local community in some overall sense. Assembling the core resources necessary for police to effectively respond to rare but critical cases to protect and rescue especially vulnerable victims is one of the basic requirements of democratic policing, rendering the marginal cost of doing so an ancillary concern.

ALPRs can be considered a core critical incident resource. ALPRs can quickly and decisively identify and locate the vehicles wanted in critical incidents, and rapidly narrow down the focus of a critical investigation so that other resources can be deployed more precisely and to greater effect, doing so in ways that improve on traditional means.

This framing suggests appropriate cost effectiveness criteria for ALPRs as a public safety tool. The criteria specify that the expense of a tool used by police is justified if:

1. It offers a discrete, articulable value in routine public safety use cases;

2. It can offer unique, decisive value in low-frequency critical incidents that are not resourced based on cost effectiveness; and

3. Utilizing it does not constitute an opportunity cost that directly interferes with other basic public safety duties.

Based on the demonstrated role of ALPRs, their comparatively modest presence in a municipality's public safety budget, and their steadily decreasing cost, they would likely meet such criteria in nearly all the jurisdictions in which ALPRs are presently deployed.

The unobserved outcomes of restraint. Another reason straightforward measures of ALPR effectiveness are elusive is their ability to reduce police activity in ways that honor the democratic principle of restraint but may not be reflected in measurable financial or public

safety outcomes. When ALPRs are used to focus an investigation on a particular vehicle rather than a more general description of one, to provide exculpatory evidence that eliminates people from suspicion, or to better target the search for a suspect, it protects the rights and liberties of innocent people in a way that may not be reflected financially or in traditional police outcome metrics.

“Using ALPRs to reduce police contacts with innocent people is a genuine public good.”

Using ALPRs to reduce police contacts with innocent people is a genuine public good, but it does not necessarily mean a case will be solved more quickly, that it will be solved at all, or that fewer stops of ultimately innocent people will save money or meaningfully conserve police resources. The use of ALPRs therefore generates a counterfactual that cannot be easily measured or monetized: the number of police stops and interactions with innocent people that would have occurred but for the narrowing effects of using ALPR data. Rather, this effect of ALPR use creates an independently valuable outcome in restraining the exercise of police power in a community.

The same ALPR data that protect the innocent should also serve the rights of the accused. A defendant should be able to obtain the record of the ALPR searches that produced evidence to be used against him, and agencies should honor reasonable requests to preserve ALPR data that may be exculpatory before a retention period deletes it. As a matter of due process, the potential for ALPR data to protect the innocent should be extended to people facing prosecution.

PART III

The Democratic Regulation of ALPRs

Regulating the tools of policing is an expectation of the profession, and the careful regulation of ALPR data is no different. Recognizing that nearly all the tools of policing have the potential for misuse, statutes, policies, and processes regulate the use of things ranging from firearms and pepper spray to the FBI's Criminal Justice Information System and a given state's motor vehicle and driver databases. Likewise, criminal records databases are regulated to seal certain records and purge others from the system after a given time. In all these cases, the goal is to prevent misuse, unnecessary harm, or storage of highly personal information beyond its usefulness and relevance. The use of ALPR technology should be subject to the same regulatory measures.

Principles of ALPR regulation. Leveraging ALPR regulation for the ends of public safety requires merging license plate data with other sources of information in ways that improve the quality of policing without exposing citizens to three risks: arbitrary or overbearing enforcement; use of the data by agencies for the enforcement of laws the community explicitly does not consent to (e.g., immigration law or the infringement of reproductive rights); and use for personal or commercial reasons unrelated to public safety.[10] Honoring this commitment means creating safeguards around data access, sharing, and retention, along with the ability to deter misuse, detect it when it occurs, and take transparent and appropriate disciplinary action.

Methods of ALPR regulation. The fair and effective use of ALPRs can be achieved through three complementary mechanisms: law, policy, and system programming or business processes. Laws define an agency's authority to collect, retain, access, and share ALPR data, while also providing avenues for oversight and accountability. Agency policies translate those legal requirements into operational standards in conjunction with internal knowledge about how to effectively deliver public safety, prescribing how personnel should collect and use ALPR data, under what circumstances, and with what supervisory oversight. Finally, system programming and business processes embed those rules into the technology itself through permissions, retention schedules, audit logs, automated alerts, and workflow requirements. In this way, vendors are key players in regulating ALPR technology: the firms that create, sell, and operate ALPR networks are positioned to build oversight tools into the product itself, such as automated, AI-based detection of anomalous or suspicious searches, mandatory reason codes that can be validated against other agency documents and information systems, and auditing capabilities that make administrative review feasible, frequent, and effective. A vendor that makes oversight more effective is a critical partner.

Tools of ALPR regulation. Beyond law and agency policy, the architecture of an ALPR system itself can serve as an effective mechanism of regulation. Processes built into the collection, retention, and use of ALPR data shape how the technology is used in practice by

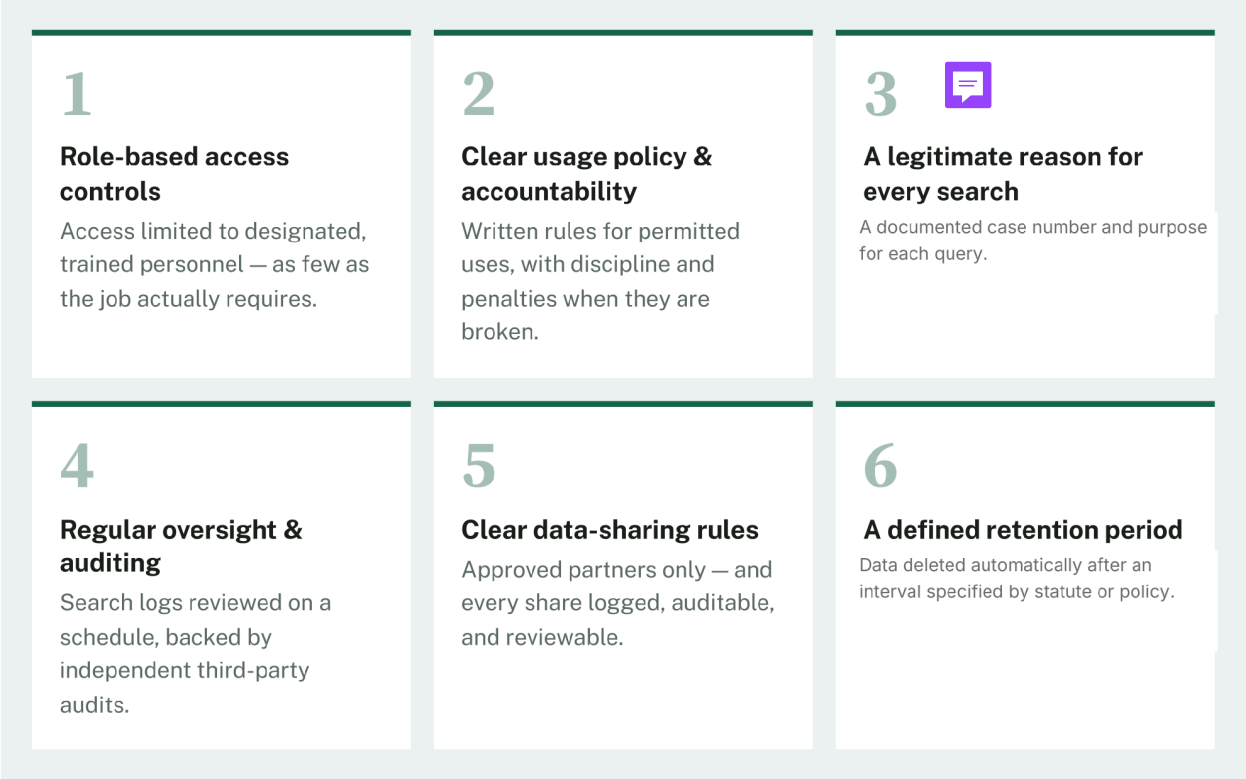
constraining discretion and ensuring transparency and accountability. Specified retention periods determine how long historical data is stored for investigative purposes, while geofencing can restrict ALPR data collection around designated locations such as houses of worship or medical facilities, for example.

