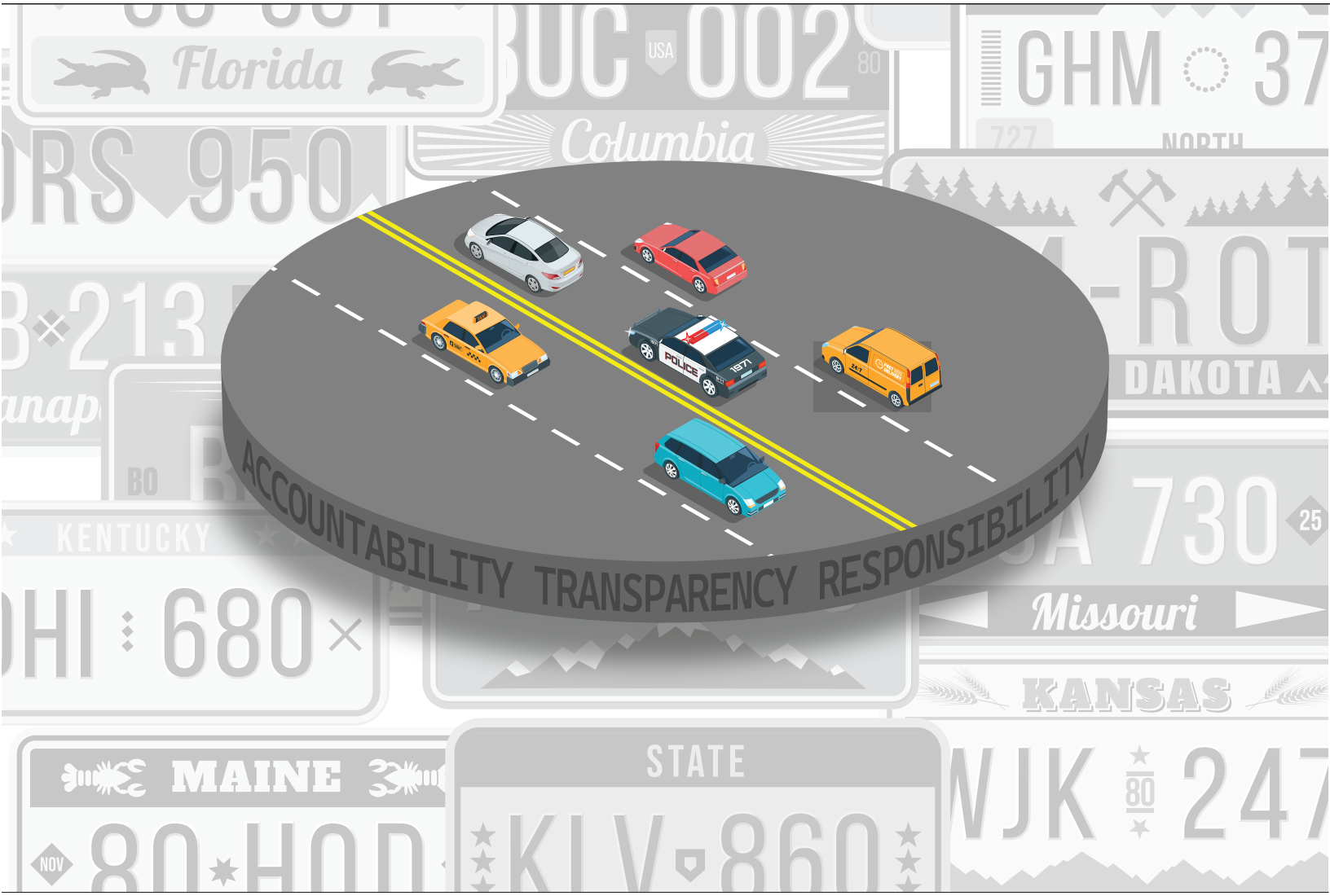
MAJOR CITIES CHIEFS ASSOCIATION

Automated License Plate Reader Technology in Law Enforcement

RECOMMENDATIONS AND CONSIDERATIONS



PRESENTED BY MCCA ALPR WORKING GROUP

Table of Contents

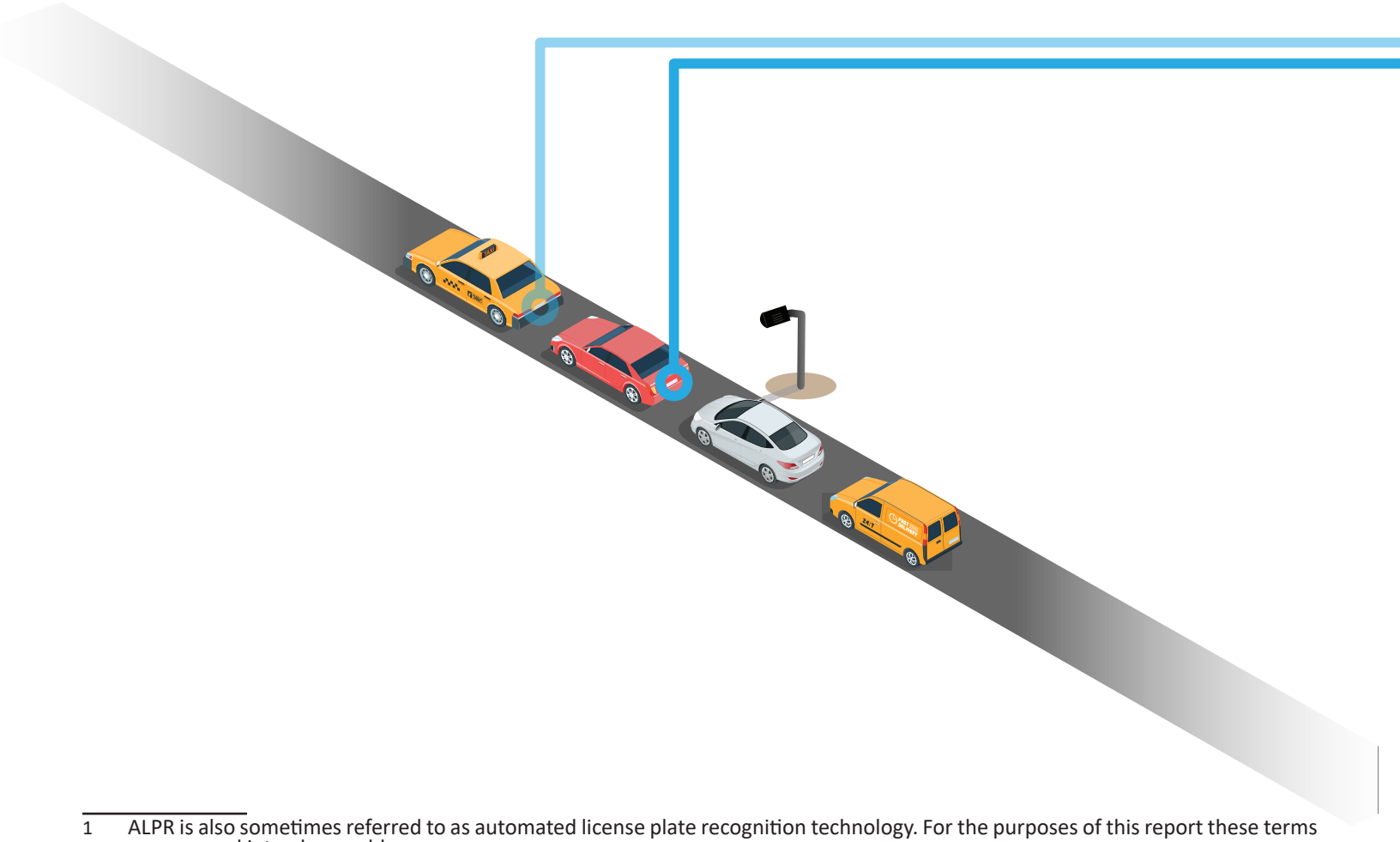
Introduction

Modern-day law enforcement relies on advanced technologies to enhance investigative capabilities. One example of these technologies is automated license plate reader (ALPR).[1] ALPR has been used for decades by law enforcement agencies throughout the United States, Canada, and across the globe to help generate leads and close cases. Law enforcement agencies that utilize ALPR continuously report that the technology is a critical tool that helps advance their efforts to fulfill law enforcement's ultimate mission of keeping our communities safe.

ALPR is a proven technology, but all law enforcement tools must be used ethically and appropriately. This product is designed to assist law enforcement agencies with developing and maintaining an ALPR program that respects citizens' Constitutional rights and privacy while maintaining ALPR's effectiveness as a tool to address crime.

In October 2022, the Major Cities Chiefs Association (MCCA) established an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts in the ALPR field to achieve this goal. The Working Group has created a set of best practices related to procurement, development, operation, data collection and reporting, and other elements instrumental in creating a well-balanced ALPR program. Like any other technology, ALPR will continue to evolve.

The product is a true public-private partnership, and the framework outlined in it will help law enforcement agencies seeking to utilize ALPR achieve the highest possible standards. However, it is essential to remember that every community is different, and what works in one community may not work in another. Therefore, while the Working Group's recommendations provide a strong foundation, agencies are encouraged to tailor them to meet the specific needs of their community as they develop, implement, and manage their ALPR program.



1 ALPR is also sometimes referred to as automated license plate recognition technology. For the purposes of this report these terms are used interchangeably.

Executive Summary

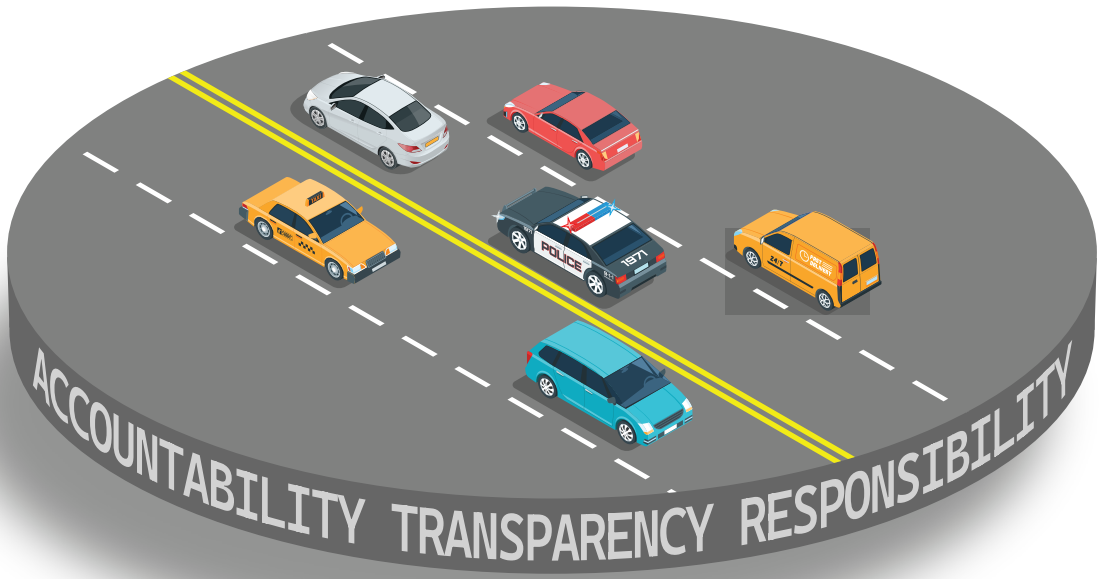
In October 2022, the Major Cities Chiefs Association (MCCA) launched an ALPR Working Group composed of trusted technology partners, law enforcement agency stakeholders, and subject matter experts. The Working Group has developed a product that is designed to provide MCCA members and other law enforcement agencies with guidance on developing, deploying, and responsibly using ALPR technology. ALPR technology has proven to be a powerful tool to combat criminal activity, generate actionable investigative leads, and help close cases faster.

This product directly addresses the most critical aspects of ALPR technology, which can be subdivided into three main categories: accountability, responsbility, and transparency. The product outlines suggestions on ALPR program design, policy development, training considerations, and deployment strategies. The product also covers ALPR procurement. Finally, it addresses the ongoing management and oversight of the technology and provides an overview of relevant case law. While these suggestions and recommendations address the most critical aspects of ALPR, they leave sufficient room for agencies to develop programs that meet their specific needs.

Stakeholders concerned about ALPR typically focus on disparity of impact, infringement of privacy, and the effects on individual rights. However, the Working Group strongly believes these concerns can be sufficiently addressed and mitigated through thoughtful policy design, effective management, and proper oversight. Furthermore, it is important to note that recent case law differentiates the capabilities ALPR provides from those of other law enforcement technologies.

The guidance outlined in this product serves as a template for building and operating an ALPR program that is both effective in its use and responsible in its nature. By implementing the Working Group's suggestions and recommendations, law enforcement agencies can ensure their ALPR programs are helping to keep communities safe while protecting citizens' privacy, civil liberties, and Constitutional rights. In addition, this can help increase public trust and build support for using ALPR technology.

Finally, like all technology, ALPR will continue to change and evolve. For this reason, this product should be considered a living document rather than a finalized template for developing and implementing a balanced and responsible ALPR program. As the conversation surrounding ALPR progresses, so will the recommendations and suggestions included in this product.



Key Recommendations

The following key recommendations serve to highlight the MCCA ALPR Working Group's most essential recommendations and considerations. They have been grouped by their applicability to three foundational principles regarding the deployment of advanced technologies in law enforcement.

ACCOUNTABILITY

- Agencies should develop a training program that establishes accountability guidelines, procedures for responsible use, and emphasizes transparency. The use of ALPR technology should be limited to trained personnel.
- The use of ALPR technology should be limited to criminal investigations or to address an articulable public safety concern.
- The procedures for the use of ALPR technology should emphasize the need to confirm the accuracy of the information presented prior to taking enforcement action.
- Careful consideration should be given to the data retention policies implemented by the agency. Data retention time frames should be developed by balancing community needs, benefits, and concerns.
- Audits of ALPR programs should be conducted regularly. Audits should monitor user activity to ensure appropriate use in accordance with established policies.

RESPONSIBILITY

- Sharing ALPR data among law enforcement agencies can enhance the effectiveness of ALPR deployments. A clear policy should be established prior to enabling data sharing to address data usage and deconfliction requirements.
- Deployment strategies should be reviewed regularly and evaluated to ensure the ALPR program and technology continues to operate within the established objectives and policies.
- Law enforcement agencies seeking to procure ALPR technology should consult with other agencies that have deployed ALPR during program development.
- Prior to the deployment of ALPR technology, agencies should assess existing technological deployments and consider how they can complement or enhance their specific program strategy.
- Law enforcement agencies must implement strict cybersecurity protections to prevent unauthorized access of ALPR data.

TRANSPARENCY

- Deployment plans should be informed by analyzing crime data, patterns, and trends to ensure the technology is deployed in an equitable and responsible manner.
- Agencies should consult with their local public works and other relevant stakeholders to ensure the ALPR deployment plan meets all permitting, legal, and other requirements.
- Comprehensive data collection and reporting will help maximize the benefits of ALPR technology by increasing transparency and empowering agencies to determine its impact on crime and public safety.

Methodology of Product

This product represents the comprehensive collection of the MCCA ALPR Working Group's recommendations and considerations regarding law enforcement's use of ALPR technology. The value of ALPR as a crime-fighting tool is well established. However, an effective program must include certain elements to ensure the technology is being used effectively and in a manner that maintains the trust and support of the community. This document will provide law enforcement agencies with a framework to develop, implement, and manage an ALPR program that is based on responsible use, helps keep the community safe, and respects privacy, civil rights, and civil liberties.

The MCCA ALPR Working Group includes technology vendors from various backgrounds, a diverse group of law enforcement professionals, and ALPR subject matter experts. In addition, the Working Group conducted in-depth research on ALPR technology from numerous perspectives. Finally, the Working Group leveraged the expertise of the individual participants to develop its recommendations and suggested best practices.

The information and data used to support the findings of this product include material provided by MCCA member agencies and technology vendors. The Working Group also reviewed products produced by other stakeholders on ALPR and the use of technology in policing more generally. Finally, the Working Group conducted regular internal discussions to finalize the recommendations and suggested best practices.

This product's outline and overarching topics were created collaboratively with input from all Working Group participants. Each participant was responsible for drafting a section of the report, and those drafts were circulated to the entire Working Group for review. All Working Group members approved the final product.

The final product represents the MCCA ALPR Working Group's findings, recommendations, and suggested best practices. These will help law enforcement agencies create, manage, and operate an effective and responsible ALPR program.

What is an Automated License Plate Reader?

ALPR, called Automated Number Plate Recognition (ANPR) in Europe, was invented in 1976 by the Police Scientific Development Branch to combat terrorism in the United Kingdom. While seen as a valuable tool, the associated cost and requisite experience stagnated the deployment and advancement of the technology until the first ALPR cameras were installed at the Dartford Tunnel and A1 Road in 1981. The Dartford Tunnel cameras resulted in ALPR's first arrest for a stolen vehicle. This slowly led to more widespread use of the technology, including as part of the "ring of steel" created around London in the early 1990s to protect against the Irish Republican Army (IRA) bombing campaigns. Later, ALPR technology was also deployed as part of another initiative entitled "Project Laser," which sought to "target criminals through their use of roads."[1]

The success of the "ring of steel" and "Project Laser" prompted the Police Standards Unit to create the National ANPR Data Centre (NADC) in 1997. The NADC allowed for the nationwide sharing of ALPR data across the United Kingdom and the Back Office Facility (BOF), the database where ALPR data was stored and analyzed. ALPR technology took off from here. Law enforcement first used ALPR to help solve a murder case in 2005, and by 2007, nearly half of all law enforcement agencies in the UK were using ALPR technology. American law enforcement agencies followed their British counterparts closely and started using ALPR in 1998.[2]

ALPR Hardware and Software

While the technology has advanced over the years, the main components of those early ALPR deployments and today's systems remain the same. At its core, an ALPR program consists of the camera hardware and the software used to store and analyze the generated data and alert the users when a detection of interest is made. In most cases, ALPR hardware consists of a camera, processor, power supply, and data transfer hardware. In addition, ALPR cameras are typically optimized in various ways to operate in a wide range of real-world conditions (low light, inclement weather, motion detection, etc.).

Once the camera captures the image, ALPR systems use software to read the license plate. Some systems process the image at the camera level. Other systems transfer (usually via a cellular network, but it may occur through other means) data from the camera to a dedicated ALPR-system computer for processing. The image is analyzed through Optical Character Recognition (OCR) software as part of the processing. OCR recognizes alpha-numeric numbers and letters, thereby allowing the ALPR system to successfully recognize and interpret any letters or numbers observed in the image captured by the camera.

Types of ALPR

Law enforcement uses various types of ALPR technology, including fixed, mobile, portable, and mobile applications. Below is a description of each kind of ALPR system:

- **Fixed ALPR** cameras are typically permanently mounted to infrastructure such as traffic signals, bridges, and light poles.
- **Mobile ALPR** cameras are typically mounted on vehicles. These cameras may be overtly or covertly deployed depending on the needs of the law enforcement agency.
- **Portable ALPR** cameras include mobile camera trailers which can be transported and deployed based on the law enforcement agency's operational needs.
- **Mobile Applications** leverage features built into cellular devices to create ALPR detections.

1 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

2 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

The ALPR Detection Record

An ALPR record is generated when a vehicle license plate is detected, imaged, and processed to create a record. An individual ALPR record (or 'plate read') is generally composed of the following:

- An image of the license plate, which is a 'cropped' digital image of the license plate captured by the camera.
- The geo-location where the plate detection occurred, which can be determined from the GPS coordinates of a mobile reader or inferred from the location where fixed readers are placed.
- The time and date when the license plate detection occurred.
- The translated information from the plate, which is the alpha-numeric plate number and the issuing organization, typically a state. This translation can be accomplished by OCR or artificial intelligence.

In addition, an ALPR record may contain the following:

- A collateral image of the vehicle for which the ALPR read occurred.
- Metadata associated with the camera that identifies the camera unit, image settings, and other specific attributes.

Hotlist Sources

ALPR systems used by law enforcement can alert on detections of wanted vehicles. Two primary methods exist for creating a wanted vehicle within an ALPR system. First, ALPR systems allow for the manual entry of both a hotplate and a hotlist. Second, the ALPR system allows agencies to import National Crime Information Center (NCIC) records as an automated hotplate source. This is the most common method for populating hotlists.

Tactical vs. Investigative Uses

Law enforcement typically uses ALPR technology for both tactical and investigative purposes. Accordingly, agencies should consider both uses when developing their ALPR program's objectives. A tactical ALPR deployment includes placing cameras in strategically identified locations to generate information that warrants a rapid police response, such as stopping a wanted vehicle. These deployments usually seek to identify, locate, and recover a vehicle or its occupants to help address crime occurring in real time. An investigative use refers to utilizing ALPR cameras to collect license plate records that may have law enforcement interest but do not necessarily warrant an immediate police response. These detections are stored in the system and may later be queried. This information is generally used to create an investigative lead after a crime has occurred.

Business/Private Use

Since ALPR systems provide valuable data, private businesses and other organizations have also invested in ALPR technology. These uses may be for security, management, or operational needs. The following are examples of private sector use cases:

- Parking garages
- Hotels and casinos
- Homeowners associations
- Airports
- Convention centers
- Government traffic and transportation sites

Program Design and Development

ALPR has proven to be a successful law enforcement tool. Its unique ability to provide actionable leads and help close cases cannot be overstated. However, real and perceived concerns exist regarding this technology's use. Therefore, law enforcement must take careful steps to develop an ALPR program that is both effective and appropriate. Taking a thoughtful approach when designing and developing these programs is the best strategy to accomplish these goals. Some of these considerations include developing proper policies, creating comprehensive training material, and designing and implementing responsible deployment strategies.

Policy Development

Establishing clearly defined policies on how ALPR may be used is the most effective method to minimize risk to the agency and protect both department employees and the individual rights of the public. ALPR policy should direct the purpose, general use, and processes involving ALPR investigations. These policies will provide a framework by which an agency can simultaneously reap the benefits of the technology, all while respecting the privacy and civil rights of the public. Similarly, consistent policies will assist in protecting the integrity of criminal investigations, criminal intelligence collection, and justice system processes. The following components should be considered while developing ALPR policies and procedures:

- Community-directed statement on why the agency is establishing or maintaining an ALPR capability
- The purpose of the policy
- General use guidelines of the technology
- Clearly defined program oversight roles and responsibilities
- The ALPR vendor and deployment types
- Access, training, and usage requirements
- Investigative procedure requirements
- Clear guidance to department employees on being transparent on the use and reporting of the technology in court documents
- Auditing responsibilities and schedule
- Data retention and purging
- Statement affirming protections for constitutionally protected activities
- Rules governing the use of hotplates

State/Local Law Considerations

Many state legislatures have taken steps to regulate the use of ALPR technology in their states. These laws and regulations can directly impact the functioning of an ALPR program in those states, and they must be accounted for in agency policy. Examples of the types of rules and regulations implemented in several states can be found in Appendix C – State-Level Laws and Regulations.

Training Considerations

Ensuring a thorough training program is in place is critical. Users must receive training on the ALPR system before receiving access. This practice ensures ALPR systems are only used for official law enforcement purposes consistent with applicable legal limitations and department policy. The training program should address several topics to ensure that users of an ALPR system are proficient in the necessary skills, including:

- A review of the departmental policy and safeguards related to ALPR use
- Basic understanding of how the technology operates
- The ALPR data sources, vendor, type of systems, etc.
- Any significant capabilities and or limitations related to the technology
- Any potential hazards related to the technology

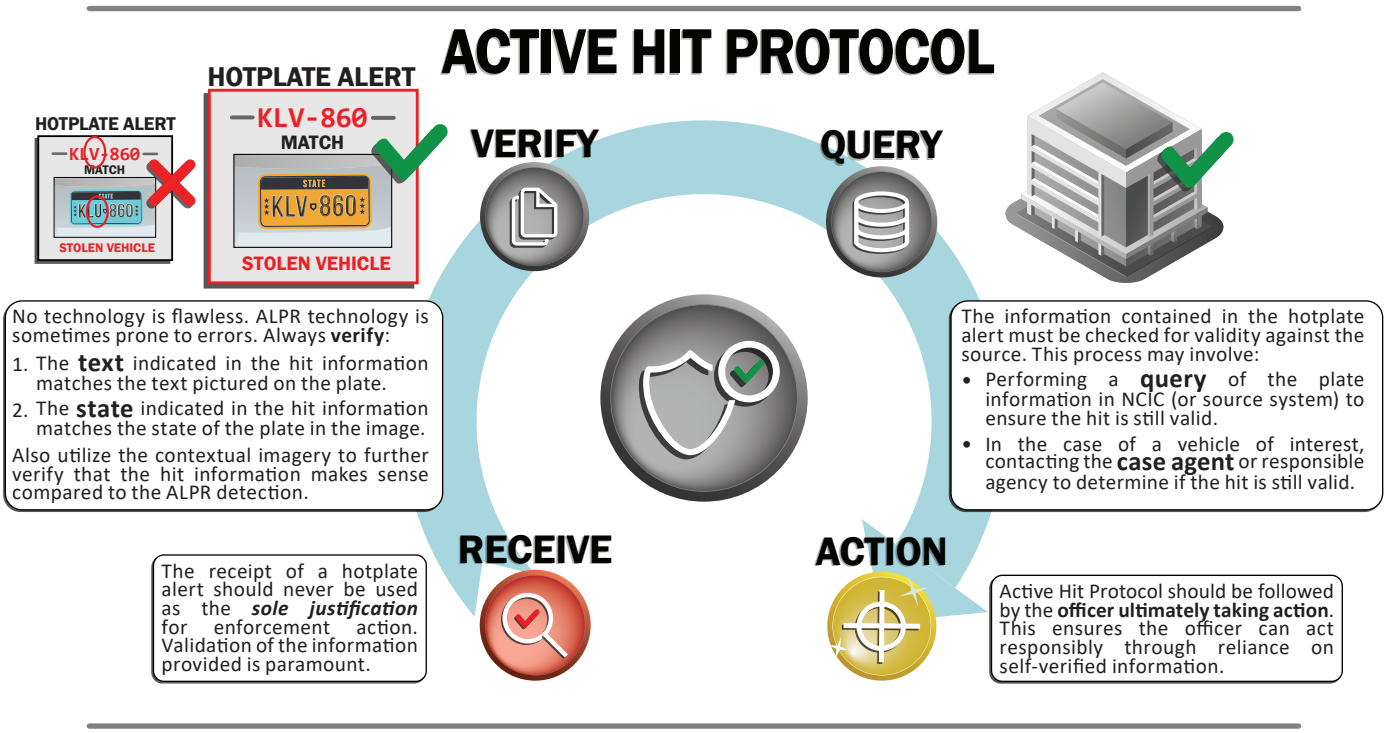
- Who is authorized to access the system and any required training
- The role of the officer or investigator in leveraging and responding to ALPR hotplate detections
- Importance of being transparent with arresting documentation
- Any applicable laws and policies that govern the use of ALPR in the specific jurisdiction
- Use of the ALPR system as an investigative tool
- The data retention period
- Auditing responsibilities