Geofencing sensitive locations refers to programming mobile ALPR units to pause data collection near locations such as houses of worship and reproductive health care facilities, and to ensure stationary cameras are not positioned to read license plates in the immediate vicinity of such places. For example, in 2026, Washington legally barred ALPR data collection at sensitive locations, and Connecticut allowed them to opt out.[17] Communities should pursue such measures through careful deliberation, however, since geofencing comes with public safety tradeoffs. Sensitive locations have consistently been the target of terrorist attacks and other acts of violence and discrimination; having a record of which vehicles were in their vicinity at the time of an incident can prove critical to identifying its perpetrators. This tension between privacy and security makes geofencing an essentially contestable measure: a community can reasonably conclude that collection near sensitive sites should be prohibited to foreclose fears about government surveillance of protected activities, or decide that these locations deserve the investigative benefits that ALPR data collection can provide precisely because of their sensitive nature, especially in a well-regulated program with strong safeguards against misuse. For example, a community could implement a variable retention schedule, where ALPR data is generally retained for a period of 7, 30, or 90 days (i.e., some appropriate amount of time for most legitimate purposes), but data around sensitive locations would only be retained for 72 hours unless it was preserved in the aftermath of a critical incident to assist with the investigation.

Role-based access controls limit users to the ALPR queries necessary for their specific duties (e.g., detectives may have more access than patrol officers, or agency ALPR queries are made through a single officer with a specialized role). Confederated searches can be restricted to defined investigative purposes or to exclude specified agencies. Automated usage logs and audits create transparency by documenting who accessed data, when, and for what reason, deterring misuse and providing oversight. Likewise, limitations on data sharing with external agencies ensure that a jurisdiction's data is accessed by others only in accordance with established legal and policy requirements. Collectively, these controls operationalize fair, effective use and oversight by embedding the substance of an agency's regulations directly into the everyday functioning of the ALPR system, reducing reliance on individual discretion and compliance.

FIGURE 2

Six policy levers to prevent misuse and unauthorized sharing



Together these measures mirror the framework used by the FBI to govern local access to its Criminal Justice Information Services, which contains sensitive law enforcement data about millions of people. [15] *The security measures apply to every use case, regardless of the magnitude of the threat posed by misuse in each.*

Role-based access and the principle of least privilege

The misuse of ALPR data is most likely to arise when a wide range of officers have access to the system's search function with little supervision or oversight, an outcome observed across numerous documented instances of serious misuse resulting in the termination and arrest of police officers. One of the most effective ways to address the potential misuse of ALPR data prior to the point where investigations and discipline are necessary is therefore to implement role-based access using the principle of least privilege.

> **"Access should be given to the smallest number of people necessary to run an agency's ALPR program effectively."**

Under role-based access, the ability to search ALPR data is only accorded to officials working in a limited range of relevant roles, such as investigators and analysts, for example.

The principle of least privilege suggests that from among these actors, only a small number of key personnel be granted search privileges, highly concentrating responsibility and accountability while providing timely access during investigations and emergencies. In other words, access should be given to the smallest number of people necessary to run an agency's ALPR program effectively.

The principle of least privilege is a requirement that access to ALPR data is limited to the fewest number of people necessary to balance operational effectiveness with strong oversight and accountability. Investigators pursuing serious crimes would require timely, consistent access to a colleague authorized to perform broad, interagency ALPR searches, while officers performing patrol functions could receive and act on alerts, but be required to obtain supervisor approval to request a search from an investigative colleague authorized to query ALPR data. Administrative functions (e.g., changing system settings, approving sharing requests, adding users) should rest with a very small number of designated administrators. As a result, search privileges can be authorized in a way that allows for effective police work while concentrating accountability among a small number of properly trained and supervised individuals. For example:

- ALPR access during critical incidents could be conducted out of an agency’s communications and dispatch center, where at least one person working at any time would have access to the agency’s ALPR data, working under a supervisor responsible for reviewing the searches they conduct.
- At the level of the large municipality or regional task force, a crime intelligence information center with specially-designated analysts can provide sole access to ALPR data for investigative purposes. Under this model, ALPR queries can be routed to a designated analyst who then documents the person and unit making the request, the reason for it, and what supervisor at the agency authorized the query.
- For smaller agencies, non-emergency ALPR data access can be granted to a designated investigator, or civilian working in an administrative role, who can be the executor of the agency's ALPR queries.

Under any of these models, requiring a documented purpose for each ALPR query, subject to supervisory review, along with specifying a case or incident number, will add a second layer of oversight and accountability to ALPR data access.

The handful of individuals granted access to ALPR data under the principle of least privilege should receive training in the recognition of suspicious or unauthorized inquiries, and be granted the ability to make confidential allegations of improper requests to an internal affairs or inspector general entity with an obligation to investigate them.

There is a precedent in policing for this type of access control. The FBI's Criminal Justice Information Services are a nationwide digital storehouse of searchable, highly sensitive criminal history and intelligence information about millions of Americans shared by nearly every law enforcement agency in the United States. The system’s use is governed by strict cybersecurity requirements, and agencies are expected to employ the principle of least

privilege in providing access to the system.[15] In general, the requirements and safeguards that protect this immense body of sensitive information can be used to inform the basis of an effective agency-level ALPR use and access policy.

Vendors. In addition, vendors can effectively reduce the incidence of ALPR misuse and violations of privacy by leveraging their own technological advances, and setting procedural norms. Technology providers can embed governance requirements directly into their products and terms of service, conditioning the sale and continued operation of ALPR systems on agency commitments to training, role-based access, auditing, and incident reporting, much as cloud providers require security attestations of their customers and the FBI requires agencies seeking CJIS access to meet its security requirements. For example, in August of 2026, the ALPR vendor Flock built the following safeguards into its operating system for all users:

- A default ALPR data retention period of seven days, down from 30;
- A means to preserve data with potential investigative value while allowing the remainder of the contemporaneous ALPR data to be deleted;
- Requiring a search category be specified for all confederated searches, while allowing agencies to block the use of their data for certain categories (e.g., immigration enforcement vs. investigating violent crimes)
- A mandatory AI-driven feature that automatically monitors all searches and flags abnormal patterns;
- Automatically locking out users the system flags as having engaged in suspicious search behavior until the incident is assessed by a supervisor;
- Requiring a verifiable agency case number before executing any historical database query;
- Allowing for a narrow range of critical incident exceptions that bypass restrictions but are then escalated to agency supervisors for mandatory review.

Vendors that adopt this type of posture can protect communities by ensuring their technology is not deployed by agencies unprepared to effectively regulate it. Where the pace of technological change has outrun the institutional capacity of some agencies to govern new tools, requirements built into the technology and its contracts can impose an appropriate regulatory standard on those agencies.

Reducing false alerts. Agencies should utilize redundant safeguards to prevent false alerts, which subject innocent citizens to dangerous and stressful encounters with police. These typically arise from errors in entering license plate numbers onto a hot list of stolen vehicles or those associated with a crime, or failing to remove expired alerts. The following three measures can serve to prevent such incidents: 1) Plates should be verified by a designated authority (e.g., a supervisor or detective) before they are entered on to a hotlist, then verified by an agency employee that they have been entered correctly, before they can yield an alert; 2) When there is doubt about the accuracy of a license plate, do not enter the plate; 3) Verify that the image captured by an ALPR matches the plate observed by an officer

before conducting a stop based in an alert; 4) Do not enter incomplete or partial plates into an alert system barring exigent circumstances, such as an imminent threat to life, that would justify forcibly stopping a vehicle if an officer were to visually spot the vehicle on the road.

Judicial process and ALPR searches

One approach to regulation would require police to obtain a judicial warrant that demonstrates probable cause before searching stored ALPR data; Minnesota, for example, has enacted this requirement for certain queries. These proposals are based on the idea, espoused in this paper, that the risks posed by ALPR data lie not in their collection per se, but in how the data is subsequently used. A warrant requirement therefore imposes a high threshold for searches by regulating them through judicial oversight. It would not be an appropriate requirement for several use cases, however. For real-time alerts for stolen vehicles, missing and abducted persons, and wanted felony suspects, judicial process would be impracticable, which is why warrant-based regulatory proposals typically carve out exceptions for these cases. Beyond this, quickly identifying a suspect in the immediate aftermath of a crime or other cases where ALPR data can be used to help generate probable cause and eliminate innocent parties would be foreclosed by a warrant requirement, rendering an important function of ALPRs moot. However, use cases such as the extensive search of a person's historical movements over a long period approach the reconstruction of a person's private life in a manner that has led courts to require warrants for long-term cellphone location tracking and other roughly analogous types of data collection. In light of this, communities that adopt long retention periods should recognize that the case for a warrant requirement strengthens as the retention period grows and the agency's range of authorized use cases remains broad. In contrast, jurisdictions that pair shorter retention with a thorough use policy, a limited range of use cases, and effective administrative controls, can more persuasively argue that a warrant requirement would be unnecessary.

Retention periods

Deleting ALPR data after a specified period demonstrates an agency's commitment to leveraging the data only in accordance with its declared use cases, and otherwise respecting the privacy and liberty of citizens by discarding the data when it is no longer likely to be useful. ALPR data should therefore be retained only as long as it can be reasonably expected to play a role in the use cases it has been authorized for. As an underlying principle, once ALPR data has been gathered, neglecting an opportunity to use it to solve a serious case, or to build as strong a body of evidence as possible, would be a notable act of omission on the part of the agency involved. However, once enough time has passed that this use becomes unlikely, the data should be deleted.

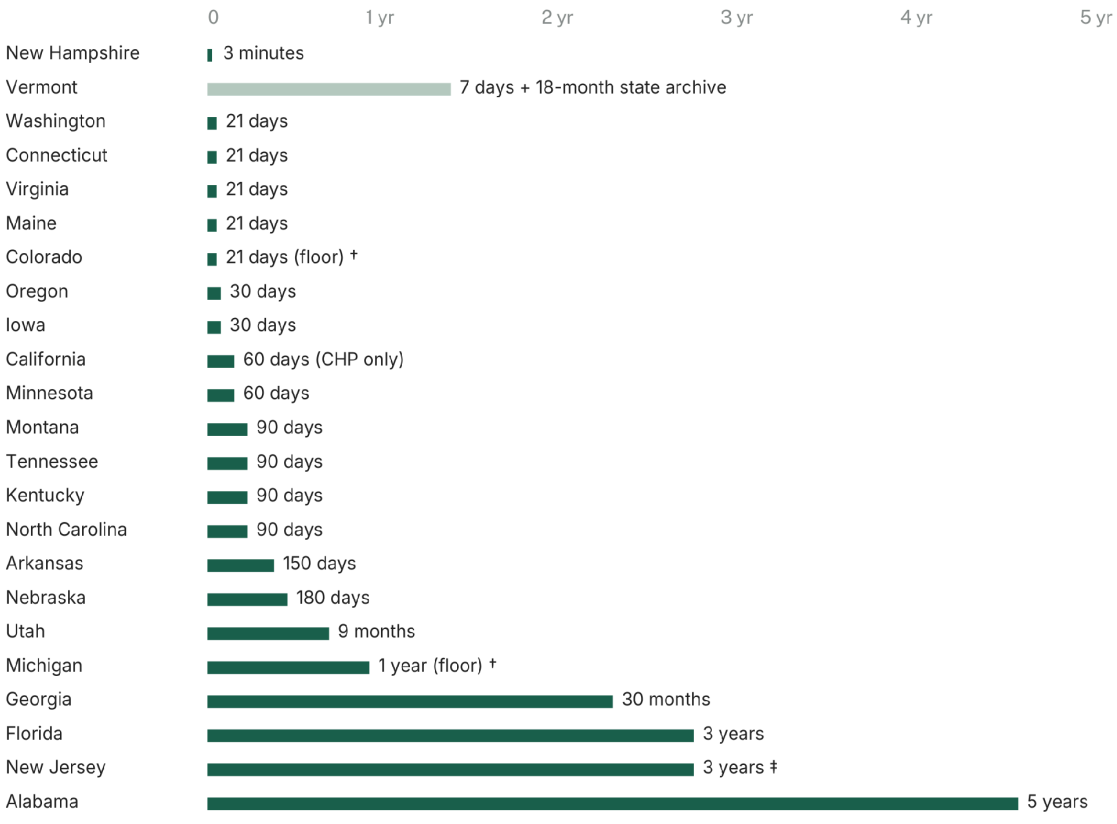
Critically, this duration is an empirical question. For their most serious crime types, agencies can measure the interval of time between a given incident and the point at which