An ALPR training program should include a tactical-level discussion of how to use the technology appropriately. For mobile units, this should consist of an initial check to ensure that the ALPR system is operating correctly at the beginning of each shift. This includes logging into the system, running any necessary diagnostics to determine that it is working correctly, and doing a quick physical inspection of the system (cameras, cables, connections). In addition, a program manager should conduct periodic checks of fixed ALPR sites to verify that the hardware is operational and communicating with the software as intended.

Field Officer Responsibilities

A critical piece of the officer training on ALPR should include an element that instructs how ALPR notifications are processed and the appropriate response protocols for those notifications. Some departments may have fixed ALPR hits reviewed and confirmed by the public safety answering point or real-time crime center before dispatching them to an officer to investigate. Other systems may provide an in-car alert on the car computer system.

Officers should be required to review hotplate detection, confirm the detections, and appropriately respond to actively wanted vehicles. This process can be referred to as “Active Hit Protocol.”



Investigator Responsibilities

The ALPR system is a valuable investigative tool. It can be used to develop leads in cases involving vehicles where the license plate is unknown or to establish that a car was not in the vicinity during the time frame a crime occurred. An ALPR training program must include how to access the system and the criteria required before conducting a query, such as the reason for the search and the associated case number. Additionally, investigative tool training should address how to query the system, instructions on operating the various analytical tools within the system, how to interpret the data, how to preserve a record, and any required transparency, audit, or reporting requirements.

Types of Training

Training should be broken down into multiple categories:

- **New User Training:** This training will be detailed and define proper usage. In addition, this training should include policy, procedures, state and local laws, and an in-depth walk-through of the ALPR products and software.
- **Refresher Training:** This is considered a refresher of policy and procedures. It may also include changes to case law and examples of ALPR use. This training should ideally occur immediately after any changes to policy take place.

Authorized instructors should provide training on ALPR technology based on an established, accredited curriculum. An example of an accredited curriculum is one that has been approved by the state's Peace Officer's Standards and Training (POST) or equivalent body.

Deployment Strategies

Determining the ALPR deployment type and kind is one of the most critical decisions an agency will make concerning its ALPR program. Law enforcement is responsible for deploying advanced technology in a manner that is effective in its use and appropriate in its scope. Law enforcement also has a fiduciary duty to use public funds responsibly. For these reasons, ample consideration should be made when determining the type and kind of ALPR deployment.

ALPR Deployment Theories

As previously addressed, various types of ALPR technology exist, including fixed, mobile, portable, and smartphone applications, with each serving a unique purpose. Therefore, the kind of ALPR selected should be determined by the environment, infrastructure, and objectives for the ALPR deployment. Several ALPR deployment strategies are often considered when determining the value and placement of ALPR cameras. The most common of these strategies include the following:

- **High Traffic Areas:** The primary objective is to collect the maximum number of detections that can later be leveraged for investigative leads.
- **High Crime Areas:** This strategy focuses on producing information anticipated to be of investigative value instead of creating as many detections as possible.
- **Places of Interest:** This strategy is more of a hybrid between the first two. An example of this strategy would be deploying ALPR cameras around a shopping mall targeted by organized retail theft gangs or where assaults have occurred. Agencies may also place ALPR cameras in proximity to their community's major ingress/egress points and critical infrastructure or routes associated with gun, drug, or human trafficking.

Deployment Considerations

Infrastructure and permitting are two common factors that can limit an agency's deployment strategy for ALPR systems. Agencies must carefully consider each physical deployment site. The infrastructure to mount the necessary hardware must exist for the technology to be successfully deployed. Furthermore, the owner and operator of the infrastructure or property must allow for the installation of ALPR hardware. Agencies must also ensure that the proposed site is appropriate for the type of power the ALPR utilizes. Some systems run on AC power. While this provides constant and consistent power, installing it can be more expensive. Others rely on solar energy, which may only provide enough power if the camera site receives sufficient sunlight to account for the traffic volume. Finally, this infrastructure must have access to a data transmission service, such as cellular, fiber optic, or Wi-Fi.

Once a deployment plan has been established, site locations have been determined, and in-person inspections of the sites have been completed, the agency will need to navigate any legal and permitting processes. Since permitting can vary significantly across jurisdictions, it is recommended that agencies consult with their local public works or other appropriate governmental entities to ensure all necessary procedures are being met. Engaging these entities earlier in the process will help secure their buy-in, which will be critical for a successful deployment.

Equitability Concerns

Deployment strategies must account for concerns over bias, surveillance or other threats to privacy, and potential chilling effects on First Amendment, defendant, or related rights. The following recommendations will help ensure ALPR technology is deployed in a manner that supports just and equitable policing:

- Deployment plans should be informed by analyzing crime data, patterns, and trends. The site selection process should be based on this information and account for any relevant privacy, equitability, or other concerns.
- Agencies should consult the community, other stakeholders, and appropriate oversight committees. This includes providing specific information on why and how the deployment sites were selected.
- Deployment strategies should regularly be reviewed and evaluated to ensure the ALPR program and technology continue s to operate within the established guidelines and policies.

Partner Technologies

While developing the deployment plan, it is important to consider other law enforcement technologies that may complement the ALPR system. Law enforcement agencies may deploy complementary technologies within the same area, which have different capabilities. Agencies can leverage these capabilities to increase their ability to suppress crime, create actionable leads, solve cases, and potentially deter future crimes. Potential partner technologies can be subdivided into two categories: tactical and investigative.

Tactical technologies include tools such as gunshot detection technology, public safety cameras, and drone detection technology. An example of investigative technology is a records management system (RMS). Integrating ALPR and RMS can join plate reads to hotlists, allow investigators to search plate reads within a familiar interface, and provide a direct link between case management and the ALPR database. Another example of investigative technology is crime analysis software. Bringing ALPR data into an agency's chosen analysis software can aid in ongoing investigations. For example, agencies can import ALPR data to help create accurate timelines for vehicle travel that can provide investigators with unseen leads and valuable knowledge.

Procurement

Responsible procurement of ALPR technology is a critical component of an effective program. The importance of obtaining stakeholder feedback early in the procurement process cannot be understated. Program managers should make every effort to embrace a spirit of transparency, accept critical feedback, and attempt to address any concerns raised by stakeholders directly.

The procurement phase is also the appropriate time to begin building departmental policies, procedures, and protocols, as this will be crucial in gaining stakeholder buy-in. It is imperative that the stakeholders understand how these policies will protect the public's privacy and civil liberties. Agencies should also seek to mitigate any concerns that stakeholders raise about the proposed ALPR program through thoughtful policy design.

Vendor and Product Assessment

Before choosing a vendor for their ALPR program, law enforcement agencies should conduct an appropriate degree of market research. This should include a trial of the product and conversations with existing customers to evaluate its performance in a real-world setting. A trial period provides the opportunity to test the technology, the associated policies and procedures, and highlight initial successes. This can provide tangible examples that can be shared with stakeholders to show how ALPR serves to enhance public safety.

Should an agency engage in a pilot program, it is recommended that the community be notified. Agencies should also determine how any information collected may be used in investigations or other law enforcement operations until a final protocol and all other areas of the program are formalized.

When determining the best hardware for their ALPR program, law enforcement agencies should consider the following:

- Hardware requirements for specific sites
- The lenses, processor, and other technical specifications of the hardware
- Average detections per hour
- General cost
- The number of lanes of traffic a single camera can capture
- The maximum speed at which the camera can read a license plate

When determining the best software for their ALPR program, law enforcement agencies should consider the following:

- The accuracy of the OCR software and whether it's enhanced by artificial intelligence, machine learning, or another capability
- The technology's alerting system, including desktop, laptop, mobile, app-based, and in-car alerts
- The software's ability to connect and share data with other law enforcement analytical platforms

Technical Challenges

There are some challenges with ALPR software that agencies must acknowledge. For example, OCR technology analyzes all letter or number sequences in the imagery; it cannot specifically isolate only license plate images. Therefore, a detection can be created on something that is not a license plate. This includes billboards, signage, marketing material on vehicles, etc. Additionally, the full license plate letter and number sequence must be visible to create an accurate license plate detection. Occlusion, missing plates, and temporary paper plates may result in no detection, a partial detection, or a misread.

Misreads may occur for several reasons, but most are due to the incorrect translation of a letter or number. For example, the system may read an "8" as a "B" or a "K" as an "X." These technical challenges should be readily acknowledged by both the agency and a prospective ALPR vendor. Agencies must ensure their policies account for these challenges and contain sufficient safeguards to limit instances where officers act based on a misread or other error.

Procurement Ethics

While local procurement ordinances vary across jurisdictions, agencies must follow those ordinances along with broader guiding principles when procuring an ALPR platform. The National Institute of Governmental Purchasing's (NIGP) Values and Guiding Principles of Public Procurement are one such set of broad principles that agencies can use to inform any ALPR procurement process. The NIGP principles are as follows:

- **Accountability:** Taking ownership and being responsible to all stakeholders for our actions. This value is essential to preserve public trust and protect the public interest.
- **Ethics:** Doing the right thing. This value is essential to deserve the public's trust.
- **Impartiality:** Unbiased decision-making and actions. This value is essential to ensure fairness for the public good.
- **Professionalism:** Upholding high standards of job performance and ethical behavior. This value is essential to balance diverse public interests.
- **Service:** Obligation to assist stakeholders. This value is essential to support the public good.
- **Transparency:** Easily accessible and understandable policies and processes. This value is essential to demonstrate the responsible use of public funds.[3]

3 Additional information on NIGP's Guiding Principles can be found here: https://www.nigp.org/our-profession/values-and-guiding-principles-of-public-procurement

Program Management and Oversight

An ALPR program's design and operational management are part of the framework of a successful program. Effective management and oversight of the program help ensure operational transparency and accountability and that ALPR technology is being used responsibly.

To ensure the program operates responsibly, agencies should assign a manager operational control of the ALPR program. This individual should be well versed in the technology, have a sound understanding of all significant components of the ALPR program, and be empowered to ensure the program follows protocols, policy, applicable law, and community and agency expectations.

A program manager's responsibilities include the following:

- Developing policies
- Overseeing training
- Ensuring appropriate use of the technology
- Managing data collection and reporting

A program manager is also responsible for staying current on technology changes and emerging ALPR trends. Similarly, they must ensure that their agency's ALPR policies and training are current and address technological changes or advancements. Finally, having a program manager establishes a clear point of contact between the law enforcement agency and the ALPR vendor. This can enhance the communication between the agency and vendor, which creates an opportunity to share and address any technological or other challenges.

Access and Appropriate Use

Law enforcement agencies are responsible for using ALPR data to uphold public safety, solve crimes, and prevent future crimes. Agencies have an opportunity to build public trust and support for the use of ALPR through transparency and responsible use. As such, agencies should carefully consider the circumstances under which using ALPR is appropriate and what personnel within the agency can access this tool.

Law enforcement agencies must scope their ALPR programs in a manner that ensures the agency is still able to conduct proper oversight and operate the program transparently. One method for achieving this is by limiting who can access the ALPR technology. For example, many law enforcement agencies restrict access to specialized personnel to ensure that the use of ALPR technology is adequately audited and controlled. Access should only be authorized once a user has completed the requisite training and demonstrates a baseline understanding and operational knowledge of the technology. Information on new user training, access, and use should be part of standard data collection and reporting related to the ALPR program.

Agencies that deploy ALPR must have written policies that outline the appropriate use of the technology. Several core principles should be incorporated into these policies to ensure the responsible use of the technology. First and foremost, ALPR technology should only be used as part of a criminal investigation or to address an articulable public safety concern. Secondly, the investigator must also have a legitimate "need to know" before querying any ALPR data. These guardrails will help prevent "curiosity checks" or other bad faith uses and ensure that privacy, civil rights, and civil liberties are respected.

Agency users must also demonstrate adherence to established policies when searching archived ALPR data. For example, if the ALPR software allows it, agency policy should require users to document the investigative purpose and case number associated with each query. Vague or ambiguous reasons for a search, such as "criminal subject" or "research," should be avoided. An agency's ALPR policies should also outline the potential consequences and corrective methods for improper use of the technology. Examples may include mandatory retraining, loss of access privileges, or other appropriate corrective punishments.

Data Retention

Data retention policies are ultimately determined by the agency using ALPR technology. These policies are informed by various considerations, including the agency's objectives, stakeholders' expectations, and local laws or regulations. Therefore, it is essential that the ALPR technology, vendor, and any other relevant service providers support the agency's policies on retention.

While a general best practice is not to retain data any longer than is necessary, what constitutes "no longer than necessary" is not a simple determination since different use cases may benefit from different retention periods. For example, cold cases may benefit from years-old data, while other uses rely on more recent data.

Outside of specified legal requirements, the retention schedule for ALPR data is primarily determined by agency policy.[4] As such, law enforcement must work with the community and other stakeholders to determine appropriate retention periods for each type of ALPR data. Ideally, ALPR systems should allow agencies to define retention schedules and automatically purge any record not designated for retention by a registered user. In addition, regular system audits ensure retention standards are followed and instill confidence that system data is utilized appropriately.

Data Sharing

For good reason, law enforcement agencies worldwide are embracing ALPR technology. A 2013 Bureau of Justice Statistics study showed that 77% of agencies serving populations of 100,000 or more have access to ALPR technology.[5] Moreover, given ALPR technology's value to a single jurisdiction, law enforcement has begun to explore sharing ALPR data across jurisdictional boundaries. Sharing ALPR data amongst law enforcement agencies fosters a more collaborative approach to addressing public safety concerns across jurisdictional boundaries.

Benefits of Data Sharing

When law enforcement agencies share ALPR data across jurisdictions, the technology can provide more comprehensive data. A shared system creates more unified and robust coverage throughout a region. Several ALPR vendors currently provide their law enforcement customer base with the ability to share data with other law enforcement customers. The potential to cross-reference information between separate ALPR systems allows law enforcement to enhance their investigative capabilities and can reveal elements of illegal activity that may otherwise be unknown to the investigating agency. Several elements of ALPR data and systems can be shared, including the ALPR detections and user-created hotlists. Some ALPR vendors also allow agencies to establish data-sharing relationships between their products and other technology systems.

As a standard practice, law enforcement agencies should consider sharing ALPR data with one another to the extent that state or local laws and regulations permit. Agency policy should define what, if any, type of data sharing is in place, who is authorized to establish data-sharing relationships, and any procedures that govern the sharing of ALPR data. These procedures and data-handling agreements should be implemented in policy for both the sharing and receiving agencies.

The success of ALPR technology among law enforcement has led non-government entities to acquire the same technology. This includes retailers, property managers, towing and repossession companies, parking lot operators, homeowner associations (HOAs), and even individual households. Since the generated data is of the same format and often targets issues of mutual interest, ALPR vendors have created Public-Private Partnership (PPP) friendly user interfaces. These programs typically allow the unidirectional sharing of ALPR data from the non-government side to the law enforcement side only. These partnerships strengthen community relationships and ensure public investments are used responsibly.

4 David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, National Institute of Justice, U.S. Department of Justice, 2012. https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf

5 B.A. Reaves, Local police departments, 2013: Equipment and Technology. Bureau of Justice Statistics, U.S. Department of Justice, July 2015. https://bjs.ojp.gov/library/publications/local-police-departments-2013-equipment-and-technology

Data Sharing Considerations

While data sharing benefits agencies, safeguards are needed to protect the agency that generates and owns the data. Data sharing guidelines can be specific to the type of shared data. For instance, if agency "A" shares ALPR detection data with agency "B," there may be no requirement for a formal agreement. In contrast, if agency "A" shares hotplates or agency-generated hotlists with agency "B," this scenario may require a formal agreement. This is because hotplates or hotlists are typically generated from a criminal investigation or law enforcement process or function that may require an officer to take action if there is a confirmed detection. Furthermore, the agency that receives the information should bear the responsibility and liability for their officers' actions in response to an alert.

Law enforcement agencies seeking to share or receive ALPR data must be aware of applicable federal, state, and local laws. As such, agencies should consult with their legal representatives to identify pending, proposed, or existing laws that may be relevant. For example, legislation is proposed annually at all levels of government which, if enacted, could limit law enforcement data sharing. Finally, agencies must consider any concerns from the community or other stakeholders before establishing multi-jurisdictional data-sharing relationships.

Auditing, Data Collection, and Reporting

Auditing and reporting an agency's use of ALPR technology is a critical component of a transparent and accountable ALPR program. The failure to operate a program in this manner will only exacerbate concerns related to misuse or contribute to the perception that ALPR technology is synonymous with increased surveillance. This will undoubtedly negatively impact police-community relations. Agencies should develop robust mechanisms to evaluate the efficacy of the technology and ensure it is being used appropriately.

Auditing Requirements

Regular audits on an ALPR system are one method for validating compliance with agency policies and applicable laws and regulations. As with other reporting requirements, the specific auditing measures, and the frequency of said audits, should be clearly defined in the ALPR program's governance documents. In general, audits should verify what ALPR information was accessed and by whom, in order to identify any improper or unauthorized uses of this data. Audits should also ensure that data within the system is being handled per agency policy, including information sharing agreements. They should also confirm that data is being purged as required under any applicable data retention schedules.

Data Collection and Reporting Considerations

Studies have shown that ALPR technology is most effective when used systematically and when deployment sites are strategically selected.[6] In addition, comprehensive data collection and reporting will assist agencies with maximizing the benefits of ALPR technology. Finally, robust data collection and reporting will help increase transparency.

At a minimum, agencies using ALPR should collect and report the following information:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly attributed to ALPR hotplate detections
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

By analyzing this data, agency leaders and stakeholders can determine whether their ALPR system is meeting deployment goals and has significantly impacted crime or other areas of police operations. ALPR data collection and reporting also provide valuable insight into ALPR system adoption throughout the organization.

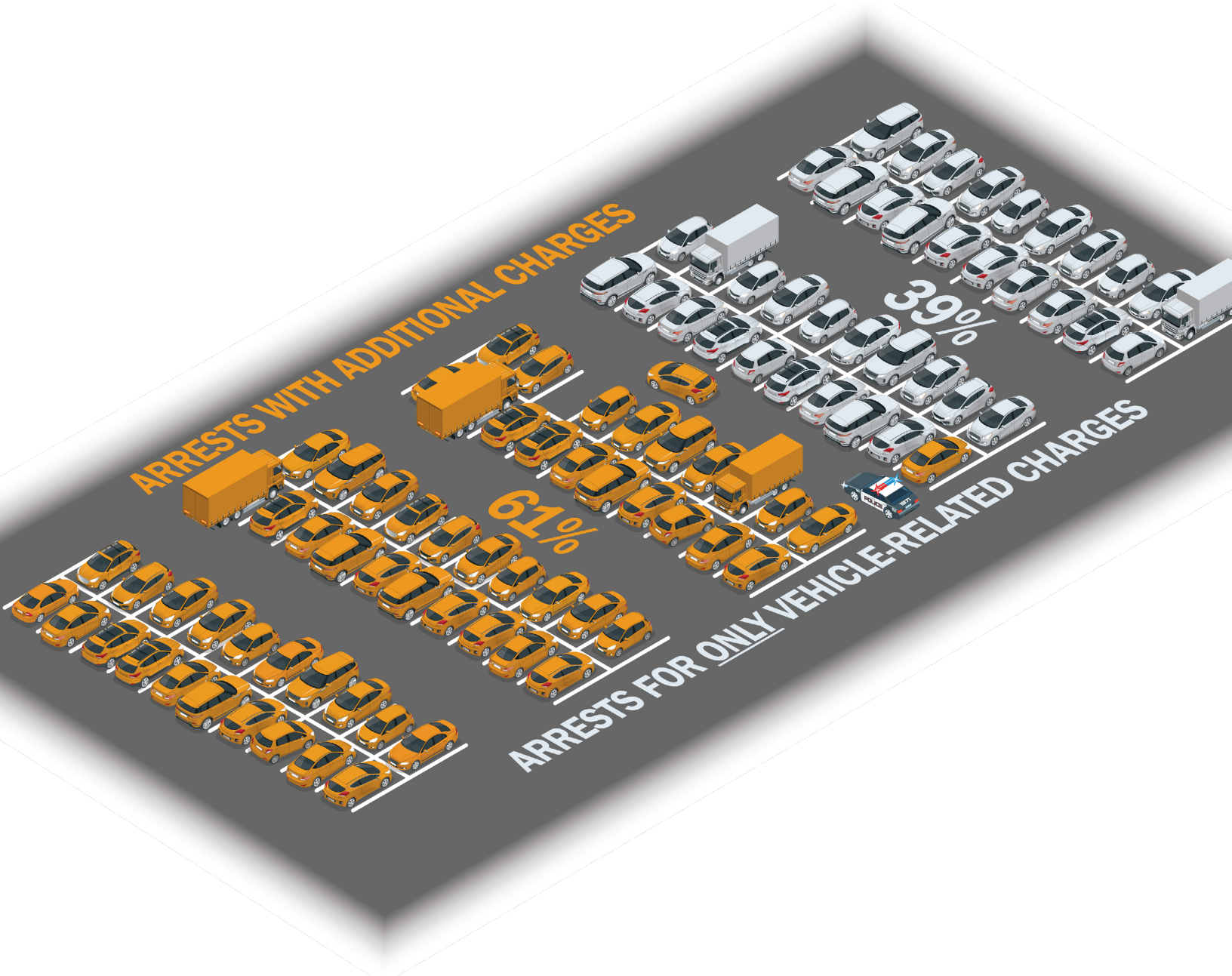
6 C. S. Koper and C. Lum, "The impacts of large-scale license plate reader deployment on criminal investigations," Police Quarterly, 22(3), 305–329, 2019. https://doi.org/10.1177/1098611119828039

The Importance of Analysis and Reporting

Quantitative data is an excellent tool to measure the impact of law enforcement technology. The ability to answer the questions “how many” and “how often” is necessary to evaluate real-world outcomes. Additionally, the quantitative analysis of ALPR data can provide an agency and stakeholders with the information needed to determine the impact of the technology on community safety.

To explore the potential of quantitative reporting, an MCCA member agency recently analyzed the impact of a localized ALPR deployment. The data presented below represents a period of four months after the installation of ALPR cameras within the evaluated area. The types of charges related to any arrests resulting from an ALPR event were analyzed. The data suggests that ALPR technology generates leads and solves more types of crimes than those related to ALPR’s most frequent use: the recovery of stolen vehicles.

It is important to capture and analyze the impact of any ALPR program to dispel misconceptions and demonstrate the impact of the technology.



Data Stewardship

Throughout the design of an ALPR program, the hardware, software, and policies implemented will shape how ALPR data is collected and stored. Therefore, a comprehensive strategy should be developed to ensure all data collection aspects are secured and managed effectively.

Data Roles and Responsibilities

ALPR records are typically stored in databases that can be indexed, searched by individual or composite conditions, and analytically processed by applications that power ALPR use cases. This is an important and powerful compilation of data that must be managed judiciously. The two primary roles relative to this data are data owners and service providers.

The data owner is the organization that controls the data and decision-making authority. The data owner, typically the data's generator and user, determines how the data may be used, who it can be shared with, and its retention limits. For example, law enforcement is always the data owner for the ALPR data it generates. While this data may be shared with other law enforcement entities, the owner and provider of any particular data always retains control over all aspects of it. Therefore, other organizations that have received access to that data must act in accordance with the data owner's direction, such as adhering to retention limits established by the owner on the data.

A service provider is an entity that may take possession of data to store or process it on behalf of the data owner. The service provider operates at the behest of the data owner and enacts the owner's wishes and directions. This can include management of data sharing with other designated users, enforcing retention limits, etc. The service provider has no entitlement to the data and may not sell, derive secondary insights, or otherwise share it. Furthermore, they may only access the data to perform a function at the direction of the data owner. Law enforcement agencies often hire an outside company to be their service provider for ALPR data.