investigators develop a vehicle-related lead, query ALPR data, and incorporate the results into the investigation, while also accounting for incidents in which a suspect could have stalked a victim or conducted reconnaissance beforehand. This interval for each case, between the date of incident and the date ALPR data is incorporated into a case, will coalesce into a time range that reflects the natural variance in the progression of investigations. Within this time frame, a retention period can be set that allows ALPR data to be accessed in all but the most outlying instances. Stated more rigorously, a fair and effective retention period would sit at the tail end of this time frame, i.e., the second or third standard deviation of the mean incident-to-incorporation time for the most serious crimes a community expects the technology to help solve. To date, however, states have not taken this type of empirical approach. Instead, they have set maximum retention periods ranging from three minutes to several years based on sentiment or intuition rather than evidence.[16]

FIGURE 3

ALPR retention periods by state: three minutes to five years

Statutory maximum retention of non-evidentiary ALPR data, May 2026 — bar length proportional to time [17]



The other 27 states set no statutory retention limit.

The retention period that best balances significant investigative value with privacy protections is an empirical question that national clearance data have only begun to answer.

‡ Set by Attorney General directive rather than statute.

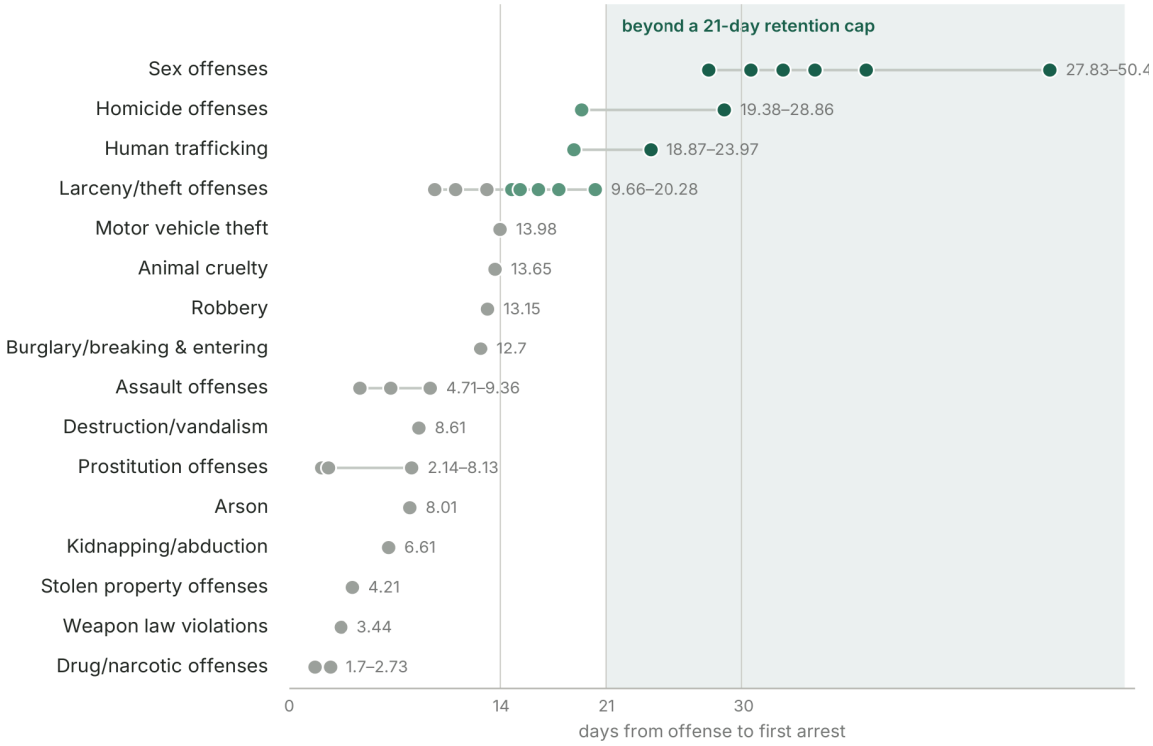
† Colorado and Michigan derive from LPR-specific records-retention schedule provisions, not standalone statutes.

Absent such analyses, national crime data can be used to assess what retention periods are likely to comport with the empirical approach described above. A replicable analysis of the 2024 incident data publicly available in the FBI's National Incident-Based Reporting System (NIBRS), covering roughly 96 percent of the U.S. population, was conducted by Flock Safety, an ALPR vendor. The vendor examined the interval from the date of incident to the date of arrest for several crime categories, under the logic that the resulting time frames can preliminarily suggest the outer limits of a suitable data retention period.[18] The study found that 21% of homicide arrests, 23% of human-trafficking arrests, and 31% of sex-offense arrests, for example, occurred more than 21 days after the date of incident, and 24 serious crime types average more than 14 days from the date of incident to arrest. Figure 4 presents the scene-based offenses among these categories, i.e., those in which a suspect's physical presence is a basic element of the crime. While this analysis does not yield a precise recommendation, it infers that retention periods of 21 days or fewer will discard ALPR data while a significant share of serious investigations remain unsolved, suggesting that the default 7-day retention period set in August of 2026 by Flock is a starting point that strongly emphasizes privacy protections over the sheer efficacy of the technology.