Storing and Processing ALPR Data

There are several general models for storing and processing ALPR data:

- The data is stored on-premises and processed by applications under the direct physical control of the organization that generates and uses the data.
- The data is stored off-premises by a cloud service provider and processed by applications in the cloud or on-premises under the direct control of the organization that generates and uses the data.
- The data is stored in the cloud or at an off site data center and is processed by a service provider.

In the first model, the data owner is effectively their own service provider, and there isn't necessarily a third party service-providing entity. The other two models imply some degree of a third party service provider. In those cases, the data may be held or accessed by another entity on behalf of the data owner. For ALPR systems, this could be either a cloud computing service or an ALPR technology vendor. However, in both cases, control of the data remains with the data owner.

Data Security

Law enforcement agencies should treat ALPR data like any other sensitive data it collects, uses, and manages. It should be protected as judiciously as law enforcement records, video, and other critical operational data. This includes ensuring responsible usage of the data by law enforcement personnel and vetting any service providers that may process the data. Law enforcement agencies must also apply rigorous cybersecurity practices to protect and secure the ALPR data it generates and uses. This includes, but is not limited to, proper authentication methods (multi-factor authentication is generally considered a best practice), data-sharing controls, and role-based access controls for users. Law enforcement agencies must ensure that their technology vendors provide adequate security practices to protect the ALPR data they possess and process on behalf of the agency.

Whether a service provider provides on-premise technology, stores data on behalf of a law enforcement agency, or hosts the processing applications, they have an important role in ensuring the secure and trustworthy operation of an ALPR program. The service provider is responsible for securing the data it processes to protect it from unauthorized access, theft, or misuse. They must provide the necessary capabilities, controls, and training to enable law enforcement agencies to enforce their own defined data governance policies, security standards, and procedures. This includes:

- **Enforcement of Retention Limits:** This may be applied absolutely or in a role-based fashion. For example, the absolute retention limit for ALPR data could be three years, but only cold case investigators may access data older than six months.
- **Positive Controls Over How Data is Shared:** Data must only be shared after law enforcement specifically enables it with individual partners at its discretion and under the auspices of its policies.
- **Enforcement of Personnel Controls:** These controls include system and user-level authorization, role-based access controls, and regular audits.

The FBI's Criminal Justice Information Services (CJIS) Security Policy provides a comprehensive reference and standard that agencies may use to design or measure data management for their program. For cases where service providers take possession of ALPR data from law enforcement agencies to store and process on their behalf, agencies should consider using the CJIS Security Policy to assess and set expectations of service providers.[7] An explanation of relevant sections of the CJIS Security Policy can be found in Appendix D – CJIS Security Policy.

As mentioned earlier, cloud services may be part of an agency's ALPR program. These services' security and integrity depend on the efficacy of the underlying cloud platform. Cloud service providers (or service providers that operate their own data center directly) should comply with ISO 9001:2015, an internationally recognized standard for Quality Management Systems. Compliance with this standard should be independently audited and verified for compliance under the Statement of Auditing Standards Number 70 [SOC 2 Report]. In addition, compliance with FedRAMP medium security controls provides an additional level of validation and may be required for information sharing with federal entities. Even though license plate detection records are not personally identifiable, they may be linked through other sources that may enable the end user to input data that could be viewed as personally identifiable or criminal justice information.

ALPR Reader Device Integrity

An ALPR reader that captures ALPR images and does local image processing contains instances of ALPR data. This data may be transient or stored on the device for extended periods. Since ALPR readers are often distributed in the environment and may be difficult to physically secure, it is increasingly important to consider the device's ability to locally secure ALPR data that is either at rest or in motion. FIPS (Federal Information Processing Standards) 140 standards are used to evaluate the hardware and software integrity of cryptographic modules. This applies to many devices, including ALPR readers, that need to encrypt data to secure it from compromise. FIPS 140-2 is broken into four, successively increasing levels of security.[8]

- FIPS 140-2 Level 1 is the lowest and imposes limited requirements.
- FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to the sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.

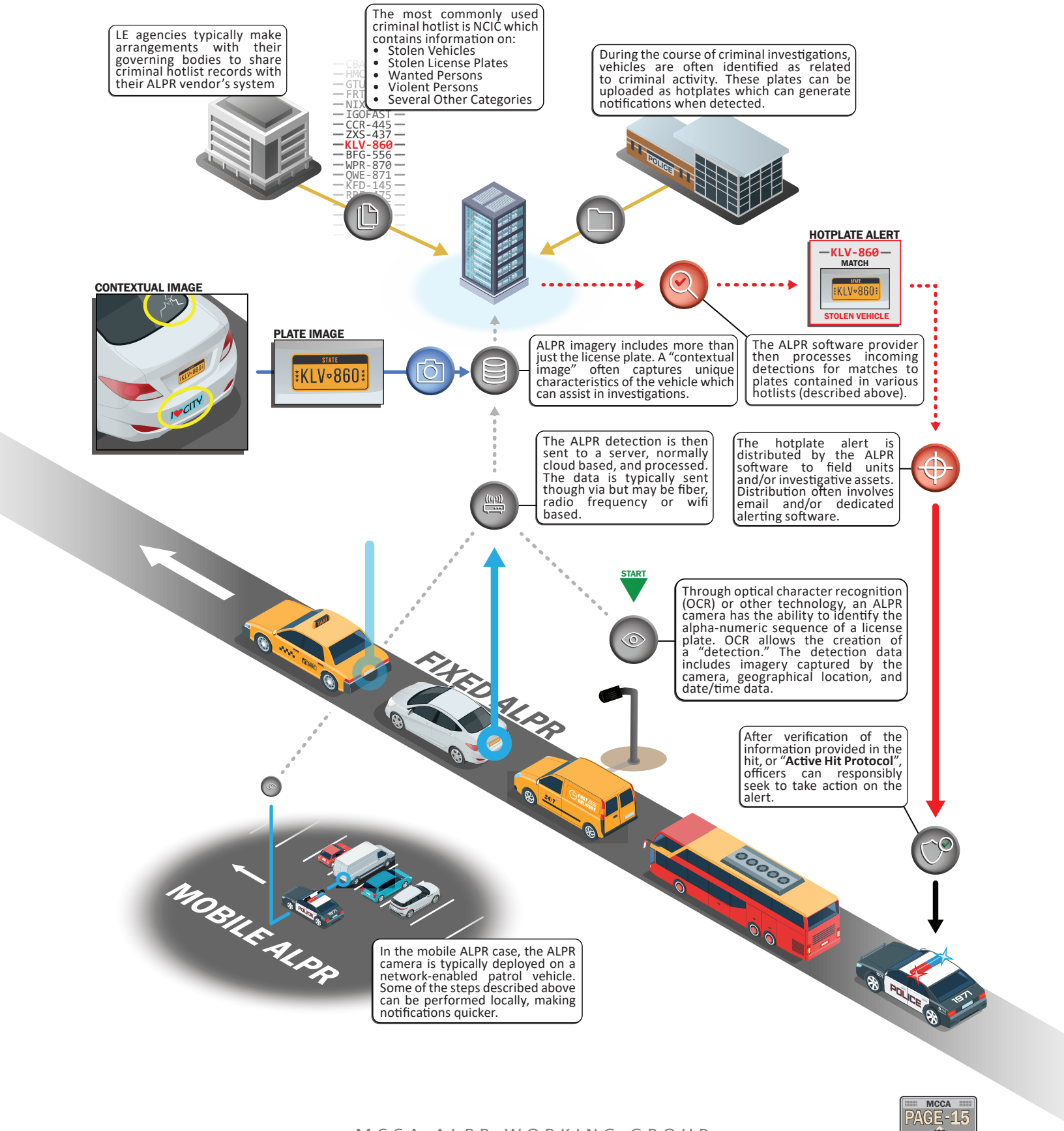
Depending upon the specific environment where it is deployed, the ALPR reading device should, at a minimum, support FIPS 140-2 Level 2. Aspects of FIPS 140-2 Level 3 are also becoming increasingly desirable and necessary, especially as ALPR technology advances.

7 Criminal Justice Information Services (CJIS) Security Policy, CJISD-ITS-DOC-08140-5.9.1, US Department of Justice - Federal Bureau of Investigation, Version 5.9.1, October 22, 2022.

8 A. Lee, M. Smid, S. Snouffer, Security Requirements for Cryptographic Modules [includes Change Notices as of 12/3/2002], (NIST FIPS), National Institute of Standards and Technology, 2001. https://doi.org/10.6028/NIST.FIPS.140-2

ALPR Operations Infographic

Several aspects of the operation of ALPR technology can be better understood when put in the context of the technological workflow.



ALPR Synergy with Other Law Enforcement Technologies

As law enforcement gains access to more information, technology will help ensure the data is organized so law enforcement officers can solve complex policing problems. Any single data source, such as ALPR, only answers one of many questions. It only tells law enforcement where a vehicle was at a given time. ALPR alone does not answer critical questions such as whom the car belongs to or who has been associated with it before, whether any of those individuals have a history of involvement in similar incidents, and other critical questions.

By integrating data across common law enforcement data sources, those questions can be asked and answered immediately, drastically increasing the odds of solving cases. Here are a few examples:

> *Consider a situation where CCTV footage captures a partial plate on a vehicle shortly after the commission of a crime. In an ideal scenario, an ALPR database may be queried to determine the rest of the characters on the license plate. Then a separate RMS system could be queried to determine if that license plate has ever been mentioned in a case report.*
>
> *A platform has ALPR, RMS, citation, and crash data integrated into one place. An ALPR detection can be searched and then linked to see if that plate has been named in an RMS case, vehicle citation, or crash report, along with any involved individuals. Links between vehicles, people, and incidents can be seen without having to search each database individually.*
>
> *An ALPR alert occurs in a platform that has CAD & CCTV integrated. As a result, an immediate CAD call can be created to accompany the alert, and any relevant CCTV footage in the area can be attached and sent to the responding officer, better preparing them to engage with the vehicle that triggered the alert.*

In these examples, a singular piece of information would have failed to fully identify the suspect vehicle. It is the utilization of an ALPR database in conjunction with other technologies produces an actionable investigative lead. For ALPR detections to be used to their fullest potential, that data must be connected to other relevant data sets.

The ultimate goal of connected data should be to allow for insights that are impossible to see currently or take too much time to consider. Departments should own all their data, including ALPR detections, and be able to link, connect, or integrate data sets as department leadership deems appropriate. When developing an ALPR program, agencies should ensure their vendors are aligned with this perspective and are capable of facilitating integrations with other law enforcement technology.

Beyond ALPR: AI-Enhanced Vehicle Detection

With advances in image processing technology, specifically those afforded by artificial intelligence and machine learning, it is becoming increasingly possible to identify a vehicle solely from an image. Artificial intelligence is able to focus on characteristics of a vehicle such as make, model, color, or distinguishing attributes/markings. These advanced image processing technologies improve the accuracy of ALPR systems and allow law enforcement to corroborate ALPR information. For example, they could assist with confirming that the vehicle associated with a detection matches the description in the registration record. Image-based detection and identification will continue to advance and improve the efficacy of ALPR technology.

Case Law Related to ALPR

License plates are required in every state to display proof of registration. Registration identifies a particular vehicle and confirms that it meets minimum state-mandated safety requirements to be operated on public roadways. In addition, operators of vehicles must be licensed to drive legally on public roads.

It is possible in many states to own a vehicle and, if it is never parked or operated on a public roadway, not be required to display license plates. Furthermore, one can own a car but have no authority to operate it, just as one can be licensed to drive a car but never actually own one. Collecting information related to people and vehicles are separate and distinct concepts, although not entirely mutually exclusive. The alpha-numeric characters of a license plate alone do not indicate who owns the vehicle or is licensed to operate it.

For more than 50 years, the United States Supreme Court, and many lower courts, have repeatedly acknowledged that vehicles are inherently subject to greater regulation when operated on public roadways. In the age of enhanced technology, ALPR invokes specific legal considerations:

- Reasonable privacy expectations of those in vehicles on public roadways
- Persistent tracking and the nature of ALPR technology
- The nexus between license plates and personally identifiable information
- Collecting and sharing ALPR data
- The degree of intrusion authorized by an ALPR hotplate detection

An examination of existing case law related to these concepts follows. There is often no bright-line precedent when considering emergent technology. In such instances, reasonable legal conclusions can be inferred from cases related to other technology and privacy issues already adjudicated by the courts.