FIGURE 4

How many days scene-based crimes take to clear by arrest

Each dot is one offense type: its mean number of days from offense to first arrest, 2024 NIBRS [18]



Green dots: offenses averaging more than 21 days to clear. Limited to offenses in which a suspect's physical presence at a scene is intrinsic to the crime; remotely committed and financial offenses are excluded. Compiled by Flock Safety from FBI 2024 NIBRS data; cleared cases only; publicly reproducible. Measures when crimes are solved by arrest; the data enters a case earlier, when a vehicle lead develops. [18]

In sum, data retention periods should be formulated considering the investigative value of historical ALPR data rather than exclusively by its real-time operational uses. Ongoing investigations that capture ALPR reads associated with designated vehicles of interest, as well as efforts to locate actively fleeing suspects, do not depend on a predefined retention period because the value of the ALPR data in these cases lies in near real-time detection. By contrast, retention periods affect the extent to which historical ALPR data enables investigators to solve crimes after they occur, develop investigative leads, corroborate emerging evidence, and ultimately improve investigative outcomes. In doing so, historical ALPR data can eliminate suspects and affirm innocence as well as build criminal cases against the guilty. Consequently, retention schedules can be informed by empirical evidence demonstrating the period over which stored ALPR data continues to contribute meaningfully to criminal investigations, rather than by arbitrary or solely precautionary timeframes.

FIGURE 5

How retention period affects privacy exposure

Longer retention periods increase both investigative reach and potential privacy concerns

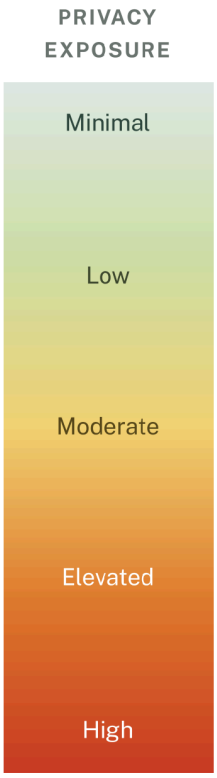
Minutes to days — up to 7 days
Instant alerts: stolen cars, abducted & missing people; immediate follow-up on hit-and-runs and fresh crime scenes.
e.g., New Hampshire's 3-minute rule; Vermont's 7-day active window

Weeks — 21–30 days
Adds recent-crime searches: witness-description sweeps, direction of travel, alibi and exculpatory checks.
e.g., Washington, Virginia, Maine, Colorado, Oregon, Iowa

Months — 60–180 days
Adds pattern crimes: serial burglaries, trafficking routes; linking older unsolved cases to fresh leads.
e.g., eight states from 60 to 180 days

A year or more — 9–30 months
Adds long-running investigations: organized crime, extended conspiracies, multi-season patterns.
e.g., Utah, Michigan, Georgia

Years to forever — 3–5 years, or no limit
Adds cold-case lookbacks, and enough history to corroborate significant patterns in a driver's private life.
e.g., Florida, N.J., Alabama — plus the 27 states with no limit



Elements of an agency ALPR policy

There are several core topics that every ALPR policy should address:

- The range of use cases, tying ALPR use to public safety objectives rather than general surveillance. Legislatures can list the authorized uses of ALPR data collection directly in statute (e.g., the recovery of stolen vehicles, locating missing and endangered persons, the investigation of serious crimes, etc.) as well as legally restrict the use of ALPR data for purposes of immigration enforcement or the investigation of lawful reproductive healthcare.
- The methods used to determine ALPR deployment, the public safety and democratic principles they reflect, and the underlying assumptions that drive them.
- Privacy and civil liberties safeguards, including consideration of deployments near sensitive locations (e.g., places of worship, health care facilities, or political gatherings).
- Criteria for populating alert lists and periodic review of their content and necessity.
- Policies governing sharing and use of commercial/third party ALPR data, including defining authorized sources.
- Oversight of access and use, including auditing and compliance frameworks.
- Oversight of AI and other analytical tools that may be applied to ALPR data to detect patterns, draw inferences, or merge ALPR data with other sources.
- Periodic review to reflect changes in technology, law, and community expectations.

Core themes and content of ALPR legislation

In order to ensure ALPRs enhance public safety while safeguarding rights in accordance with the principles of democratic policing, state and local legislation should address the following areas that govern ALPR procurement, deployment, and use:

1. Authorized purposes of ALPR use in furtherance of public safety

2. Agencies authorized to use ALPRs

3. Transparency in the principles and methods used to determine ALPR deployment

4. Data retention periods and requirements to document data deletion

5. Data sharing between federal, state, and local agencies: conditions, limits, MOU and compliance requirements

6. Mandatory privacy protections, to include geofenced protected areas such as health care facilities and houses of worship

7. Security safeguards for both physical and cybersecurity

8. Creation, maintenance, and inspection of audit logs

9. The requirements for agencies to devise a written agency policy

10. Training and certification requirements

ALPRs and public trust

> **"Accomplishing these goals together demonstrates a commitment to using evolving technologies to foster greater trust in police, not as a technological measure that attempts to compensate for a gap in that trust."**

The use of ALPR technology presents a two-pronged opportunity to improve public trust in police. First, the effective use of ALPRs demonstrates local leaders take the safety of their citizens seriously and are willing to invest in evolving technologies to achieve it. Second, effectively regulating the use of ALPRs demonstrates that a police department understands the power of its tools, their potential for misuse, and carefully regulates its work to respect citizens' rights and liberties. Accomplishing these goals together demonstrates a commitment to using evolving technologies to foster greater trust in police, not as a technological measure that attempts to compensate for a gap in that trust.

Conclusion

The concerns surrounding ALPRs have often been framed as a binary choice between public safety and privacy. Instead, the more appropriate question may be how ALPRs can be implemented so that they improve public safety while remaining faithful to the democratic principles of fairness, restraint, transparency, and accountability. ALPRs are investigative tools that can generate accurate information about vehicles in public places. Their public safety value arises when this data is combined with other knowledge and evidence to locate victims, apprehend dangerous offenders, improve the quality of criminal investigations, and exonerate the innocent. Yet, this data can be misused in ways that threaten people's privacy and erode their trust in government. Their legitimacy therefore depends not only on the public safety benefits of ALPRs, but on the safeguards that prevent their misuse and demonstrate that police are careful stewards of the data citizens place in their trust.

Democratic policing requires the careful regulation of state power. ALPRs can advance this objective by enabling police to conduct more precise, restrained, and effective investigations that reduce unnecessary police contact with innocent members of the public. Achieving these ends requires an evidence-based framework that integrates law, policy, and system design in a manner that grounds retention periods and deployment strategies in empirical research, and evaluates whether ALPR programs fulfill the public safety purposes they were designed to. By treating ALPRs as one component of a broader public safety strategy rather than as a standalone technology, police departments can leverage their benefits while enhancing the public's trust.