Privacy Expectations on Public Roadways

In 1967, the U.S. Supreme Court clarified in *Katz v. U.S. (1967)* that "the Fourth Amendment protects people, not places." [9] The Fourth Amendment of the United States Constitution ensures:

> *[The] right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

In *Cady v. Dombrowski (1973),* the U.S. Supreme Court noted that vehicles, while "effects," are constitutionally different from a person's home. The case also referenced the regularity with which police engage in activity unrelated to the enforcement of laws, such as maintaining the efficiency of the flow of traffic and ensuring the safety of those using the roadways. The Court acknowledged that this regular contact with automobiles contributes to police being more often in "plain view" of evidence, instrumentalities of a crime, or contraband.[10]

Delaware v. Prouse (1979) offers historic guidance concerning the constitutionality of stopping or seizing vehicles. The U.S. Supreme Court cites, "the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[11] One can reasonably infer that photographing a plainly visible license plate, on a public roadway, or from a location plainly visible from a lawfully authorized location, with no intrusion upon the vehicle occupants or otherwise interfering with their movement or affecting any person's possessory interest in the vehicle or license plate, is not a seizure constitutionally.

Lower courts have routinely ruled that law enforcement officers may, without specific suspicion, check the status of a license plate against a law enforcement database.[12][13] Therefore, searching aggregated photographs, which contain no specific information about a particular vehicle owner or operator, even when correlated with additional information such as the time, date, and location of the photograph, does not constitute a search.

9 Katz v. United States, 389 United States Supreme Court. 347, (1967). https://supreme.justia.com/cases/federal/us/389/347

10 Cady v. Dombrowski, 413 United States Supreme Court. 433 (1973). https://supreme.justia.com/cases/federal/us/413/433

11 Delaware v. Prouse, 440 United States Supreme Court. 648 (1979). https://supreme.justia.com/cases/federal/us/413/433

12 Jones v. Town of Woodworth, Court of Appeal of Louisiana. 15-568. (2015). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

13 State v. Davis, 237 Or. App. 351, 239 P.3d 1002, Oregon Court of Appeals. (2010). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

Is ALPR Persistent Tracking?

The notion that vehicle travel on public roadways is an unavoidable element of modern living merits consideration, given how ALPR is deployed. Recent U.S. Supreme Court rulings related to law enforcement's use of other technologies have considered the inescapable and automatic nature of data collection. An analysis of these rulings is offered to differentiate the substantially greater capabilities of such technologies compared to those of ALPR.

Two recent U.S. Supreme Court rulings merit particular consideration for the use of technology to investigate the historical movement of persons. In *U.S. v. Jones (2012)*, the U.S Supreme Court held that police need a search warrant to install a covert GPS tracking device on a vehicle to monitor its location for an extended period of time. In *Carpenter v. U.S. (2018),* The Court ruled that police must secure a warrant before obtaining cell-site location information from service providers regarding an individual's location history.

The theme of both cases concerns the capacity that modern technology affords the government to explore comprehensive, specifically personal location information, which was not possible until the advent of recent ubiquitous technology. GPS and cell-site location information enable persistent automated tracking of a targeted individual's activity with such detail and scope that the techniques constitute a search. In the case of *Carpenter v. U.S. (2018),* the Government obtained 12,898 location points cataloging Carpenter's movements. This extensive amount of information amounted to an average of 101 data points per day during the period they obtained historical records.[14]

An ALPR system cannot independently predict life patterns accurately or be used to conduct real-time surveillance of any person or vehicle. Even if police acted with willful disregard for the protections of the Fourth Amendment, it is impossible to accomplish such a degree of ongoing surveillance using ALPR technology. A fixed ALPR camera may be able to collect information about every car that passes its location. Still, the data is limited to an otherwise anonymous characteristic of the vehicle, not automatically attributable to any individual without accessing other restricted databases, and for only a single moment in time at a single location.

Images of plates stored in the ALPR database are retained and made available for specified queries. Tangential information may include the nature of a vehicle's location, direction of travel, and any criminal justice information associated with the detection. As to the question of whether a collection of images from multiple cameras, aggregated in a searchable database implicates Fourth Amendment considerations, the US Supreme Court has not taken up precisely to what extent ALPR coverage, or how robust an ALPR database is, may trigger specific Fourth Amendment implications.

In *Commonwealth v. McCarthy (2020)*, the Massachusetts Supreme Judicial Court concluded that "While the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of ALPRs, that interest was not invaded by the limited extent and use of ALPR data in this case." The case involved law enforcement's use of four ALPR devices on two bridges to investigate a defendant's movements during a period of two months. In that case, the court ruled that the limited use of ALPR data did not violate the defendant's reasonable expectation of privacy.[15]

License Plates & Personally Identifiable Information (PII)

Individuals (people) are licensed, but a vehicle is registered. A vehicle is registered with an organization (typically a state), which then authorizes the vehicle to be driven on public roads and highways by a licensed driver. For example, passenger and commercial vehicles must be registered as a condition of use on a public thoroughfare. Upon registration, the state department of motor vehicles then issues a license plate which must be attached to the vehicle and openly displayed for vehicle identification purposes. The purpose of a license plate is to identify a vehicle uniquely, and it does not include personally identifiable information of any individual. By itself, a license plate number is an anonymous code unless combined with other registration information containing owner/operator information (i.e., a department of motor vehicles database or an employee or homeowner registration). Thus, an ALPR record is generated from publicly available data and corresponds with detecting a vehicle, not an individual, at a specific location and time.

The federal *Driver's Privacy Protection Act (DPPA)* was enacted in 1994 to "protect the personal privacy and safety

14 Carpenter v. United States, United States Supreme Court. 585 (2018). https://supreme.justia.com/cases/federal/us/585/16-402

15 Commonwealth v. McCarthy, 484 Massachusetts Supreme Judicial Court (2020). https://cases.justia.com/massachusetts/supreme-court/2020-sjc-12750.pdf

of licensed drivers consistent with the legitimate needs of business and government." DPPA made it "unlawful" to access, disseminate, or otherwise misuse information held by a state's motor vehicle office, including information related to both drivers and vehicles, without the owner's consent or for another legitimate, legally authorized purpose, such as criminal justice purposes. ALPR systems do not automatically link to data governed by DPPA. Law enforcement can only obtain such protected information from other secure, access-restricted criminal justice databases.

The case of *Harrison Neal v. Fairfax County Police (2020)* examined the use of an ALPR system to passively scan and retain license plates that were not on a hotlist to determine if such a practice violated the state's *Government Data Collection and Dissemination Practices Act.*

A key element of the case was whether an ALPR system constitutes an information system governed by the Code of Virginia. The court found that the ALPR system did not, noting that the ALPR database can be searched only by license plate number, not by any person's information. Furthermore, the system does not gather identifying information about the vehicle owner. To acquire such personal data, an officer must query a wholly separate criminal justice database via a different computer program.[16]

California Code 1798.29 specifically expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. While not adjudicated by any court, ALPR information is considered personal information in California due to unique state legislation.

Data Collection & Sharing

A license plate is a required government instrument specifically intended to identify the vehicle to which it is affixed publicly. In the case of *United States v. Ellison (2006)*, the Court noted:

> *This court has yet to address in a published opinion the question of whether an individual has a reasonable expectation of privacy regarding their license plate. In two unpublished decisions, however, this court has agreed with the other circuits that have decided this issue by holding that no such privacy interest exists. The reasoning of these opinions, as well as that of the Supreme Court in related cases, leads us to agree that a motorist has no reasonable expectation of privacy in the information contained on his license plate under the Fourth Amendment.[17]*

Publicly viewing or photographing a displayed license plate constitutes activity protected by the First Amendment of the United States. The cataloging and subsequent sharing of such data remain largely regulated by state or local legislation. In the case of *U.S. v. Yang (2020),* the Ninth Circuit ruled that the defendant did not have standing to challenge government queries of a vendor's ALPR database for records of his movement when he kept a rental car beyond the contract due date. The court noted that Yang failed to establish that he had a reasonable expectation of privacy in the historical location information of the vehicle that was the subject of the query. The Court declined to address any potential privacy interests related to the warrantless use of ALPR technology.[18]

16 Harrison Neal v. Fairfax County Police, Record No. 191127, Supreme Court of Virginia (2020). https://cases.justia.com/virginia/supreme-court/2020-191127.pdf

17 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

18 United States v. Yang, No. 18-10341, United States Court of Appeals for the 9th Circuit (2020) https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

ALPR Hits & Degrees of Intrusion

Several cases have affirmed that an ALPR hotplate detection, also referred to as a "hit," constitutes sufficient reasonable suspicion to affect a traffic stop. For example, in the case of *Hernandez-Lopez v. State (2013)*, the Georgia Court of Appeals held that an ALPR system merely aided the officer by augmenting his sensory faculties and that based on the alert provided by the ALPR, the officer had reasonable, articulable suspicion to conduct a traffic stop. [19]

Similarly, in the case of *Traft v. Commonwealth (2018)*, the Supreme Court of Kentucky held that an officer obtaining information linked to his license plate did not violate the defendant's rights under the Fourth Amendment. This information indicated that Traft had an outstanding bench warrant and, therefore, reasonable suspicion existed to stop the vehicle. Furthermore, the court noted that the license plate "was displayed in a place where he had no reasonable expectation of privacy."[20]

In the case of *Green v. City and County of San Francisco (2014)*, an ALPR system returned a hit based on a misread. The officer was transporting a prisoner at the time and could not verify the hit's validity. The image on the ALPR was "dark and blurry." The officer subsequently provided a description of the vehicle via police radio, including the incorrect license plate indicated by the ALPR system, not the actual plate displayed on the car. Dispatch ran the plate as provided and noted that it belonged on a pick-up truck.[21]

A second officer observed Green's sedan bearing the plate as broadcast by the first officer. However, this officer also failed to confirm whether the radioed license plate number matched the plates on Green's car. Consequently, Green was stopped, challenged at gunpoint by multiple officers, placed on the ground, and handcuffed. Green filed suit against the defendants, alleging claims under 42 U.S.C. 1983 and California state law for wrongful detention, false arrest, and excessive force. The Ninth Circuit ruled that "an unconfirmed hit on the ALPR does not, alone, form the reasonable suspicion necessary to support an investigatory detention."

While legally permissible to affect a stop based on an ALPR hit, independent verification of the validity of an ALPR alert should be considered a best practice. Verifying that the actual vehicle license plate and the read on the ALPR screen are safeguards against a potential unjustified intrusion upon any person. Such guidance should neither cause officers to hesitate when officer safety is a concern nor preclude officers from acting on indicators amounting to reasonable suspicion based on other observations coupled with their training and experience. However, inappropriate outcomes resulting from the use of law enforcement technology can have substantial repercussions on perceptions of police legitimacy and the continued availability of such tools.

In conclusion, ALPR systems detect license plates in public locations collecting information that is generally not considered private. Critical elements of an ALPR system, such as the extent of camera coverage, reasons for selecting fixed deployment locations, length of time that data is retained, and the extent to which the information is shared, may factor in with respect to if an ALPR system implicates Fourth Amendment considerations. The consistently responsible use and thoughtful deployment of ALPR technology will ensure that all civil rights and liberties are respected.

19 Hernandez-Lopez v. State, 319 Ga. App. 662, 738 S.E.2d 116, Court of Appeals of Georgia (2013) https://cite.case.law/ga-app/319/662

20 Traft v. Commonwealth, 539 S.W.3d 647 Supreme Court of Kentucky (2018) https://cite.case.law/ga-app/319/662

21 Green v. City and County of San Francisco, No. 11-17892, United States Court of Appeals for the 9th Circuit (2014). https://law.justia.com/cases/federal/appellate-courts/ca9/18-10341/18-10341-2020-05-04.html

Conclusion

As stated in the introduction, this product contains suggestions and recommendations, which, if adopted, will maximize ALPR technology's effectiveness while ensuring it is used ethically and responsibly. While this product provides a robust evaluation of the technology, it is impossible to cover every aspect of the technology. Therefore, the Working Group recommends that law enforcement use the tenets discussed in this document to help evaluate decisions regarding the use of ALPR technology. This must include the potential impact of ALPR technology on public trust and the community served. It is essential that, when implementing any technology program, law enforcement operate in a manner that is thoughtful, disciplined, and contextually mindful of its constituencies.

For those agencies wishing to implement an ALPR program but are still determining how to move forward, collaboration with other entities who have already developed robust, responsible programs is recommended. The sharing of best practices in crime-fighting technology among law enforcement has a history of beneficial impacts. Law enforcement must be good stewards of information and policies and be willing to share this with fellow law enforcement agencies wishing to begin using ALPR.

Law enforcement's use of ALPR is ubiquitous because the information these systems provide is advantageous. ALPR data has aided in countless successful criminal investigations and has proven to be one of the most valuable technologies available to law enforcement. Few technologies have aided law enforcement in keeping communities safe like ALPR. However, the capabilities of ALPR technology are continuously evolving, and the MCCA will continue to monitor it. The MCCA will remain engaged with all interested stakeholders and communicate the latest information with member agencies and the entire law enforcement profession so best practices can be adjusted as needed.

Acknowledgments

Major Cities Chiefs Association would like to extend a special thanks to the ALPR Working Group and its members listed below. The contents of this document would not be possible without the collaboration between these law enforcement professionals and the technology vendor participants.

Kelly Bluth
DETECTIVE
Las Vegas Metropolitan Police Department

Blake Bullock
SENIOR DIRECTOR & GM FLEET PRODUCTS
Axon

Paige Burley
CLIENT FACING DEPLOYMENT
Peregrine

Gabriel Candelaria
LIEUTENANT
Dallas Police Department

Jeffrey Carroll
ASSISTANT CHIEF OF POLICE
Metropolitan Police Department Washington D.C.

Laura Cooper
EXECUTIVE DIRECTOR
Major Cities Chiefs Association

Travis Eicher
LMPD TECHNICAL SERVICES
Louisville Police Department

Dan Gillespie
TECHNOLOGY PROGRAM MANAGER
Louisville Police Department

Jeremy Harrison
MAJOR
Oklahoma City Police Department

Kyle Hoertsch
PRODUCT DEVELOPMENT MGR ENTERPRISE SOLUTIONS
Motorola Solutions

Milton Wyatt Martin
ASSISTANT CHIEF
Houston Police Department

Matt Melton
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Jason Olin
DIRECTOR OF GOVERNMENT AFFAIRS
Major Cities Chiefs Association

Samuel Paul
DEPUTY
Los Angeles Sheriff's Department

Christian Quinn
MANAGING PRINCIPAL
Fulcrum Innovation LLC

Jeremy Slavish
SENIOR BUSINESS DEVELOPMENT MANAGER
Amazon Web Services

Paul Steinberg
SENIOR VICE PRESIDENT OF TECHNOLOGY
Motorola Solutions

Josh Thomas
VP OF POLICY AND COMMUNICATIONS
Flock Safety

Matthew Thomas
COMMANDER
Indianapolis Metropolitan Police Department

Mark Torres
COMMANDER - REAL TIME CRIME CENTER
Albuquerque Police Department

Mike Wagers
SENIOR VICE PRESIDENT STRATEGIC INITIATIVES
Axon

Dalton Webb
DIRECTOR OF RTCC STRATEGY
Flock Safety

Paden Weber
INTELLIGENCE OFFICER
Las Vegas Metropolitan Police Department

William Zelms
CAPTAIN
Virginia Beach Police Department

GRAPHIC DESIGN BY PADEN WEBER

Definitions

Automated License Plate Reader/Recognition (ALPR): ALPR systems comprise cameras that capture an image of a vehicle's license plate and use Optical Character Recognition (OCR) to automatically read license plate characters.

Contextual Photo/Image: An overview image of the area around a detection.

ALPR Record/Detection: Is generated when an instance of a vehicle license plate is detected, imaged, and processed to identify the plate.

Hit: A detection of a license plate that matches a plate previously registered on a hotlist or hotplate.

Hotlist: A file that contains the license plate numbers of stolen vehicles; AMBER, SILVER, or other law enforcement alerts; lists of license plate numbers known to be associated with specific individuals, such as wanted or missing individuals.

Hotplate: A license plate with a wanted status. It may also be entered into a system designed to provide a notification of future detections.

Misread: An incorrect translation of a license plate.

Fixed Camera: An ALPR camera that is affixed to a non-moving structure.

Mobile Camera: A vehicle-mounted camera.

Law Enforcement Data: ALPR data collected by law enforcement-owned ALPR cameras.

Data Retention: Refers to the amount of time that the collected data will be preserved.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.[1]

National Crime Information Center (NCIC): An electronic clearinghouse of crime data, such as mug shots and crime records, available to virtually every criminal justice agency nationwide.[2]

1 Guidance on the Protection of Personally Identifiable Information, U.S. Department of Labor. https://www.dol.gov/general/ppiihttps://www.dol.gov/general/ppii

2 National Crime Information Center (NCIC), Federal Bureau of Investigation. https://le.fbi.gov/informational-tools/ncic

Appendix A – Success Stories

Homicide

After committing a homicide, the suspect fled the scene by vehicle. During the investigation, investigators learned that the suspect drove a specific vehicle with damage to the body. Using the ALPR system, detectives created a geographic boundary around the crime location. While reviewing the historical ALPR detections from that immediate area, a vehicle matching the suspect's vehicle description was identified. Detectives then discovered the actual license plate registration information, which returned to the primary suspect. Another query of that vehicle through the ALPR system revealed that the suspect vehicle had fled the jurisdiction immediately after the homicide occurred. This was later confirmed and corroborated by the suspect's cell phone location records.

Homicide

During a road rage incident resulting in a shooting and murder, the suspect was reportedly driving a black hearse. Responding officers obtained the victim's license plate number and checked it through the ALPR system. The officers located an ALPR record of the victim's vehicle passing an ALPR deployment site three minutes before the shooting. The officers checked for other vehicles driving past the ALPR cameras around the same time as the victim. The vehicle driving directly behind the victim was a black hearse. The ALPR data, along with a tip from the public, were pivotal in the arrest. The suspect gave a full confession. The arrest occurred within only a few hours of the crime.

Homicide

The victim knocked on the suspect's hotel room door. Annoyed by the knocking, the suspect opened the door and immediately shot and killed the victim. Surveillance footage of the suspect and his associate leaving captured the type of vehicle used by the suspect but did not capture the license plate. An ALPR camera system was stationed just down the street from the hotel. Officers reviewed the ALPR database for the time frame around the homicide. One minute before the 911 call, the ALPR camera captured a detection of a vehicle matching the one observed in the hotel surveillance. Armed with the vehicle registration information, the vehicle's lien holder was contacted, which provided new investigative leads. Within 11 hours of the shooting, officers located the suspect's vehicle hidden in a home's garage. The suspect and his associate were detained, provided a confession, and later charged with homicide.

Burglary

A police agency used ALPR to identify two suspect vehicles involved in a burglary. Multiple suspects in two vehicles committed a residential burglary, with the resident shooting and killing one of the suspects. Doorbell camera videos were recovered, and homicide detectives used them to establish a timeline. ALPR searches focused on the timeline, which resulted in ALPR scans for both suspect vehicles. A subject associated with one of the vehicles was later determined to be involved and arrested for burglary.

Sexual Assault and Attempted Murder

A victim met the suspect at a bar. They left and the suspect drove them to the desert, where he sexually assaulted, beat, strangled, and ran her over. The vehicle plate from the bar where the incident began was queried in the ALPR system. Historical detections placed the suspect vehicle in the desert where the victim was assaulted and left behind, along with other areas where the victim reported they had driven before the assault. The ALPR data was critical in the arrest of this violent attacker.

Fatal Hit-and-Run Traffic Accident

ALPR was used to identify the suspect vehicle that left the scene of a fatal traffic accident after hitting two people. The make and model of the vehicle were identified but not the license plate. The license plate and other supporting evidence were discovered by leveraging the ALPR system. After the crime occurred, ALPR detection records showed significant damage to the suspect vehicle.

Kidnapping

A male subject attempted to grab a female in a business parking lot. Video surveillance captured the subject and his vehicle. Detectives used video footage to determine the suspect vehicle's make, model, and year range. A query of the ALPR system provided sufficient information to confirm the suspect vehicle and registration. The male was later identified. A records check revealed he had two prior arrests for sexual assaults. He was later located and arrested for the crime of kidnapping.

Arson

A subject set fire to the sign and lawn outside an FBI office building. Surveillance footage showed a gold Chevy Tahoe with distinctive damage to the passenger and rear sides of the vehicle. The license plate number was not visible. Analysts searched more than 6,000 images in the ALPR database, looking for Chevrolet SUVs similar to the one in the surveillance footage. After searching the ALPR database, analysts found a vehicle with matching damage, identified the registered owner, then disseminated a bulletin for officers to locate the vehicle. Initially, officers could not locate the registered owner, who was transient. A few days later, a patrol officer spotted the vehicle based on the bulletin and detained the suspect. The suspect was positively identified and linked to the original arson and another one in a different part of the state. Less than one month later, the suspect accepted the criminal prosecution agreement offered by the prosecutors.

Appendix B – Myths and Misconceptions

A review of case law provides a snapshot of the legalities supporting the use of ALPR technology. In contrast, some misinformation exists on the use of ALPR technology by law enforcement. Therefore, reviewing and understanding the myths and misconceptions about ALPR in law enforcement is essential.

MYTH

ALPR detections contain private, personally identifying information.

REALITY

ALPRs are designed to capture three details when a vehicle passes through their view: a photograph of the vehicle, the characters on the license plate of the vehicle, and the location, date, and time when the vehicle passes the ALPR.

Publicly-owned ALPR systems read the license plates of vehicles on public roadways and capture information that is generally not considered private. For example, if an individual were to stand by the side of a public road and take a picture of every vehicle that passed them, write down its plate number, and record the date and time, they would be within their legal rights to do so. Likewise, a person could place a camera on their property facing a public throughway and capture the same information an ALPR does. In *U.S. v. Ellison (2006)*, the Court explained that not only is there no privacy interest in a license plate number, but a subsequent entry into a computer system to retrieve other non-private information does not constitute a search.[3] By states mandating each vehicle operating on the roadway publicly display a license plate and even illuminate it at night, the expectation is for the license plate to be read at any time while on a public roadway.

An ALPR system does not automatically capture or record restricted information contained in an individual's motor vehicle records, such as their name, address, phone number, Social Security Number, driver identification number, etc. *The Driver's Privacy Protection Act of 1994* requires all states to protect this personal information ensuring ALPR reads are anonymous until additional steps are taken to access separate statutorily regulated databases. Therefore, when a law enforcement officer needs to access motor vehicle records based on data captured by an ALPR, they would need to perform the same manual processes to retrieve this information as they would in other investigative circumstances. Additionally, adequate policies limit access to ALPR data by requiring justification for the review of individual ALPR records. This effectively ensures that most ALPR-captured data is never even accessed before it is purged.

Therefore, retrieving non-public information based on ALPR data requires law enforcement to adhere not only to the policies and laws regarding the ALPR data but also to the policies and laws for accessing the restricted databases housing driver's license and vehicle information. In summary, ALPR systems do not grant expanded access to any non-public records databases, nor do they circumvent the auditing processes that are in place to ensure restricted data is accessed only for official use and as permitted by law.

3 United States v. Ellison, 462 F.3d 557, 561, United States Supreme Court. (6th Cir. 2006). https://caselaw.findlaw.com/la-court-of-appeal/1717448.html

MYTH

ALPR technology is a form of mass surveillance.

REALITY

Guided by proper policy and processes, ALPRs are effective tools for law enforcement to narrow the focus of investigations and limit negative collateral impacts when policing high-crime areas.

A scenario most major city police departments are familiar with is as follows: A motorist is stopped by police only to later be released and sent on their way in a case of mistaken vehicle identity. Their misfortune was caused by driving a vehicle matching the general description of one recently broadcasted of a suspect vehicle in a violent crime. Though the detention is usually short-lived, the trauma it causes may not be. This type of "wrong place, wrong time" scenario is most likely to occur when non-specific or incorrect information is relayed to officers during an in-progress incident. Even a single negative experience like this can spread quickly throughout a community, jeopardizing efforts to build trust. Unfortunately, these scenarios most commonly affect residents in neighborhoods disproportionately impacted by violent crime and gun violence. The use of ALPRs can help mitigate these occurrences.

ALPRs provide an additional mechanism to corroborate or refute witness accounts of suspect vehicles. This helps narrow the focus of law enforcement when canvassing and provides officers with the increased ability to bypass lookalike vehicles and only interact with the cars that truly contain the distinct characteristics of the vehicle suspected in the crime.

A common talking point designed to instill fear in ALPRs technology is that they "could" be used to track people involved in first amendment protected activities. The purpose of robust agency policy is to restrict use to legally permissible actions and ensure accountability if rules are broken. It must be noted that the same policies and laws governing law enforcement's actions without technology still apply when using technology. In fact, the audit trails in technology ensure that a hindsight review of any actions taken is afforded an even more detailed perspective than the actions taken without records produced by technology.

Appendix C – State-Level Laws and Regulations

At least 16 states have statutes regarding the use of ALPR or the retention of data collected by ALPR technology. This information was derived from a database maintained by the National Conference of State Legislatures.[4] The states and their laws are as follows:

Arkansas-Ark. Code §§ 12-12-1801 to 12-12-1808

Prohibits use of ALPRs by individuals, partnerships, companies, associations or state agencies. Provides exceptions for limited use by law enforcement, by parking enforcement entities or for controlling access to secure areas. Prohibits data from being preserved for more than 150 days.