APPENDIX A

Essential Elements of an ALPR Policy

Each element below answers one or more of the concerns documented in Part II: concerns about privacy and revealing a person's pattern of life can be addressed by retention limits and confederated-search controls; misuse of ALPR data by public officials can be minimized by role-based access, the principle of least privilege, audit logs, and discipline; overbroad use of the technology that imposes unreasonable burdens on motorists may require limiting ALPR use to specified, authorized purposes and transparency in reporting. Together, these 13 elements mitigate the risks this paper describes.

1. Purpose. The function of ALPR technology, the public safety objectives it contributes to, and the ways in which this comports with our democratic expectations of policing. The purpose statement should establish that ALPRs exist to support lawful, effective policing while protecting privacy and civil liberties.

2. Statement of principles. Articulate the principles that guide the policy: ALPRs are to be used only for legitimate public safety purposes; the protection of Constitutional rights and privacy; accountability and transparency; specify the range of use cases; ALPRs as a tool to better focus policing and reduce police encounters with innocent people; compliance with state and local laws governing ALPR use.

3. Data collection. Describe: what data will be collected; what metadata accompany each read; whether third-party or commercial data may be acquired; any geographic or deployment limitations. The rationale for camera deployment decisions: camera locations should be justified by documented public safety needs, such as crime patterns, traffic corridors, and critical infrastructure, under criteria published in advance, so that coverage verifiably follows demonstrated need, and communities are able to inspect the rationale for placement.

4. Administration, authority, and chain of command. Identify what rank/title in the agency is responsible for administering the ALPR program; assign specific responsibilities for ALPR deployment; user authorization; system configuration and maintenance; cybersecurity; auditing; training; data-sharing agreements and compliance. Ideally, a single executive-level individual, identified by title, should be responsible for user authorization, the execution and review of audits, and compliance with sharing agreements.

5. Authorized uses. This is the core section limiting discretionary use. It should define what roles and positions may use the system; what use cases are authorized and prohibited (e.g., personal use, political surveillance, curiosity searches, etc.); documentation requirements for investigative queries. The list of authorized uses should be limited enough to be readily understood, but specific enough to be audited: e.g., locating stolen vehicles and vehicles associated with wanted persons, locating missing and endangered persons, and searching for vehicles connected to criminal investigations. Prohibited uses should be clear and specific enough to accurately deter the related queries, provide a clear basis for audit conclusions, and to substantiate and resulting discipline.

6. Operational procedures. Specify how ALPR alerts are handled, verification before enforcement action; confirmation that a hit is valid and actionable; documentation of actions taken based on ALPR results. Critically, the verification requirement guards against taking action against an innocent motorist based on a stale or misread alert. Vehicle stops should not proceed until an alert has been

verified through CJIS or the original agency of record. Any consequential police action should require human confirmation of the plate, the vehicle, and the accuracy of the underlying record.

7. Data quality and accuracy. The policy should recognize that ALPR data provide investigative leads rather than definitive evidence or probable cause. Require procedures to ensure standards for creating and maintaining watch lists, hot lists, and alerts, including verification before inclusion; correction of errors; steps for quality control over manually entered information.

8. Data access. Define what agency roles may access stored data; levels of authorization for broader or deeper searches; logging of all searches and queries; supervisory oversight. Access should reflect the least-privilege framework described in Part III.

9. Information sharing. Establish rules governing sharing ALPR data with other agencies; required legal authority or agreements; documentation of disclosures; permissible recipients; restrictions on downstream use. Sharing agreements determine whether a community's governance continues to apply once its data crosses jurisdictional lines. Written agreements should bind recipient agencies to the originating agency's authorized purposes, provide for reciprocal auditing so that the sharing agency can inspect the queries run against its data, and extend the originating jurisdiction's restrictions (e.g., a prohibition on immigration enforcement or the investigation of lawful reproductive healthcare) as conditions of continued access. Where a prospective recipient does not maintain equivalent controls, the presumption should be against sharing. Since broader sharing generally yields better public safety outcomes when offenders flee or move between jurisdictions, the scope of a sharing network requires deliberation about the risks and benefits involved.

10. Data retention. Specify the agency's ALPR data retention period; legal exceptions; evidentiary preservation; automatic deletion procedures; how purging is documented. The retention policy should state a defined period, the intention, evidence, or law supporting it, and a schedule for revisiting it if it is not dictated by statute. If an empirical methodology such as the one suggested in Part III is used to calculate a retention period, the methodology should be specified in the policy.

11. Security. Require administrative, physical, and technical safeguards to protect stored data; system integrity; user credentials; audit logs; disclosure of violations.

12. Auditing, transparency, and accountability. Require periodic review of deployment decisions; which agency users have access and why; search activity; data quality; compliance with policy; misuse or unauthorized access. While the frequency of audits may vary by agency, a quarterly schedule is frequent enough to detect misuse in a timely manner. A policy should adopt a defined schedule, publish it, and release the results of each audit to the public and elected officials for inspection and review. Ideally, in an agency of sufficient size, the person with ultimate agency responsibility for the audit should not have access to the ALPR system except for the purpose of the audits, i.e, they should not be able to run the queries they are responsible for auditing.

13. Training. Require initial and recurring training, tailored to particular roles, covering system operation; legal standards; privacy protections; data management; agency policy; consequences for misuse. Training should function as a condition of access to the ALPR system.

Elements of ALPR legislation

For the purposes of legally regulating ALPR use, legislators can take the elements of the proposed model agency policy above and codify any of them in statute with the exception of those related to specific technical requirements or the unique administrative structure of the

jurisdictions the law intends to affect. In such cases, specific requirements can be replaced with more general provisions. For example, see items 4 and 8 above. Statutes are an important complement to agency-level policies because they bind every agency in a state, as well as successive administrations, and create legal rights that can be enforced. At a minimum, legislation should codify 1) authorized purposes explicit restrictions, data retention period(s), auditing and public reporting requirements, conditions under which data may or may not be shared, and 2) consequences for violations to include suppression of evidence, civil remedies, or the decertification of an agency's program.

APPENDIX B

ALPR Governance Workbook

The essential elements above describe what a sound ALPR policy should contain. This workbook converts them into two instruments a community can use: a self-assessment checklist for evaluating an existing or proposed ALPR program against those elements, and a worksheet setting out the decisions each jurisdiction must make for itself, with the considerations this paper's framework supplies for making them. Together they are intended for the settings where ALPR governance is actually decided: a council hearing, a policy revision, a procurement review, or collaboration between an agency and the community it serves.