California-Calif. Veh. Code § 2413

Provides that the California Highway Patrol (CHP) may retain data from a license plate reader for no more than 60 days, unless the data is being used as evidence in felony cases. Prohibits selling or making available ALPR data to non-law enforcement officers or agencies. Requires CHP to report to the legislature how ALPR data is being used.

California-Calif. Civil Code §§ 1798.29, 1798.90.5

Establishes regulations on the privacy and usage of automatic license plate recognition (ALPR) data and expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. Imposes privacy protection requirements on entities that use ALPR information, as defined; prohibit public agencies from selling or sharing ALPR information, except to another public agency, as specified; and require operators of ALPR systems to use that information only for authorized purposes.

Colorado-Colo. Rev. Stat. § 24-72-113

Requires that video or still images obtained by passive surveillance by governmental entities, such as images from monitoring cameras, must be destroyed within three years after the recording of the images. Specifies that the custodian of a passive surveillance record may only access the record beyond the first anniversary after the date of creation of the record if there has been a notice of claim filed, or an accident or other specific incident that may cause the passive surveillance record to become evidence in any civil, labor, administrative, or felony criminal proceeding. Creates exceptions allowing retention of passive surveillance records of any correctional facility, local jail, or private contract prison and passive surveillance records made or maintained as required under federal law.

Florida-Fla. Stat. § 316.0777

Creates a public records exemption for certain images and data obtained through the use of an automated license plate recognition system and personal identifying information of an individual in data generated from such images. Provides that images and data containing personal information obtained from automated license plate recognition systems are confidential. Allows for disclosure to criminal justice agencies and to individuals to whom the license plate is registered in certain circumstances.

Georgia-Ga. Code § 35-1-22

License plate data may be collected and accessed only for a law enforcement purpose. The data must be destroyed no later than 30 months after it was originally collected unless the data are the subject matter of a toll violation or for a law enforcement purpose. Allows sharing of captured license plate data among law enforcement agencies. Law enforcement agencies deploying an automated license plate recognition system must maintain policies for the use and operation of the system, including but not limited to policies for the training of law enforcement officers in the use of captured license plate data. License plate data collected by a law enforcement agency is not subject to public disclosure.

4 Automated License Plate Readers: State Statutes," National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Maine-29-A M.R.S.A. § 2117-A(2)

Prohibits the use of automatic license plate recognition systems except for certain public safety purposes. Provides that data collected is confidential and may be used only for law enforcement purposes. Data collected may not be stored more than 21 days.

Maryland-Md. Public Safety Code § 3-509

Specifies the procedures and protocols that a law enforcement agency must follow in connection with the operation of an "automatic license plate reader system" and "captured plate data." Requires the State Police to adopt procedures to address who has access to the data and training for those individuals and to create an audit process. Provides that data gathered by an automatic license plate reader system are not subject to disclosure under the Public Information Act.

Minnesota- Minn. Stat. §§ 13.82,13.824, 626.8472

Relates to data practices; classifies data and provides procedures related to automated license plate readers; provides the data that may be collected by such readers; relates to requirements for the sharing of such data among law enforcement agencies; requires the maintenance of a public log recording the uses of such data; requires related records maintenance and the auditing of such records; requires written procedures governing access to the data; requires certain notification when setting up readers.

Montana-Mont. Code Ann. §§ 46-5-117 to -119

Prohibits the use of license plate readers by an agency or employee of the state or any subdivision of the state on any public highway. Provides exceptions for specific agencies or purposes, such as state or local law enforcement, if specified requirements are met. Except as provided, license plate data captured by law enforcement may not be preserved for more than 90 days after the date that the data is captured.

Nebraska- Neb. Rev. Stat. § 60-3201 to 3209

Requires any governmental entity that uses an automatic license plate reader (ALPR) system to adopt a policy governing use of the system. Governmental entities also must adopt a privacy policy to ensure that captured plate data is not shared in violation of this act or any other law. The policies must be posted on the internet or at the entity's main office. Requires annual reports to the Nebraska Commission on Law Enforcement and Criminal Justice on ALPR practices and usage. Provides that captured plate data is not considered a public record.

New Hampshire-N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130

Restricts the use of automated license plate readers to local, county and state law enforcement officers, who shall only use the devices subject to specified conditions and limitations and for specified purposes. Provides that records of number plates read shall not be recorded or transmitted anywhere and shall be purged from the system within 3 minutes of their capture, unless the number resulted in an arrest, a citation or protective custody or identified a vehicle that was the subject of a missing or wanted person broadcast.

North Carolina-N.C. Gen. Stat. §§ 20-183.30 to .32

Requires state or local law enforcement agencies to adopt a written policy governing the use of an ALPR system that addresses databases used to compare data obtained by the system, data retention and sharing of data with other law enforcement agencies, system operator training, supervision of system use, and data security and access. Requires audits and reports of system use and effectiveness. Limits retention of ALPR data to no more than 90 days, except in specified circumstances. Provides that data obtained by the system is confidential and not a public record.

Oklahoma-Okla. Stat. §§ 47-4-606.1

Provides that participating law enforcement agencies may use automatic license plate reader systems to access and collect data for the investigation, detection, analysis or enforcement of the state's compulsory insurance law. States that data collected under the program may not be used by any individual or agency for purposes other than enforcement of the compulsory insurance law, prohibits sale of the data under the program, and provides that data is exempt from the Oklahoma Open Records Act, except when retained as evidence of a violation of the compulsory insurance law. These provisions do not prohibit the use of any other automated license plate reader system by an individual or private legal entity for lawful purposes.

Tennessee-Tenn. Code §§ 55-10-302, 10-7-504(a)

Provides that any captured automatic license plate data collected by a government entity may not be stored for more than 90 days unless they are part of an ongoing investigation, and in that case provides for data to be destroyed after the conclusion of the investigation. Captured plate data from automatic license plate reader systems must be treated as confidential and shall not be open for inspection by members of the public.

Utah-Utah Code §§ 41-6a-2001 to -2005

Provides that a governmental entity may not use an automatic license plate reader system except for specified uses, such as by law enforcement agencies for the purpose of protecting public safety or conducting criminal investigations and by other government entities for limited other purposes. Provides that captured plate data are a protected record under the Government Records Access and Management Act, if the captured plate data are maintained by a governmental entity. Provides that captured plate data may only be shared for specified purposes, may only be preserved for a certain time and may only be disclosed pursuant to specific circumstances such as a disclosure order or a warrant. Government entities may not use privately held captured plate data without a warrant or court order, unless the private provider retains captured plate data for 30 days or fewer. Allows an institution of higher education to use automatic license plate readers under certain circumstances.

Vermont- 23 V.S.A. §§ 1607, 1608

Requires a law enforcement officer to be certified in the use of an automated license plate reader to operate such a system. Provides that active system data may only be accessed by an officer with a legitimate law enforcement purpose for the data. A legitimate purpose includes a person's defense against certain charges and does not include enforcement of parking or traffic violations other than commercial motor vehicle violations. Limits retention and access to information gathered through the use of an ALPR system. Requires the Department of Public Safety to adopt rules to implement the law. Requires the Auditor of Accounts to examine requests for data to determine whether the request and the release complied with the law.

Appendix D – CJIS Security Policy

Agencies that wish to use the CJIS Security Policy to assess the security practices of a service provider that will be handling ALPR data should consider the following sections:

- Private Contractor User Agreements and FBI-CJIS Security Addendum [5.1.5]: Private contractors who perform criminal justice functions for a Criminal Justice Agency (CJA) shall be permitted to access CJI pursuant to an agreement between the CJA and the contractor that incorporates the FBI-CJIS Security Addendum approved by the Director of the FBI.
- Agency User Agreements [5.1.1.6]: Fingerprint-based background checks and written agreement with the agency when required.
- Secondary Dissemination [5.1.3]: If data is released to another authorized agency and not part of a primary information exchange agreement, this shall be logged.
- Security Awareness Training [5.2]: All personnel with access to CJI (Criminal Justice Information) shall receive security awareness training within six months of assignment, and biennially thereafter.
- Security Training Records [5.2.3]: Records of security awareness training shall be kept current and maintained by a Security Officer (CSO).
- Reporting Structure and Responsibilities [5.3.1.1]: Establishment of a primary Point of Contact (POC) for CJIS incident handling and response.
- Events [5.4.1.1]: Description of the events that must be logged within the system.
- Audit Monitoring, Analysis and Reporting 5.4.3]: Responsibility for review and analysis of audit records, at a minimum of once a week, to look for inappropriate or unusual activity.
- Audit Record Retention [5.4.6]: The agency shall retain audit records for at least one year.
- Least Privilege [5.5.2.1]: The agency shall approve individual access privileges and enforce the most restrictive set of rights and privileges needed by users for the performance of specified tasks. Logs maintain access privilege changes for a minimum of one year or at least equal to the agency's record retention policy, whichever is greater.
- Access Control Mechanisms 5.5.2.4]: One or more of the following must be employed: access control lists (users, groups, machines), resource restrictions (permission sets), encryption and strong key management, application-level access control.
- Unsuccessful Login Attempts [5.5.3]: CJIS Security Policy requires that after five consecutive invalid attempts, the account shall be locked out for a minimum of 10 minutes.
- System Use Notification [5.5.4]: The system shall allow a notification message to be displayed to let users know a) they are accessing a restricted system, b) usage is monitored, recorded and subject to audit, c) unauthorized use is prohibited and may result in penalties, and d) use of the system indicated consent to monitoring.
- Session Lock [5.5.5]: CJIS Security Policy requires that the system shall prevent access via a session lock after a minimum of 30 minutes of inactivity.
- Remote Access [5.6]: Rules for monitoring and controlling remote access via the internet.
- Use of Originating Agency Identifiers in Transactions and Information Exchanges [5.6.1.1]: An FBI-issued ORI number shall be assigned at the agency level and attached to all activities by the agency's users.
- Password [5.6.2.1.1]: Requirements and standards for passwords.
- Personal Identification Numbers [5.6.2.1.2]: Best Practices on PIN use.
- Advanced Authentication [5.6.2.2]: Advanced Authentication requirements.
- Identifier Management [5.6.3]: Requirements of agencies to manage user identifiers.
- Network Diagram [5.7.1.2]: Requirements for a network topological diagram.

- Media Protection [5.8]: Requirements for security and protection of electronic and physical media.
- Physical Protection [5.9]: Requirements for physical security and access controls around all hardware, software and media.
- System and Communication Protection and Information Integrity [5.10]: Prevent CJI from being transmitted unencrypted across the public network.
- Boundary Protection [5.10.1.1]: Ensure that failure of boundary protection mechanisms do not result in unauthorized release of information.
- Encryption [5.10.1.2]: Minimum of 128 bit encryption when CJI data is transmitted beyond the physical security boundary.
- Intrusion Detection Tools and Techniques [5.10.1.3]: Requirements for intrusion detection tools.
- Cloud Computing [5.10.1.5 and Appendix G.3]: Recommendations for use of cloud computing and assessment of cloud computing service providers.
- Partitioning and Virtualization [5.10.3]: Requirements for partitioning of data and virtualization of resources.
- Patch Management [5.10.4.1]: Requirements for management of software patches.
- Malicious Code Protection [5.10.4.2]: Virus Protection requirements.
- Spam and Spyware Protection [5.10.4.3]: Spam and Spyware Protection requirements.
- Security Alerts and Advisories [5.10.4.4]: Guidance for alerts and advisories.
- Personnel Security [5.12]: Fingerprint-based background checks and rules based on findings.
- Personnel Termination [5.12.2]: Terminated employees shall immediately have access revoked.
- Personnel Sanctions[5.12.3]: Process for employees failing to comply with security policies.
- Mobile Devices [5.13]: Where appropriate, the technology partner must support the agency's mobile device practices (patch management, etc.)

Appendix E – ALPR Audit and Transparency Report Template

The following template provides a rudimentary example of the details and considerations in providing a published report about the performance and effectiveness of an ALPR program.

Automated License Plate Reader Program
Annual Transparency Report

Introduction

The introduction should provide context and background as to what the report is addressing. The introduction defines the specific objectives and purpose of the report. It indicates any problems that may exist and provides answers to problems explored. Finally, the introduction will preview the report and outline the report structure.

Discussion

This is the main body of the report, and it has two primary purposes. The first is to share and explain the conclusions. The second is to justify any recommendations that may be made in the report.

Specific data points that may be considered:

- Number of detections
- Number of hotplate hits
- Number of queries conducted by users
- Number of arrests directly related to ALPR
- Number of user-generated hotplates
- Breakdown of hotplate hit types
- Year-over-year analysis and trends

Conclusion

This section should relate to the information shared in the report. It should be specific to the objectives of the report. It may also address any issues that may be interpreted from the information shared. The conclusion should be brief, logical, and specific.

Recommendations

Recommendations shared should point to future action that can be completed. Recommendations should be feasible, action-oriented and arranged in order of importance.