Part 1. Policy self-assessment checklist

Each question below corresponds to one of the essential elements of an APLR policy that satisfies the framework this paper proposes.

PURPOSE AND PRINCIPLES

- Does the policy state the public safety purposes ALPRs serve and affirm that they operate within the democratic expectations of policing?
- Does it articulate governing principles: legitimate purposes only, protection of constitutional rights and privacy, accountability, transparency, and proportionality?

DATA COLLECTION

- Does it specify exactly what data and metadata each read collects?
- Does it address whether third-party or commercial data may be acquired, and any geographic or deployment limitations?

ADMINISTRATION

- Does it name who administers the program and assign responsibility for deployment, user authorization, system configuration, cybersecurity, auditing, training, and data-sharing compliance?

AUTHORIZED USES

- Does it define which roles may use the system and for which operational purposes?
- Does it name the prohibited uses, including personal use, political surveillance, and curiosity searches?
- Does it require documentation, including a case number and purpose, for every investigative query?

OPERATIONAL PROCEDURES

- Does it require verification that an alert is valid and actionable before enforcement action is taken?
- Does it set standards for creating, maintaining, and expiring watch lists and alerts?

DATA QUALITY

- Does it require procedures for hot-list accuracy, verification of machine-read results, and correction of errors?

DATA ACCESS

- Does it define which roles may access stored data, with levels of authorization for broader or deeper searches?
- Is every search and query logged, with supervisory oversight?

INFORMATION SHARING

- Does it establish which agencies may receive data, under what legal authority or agreements, with documented disclosures and restrictions on downstream use?

RETENTION AND PURGING

- Does it state an explicit retention period, with automatic deletion, documented purging, and defined evidentiary exceptions?

SECURITY

- Does it require administrative, physical, and technical safeguards for stored data, system integrity, user credentials, and audit logs, with disclosure of violations?

AUDITING AND ACCOUNTABILITY

- Does it require periodic review of deployment decisions, user access, search activity, data quality, and compliance?
- Does it specify corrective actions, including discipline, when violations occur?

TRAINING

- Does it require initial and recurring role-tailored training covering system operation, legal standards, privacy protections, agency policy, and the consequences of misuse?

Part 2. Five decisions every jurisdiction must make

Five key decisions about ALPR use will recur across every jurisdiction committed to their fair, democratic use. For each, this worksheet presents a series of options and the considerations this paper's framework offers for choosing among them.

Decision 1. Which uses will be authorized?

- Real-time alerting only: stolen vehicles, missing and abducted persons, wanted persons with known plates.
- Adding investigative searches connected to serious crimes.
- Adding evidence gathering and pattern investigations.
- Adding enforcement of vehicle status offenses and low-level warrants.

Each additional set of uses may expand the overall utility of ALPR data, but carries increased risks as well, and likely with diminishing public safety returns. In the case of low-level

enforcement, camera placement determines which communities will bear the greatest burden of enforcement, no limit on the data's retention period reduces that burden, and communities with higher serious crime rates may receive more ALPR cameras. Whatever set of use cases are chosen, prohibited uses should also be explicitly listed in the resulting policy as well.

OUR DECISION: _____

Decision 2. How long will data be retained?

- Minutes to days: alerts are issued in real time and unmatched reads are quickly purged.
- Roughly 21 to 30 days: recent-crime searches become possible; the emerging norm among states that legislate ALPR use.
- 60 to 180 days: pattern and serial investigations become possible.
- Variable retention periods for different types of data, e.g., general ALPR records vs. those recorded around sensitive locations.
- A year or more: long-running investigations and cold-case lookbacks become possible.

Retention periods should match the longest period of time ALPR data has been shown to play a probative role in the most serious use cases an ALPR system has been authorized for. In practice, this would be the amount of time that passes between the occurrence of an incident, its reporting to authorities, the commencement of an investigation, the pursuit of investigation leads that involve vehicles, and the querying and preserving of the relevant ALPR data, accounting for natural variation such a time frame. For some incident types, this period would extend back to include the time when a suspect may have stalked their victim or conducted reconnaissance of a target location. National crime clearance data offer a basic starting point for estimating this period of time, revealing that crimes such as homicide, felony sex offenses, and human trafficking investigations yield arrests, on average, well after the shorter retention periods found in many statutes. This suggests shorter periods may impose an investigative cost, especially if vehicle-related investigative leads are usually developed shortly before arrest. To address these concerns, communities can adopt evidence-based retention periods determined by the observed age of the data that materially contributes to their agencies' case outcomes.

OUR DECISION: _____

Decision 3. Who will have access, and on what terms?

- Widespread credentialed access, with logging and audit.
- Role-based tiers, with broader search authority reserved to designated roles.
- Queries channeled through a small number of designated personnel who search on behalf of colleagues.

The principle of least privilege specifies the most restrictive access consistent with operational need: as few personnel as required to effectively use ALPR data, matched to

their duties, and never general or widespread access for agency employees. The principle concentrates accountability and deters misuse because the comparably small number of people holding access are answerable for every query made under their credentials. The FBI's governance of its Criminal Justice Information Services demonstrates that US police departments effectively access more sensitive data under such restrictions.

OUR DECISION: _____

Decision 4. With whom will data be shared, and on what terms?

- No external sharing.
- Named agencies, under written agreements, for defined purposes.
- Participation in confederated searches, subject to category conditions and audit.

Sharing rules should identify permissible recipients, require documented disclosures, and restrict downstream use. Several states now condition out-of-state sharing on written assurances about the purposes the data will not serve; jurisdictions should decide in advance which types of queries should be blocked. Because legal process seeks the database itself rather requires a specific type of search, sharing and retention decisions together determine what data would be available for subpoena.

OUR DECISION: _____

Decision 5. What will the public know, and how will it be informed?

- Publication of the ALPR policy itself.
- The criteria used to allocate ALPR resources used throughout the community, and the data used to operationalize these criteria.
- Annual transparency reports on searches, alerts, and outcomes.
- Publication of audit results and camera placement criteria.

Transparency is a key element of an ALPR program, not simply a desirable accessory to it. As a technology that collects and stores data about the public, ALPRs are an expression of government power only possible through taxpayer funding and consent, as the product of a fair democratic process. Transparency is the means by which the public and its elected representatives are empowered to undertake, authorize, and sustain an ALPR program, and the means by which the program retains its democratic legitimacy.

OUR DECISION: _____

For legislators, this checklist can be used to provide the contents of a statute. As noted in the preceding section, nearly every element of importance to the fair and democratic use of ALPRs can be codified in statute, with narrow technical requirements replaced by general directives. A statute that conforms to the items presented in the checklist should be in accordance with the values and specifications presented in this paper.

References

1. "Kidnapping, Assault Suspect Arrested With Help From License Plate Reader in Mira Mesa," NBC 7 San Diego (City News Service), June 8, 2026. https://www.nbcsandiego.com/news/local/kidnapping-assault-suspect-arrested-with-help-from-license-plate-reader-in-mira-mesa/4034320/

2. Utah Department of Public Safety, "Update on Multi-State Triple Homicide Investigation and Apprehension," March 5, 2026, https://dps.utah.gov/press-releases/update-on-multi-state-triple-homicide-investigation-and-apprehension/; see also Associated Press, "Suspect in Custody in Colorado in the Case of 3 Women Found Dead in Utah," March 5, 2026.

3. U.S. Department of Homeland Security, Science and Technology Directorate, Automated License Plate Reader Systems Market Survey Report (2025) (documenting sixteen CJIS-compliant commercial systems and vendor-integrated capabilities beyond plate reading, including AI-driven vehicle classification and attribute search).

4. United States v. Ellison, 462 F.3d 557 (6th Cir. 2006) (no reasonable expectation of privacy in a license plate, whose purpose is to provide identifying information in plain view); see also New York v. Class, 475 U.S. 106 (1986). https://law.justia.com/cases/federal/appellate-courts/F3/462/557/525039/

5. See Commonwealth v. McCarthy, 484 Mass. 493, 142 N.E.3d 1090 (2020) (collection and limited use of ALPR data held not to constitute a search), and the state authorities collected in the NCSL compendium cited at note 16. The contrary ruling is Commonwealth v. Bell (Norfolk Cir. Ct. 2024); the Virginia Court of Appeals has since rejected its holding, and courts have declined to follow it.

6. Commonwealth v. McCarthy, 484 Mass. 493, 142 N.E.3d 1090 (2020) ("With enough cameras in enough locations, the historic location data from an ALPR system . . . would invade a reasonable expectation of privacy"; four fixed cameras on two bridges did not, and the court declined to define the threshold). http://masscases.com/cases/sjc/484/484mass493.html

7. Carpenter v. United States, 138 S. Ct. 2206 (2018) (warrantless acquisition of historical cell-site location information is a Fourth Amendment search; aggregated location records that reveal "the whole of [a person's] physical movements" are protected notwithstanding their disclosure to a third party).

8. "Police: Four Accused in Killing of Transgender Man Found in San Diego," VTDigger, June 3, 2016. https://vtdigger.org/2016/06/03/police-four-accused-in-killing-of-transgender-man-found-in-san-diego/

9. "Flock License Plate Readers Shared Data With Out-of-State Agencies, Ventura County Audit Finds," CBS Los Angeles, February 28, 2026 (more than 364,000 out-of-state queries in roughly two months); "Audit Shows San Francisco Police Flock License Plate Camera Data Accessed by Outside Agencies," CBS San Francisco, June 2026. https://www.cbsnews.com/losangeles/news/flock-license-plate-readers-shared-data-with-out-of-state-federal-agencies/

10. University of Washington Center for Human Rights, "Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement," October 21, 2025 (documenting direct, back-door, and on-behalf-of searches of Washington ALPR networks by or for federal immigration authorities, and a Texas agency's query of Washington data in an abortion-related investigation); see also 404 Media, May 2025 (more than 4,000 network lookups performed at the request of federal immigration authorities). https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/

11. No subpoena or court order compelling production of a local agency's ALPR records had been publicly reported as of July 2026. See, e.g., KOMO News, February 2026 (Seattle officials confirming no subpoenas for the city's ALPR data). Federal access documented to date has instead occurred through network-sharing configurations rather than legal process; see note 10.

12. Sadie Gurman and Eric Tucker, "Across US, Police Officers Abuse Confidential Databases," Associated Press, September 28, 2016 (documenting more than 325 firings, suspensions, and resignations for database misuse, 2013-2015). https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/

13. "Murder Suspect Pleads Not Guilty in Church Street Killing," VTDigger, January 4, 2016; "Burlington Police Investigate Fatal Shooting on Church Street," Vermont Public, December 27, 2015. https://vtdigger.org/2016/01/04/murder-suspect-pleads-not-guilty-in-church-street-killing/

14. See, e.g., Christopher S. Koper and Cynthia Lum, "The Impacts of Large-Scale License Plate Reader Deployment on Criminal Investigations," Police Quarterly (2019) (survival analysis of the Charlotte-Mecklenburg Police Department's fixed-camera network: ALPR data contributed to resolving five percent of sampled auto thefts and sixteen percent of robberies, with concurrent Real-Time Crime Center operations confounding statistical isolation of effects); Measuring the Cost-Effectiveness of ALPRs (2025) (methodological critique concluding that compounding deployment variables frustrate unified estimates of marginal ALPR value).

15. Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Security Policy, ver. 5.9.5 (2024), access-control and least-privilege requirements. https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/

16. National Conference of State Legislatures, "Automated License Plate Readers: State Statutes." https://www.ncsl.org/technology-and-communication/automated-license-plate-readers-state-statutes

17. Id.; supplemented for 2024-2026 enactments by Oregon S.B. 1516 (2026); Washington S.B. 6002 (2026); New Mexico S.B. 40 (2026); Kentucky H.B. 58 (2026); Connecticut S.B. 397 (2026); Virginia H.B. 2724 (2025); and the New Jersey Attorney General directive governing ALPR retention.

18. Flock Safety, "Data Retention Talking Points: An Analysis of 2024 NIBRS Clearance Data" (2026). The underlying incident and arrestee data are drawn from the FBI's National Incident-Based Reporting System via the Crime Data Explorer (https://cde.ucr.cjis.gov) and are publicly available for independent verification. Figures reflect mean time from offense to first arrest for cleared Group A offenses; because they measure when cases are cleared rather than the specific contribution of ALPR data to any clearance, they establish that investigations remain active well beyond short retention windows, not that ALPR data was decisive in closing a given case to arrest.

19. Schmidt v. City of Norfolk (E.D. Va. Jan. 27, 2026) (granting summary judgment for the city; a fixed-camera ALPR network with a 21-day retention period and limited coverage did not capture enough of a person's movements to constitute a search under Carpenter), appeal pending, No. 26-1227 (4th Cir.); State v. Simonson (Wash. Ct. App. Jan. 29, 2026) (an ALPR image of a plate on a public roadway is a momentary observation of what is already exposed to public view; rejecting analogies to GPS tracking and cell-site location records).