The author(s) shown below used Federal funds provided by the U.S. Department of Justice and prepared the following final report:

Document Title: **Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement**

Author: **David J. Roberts and Meghann Casanova**

Document No.: **239604**

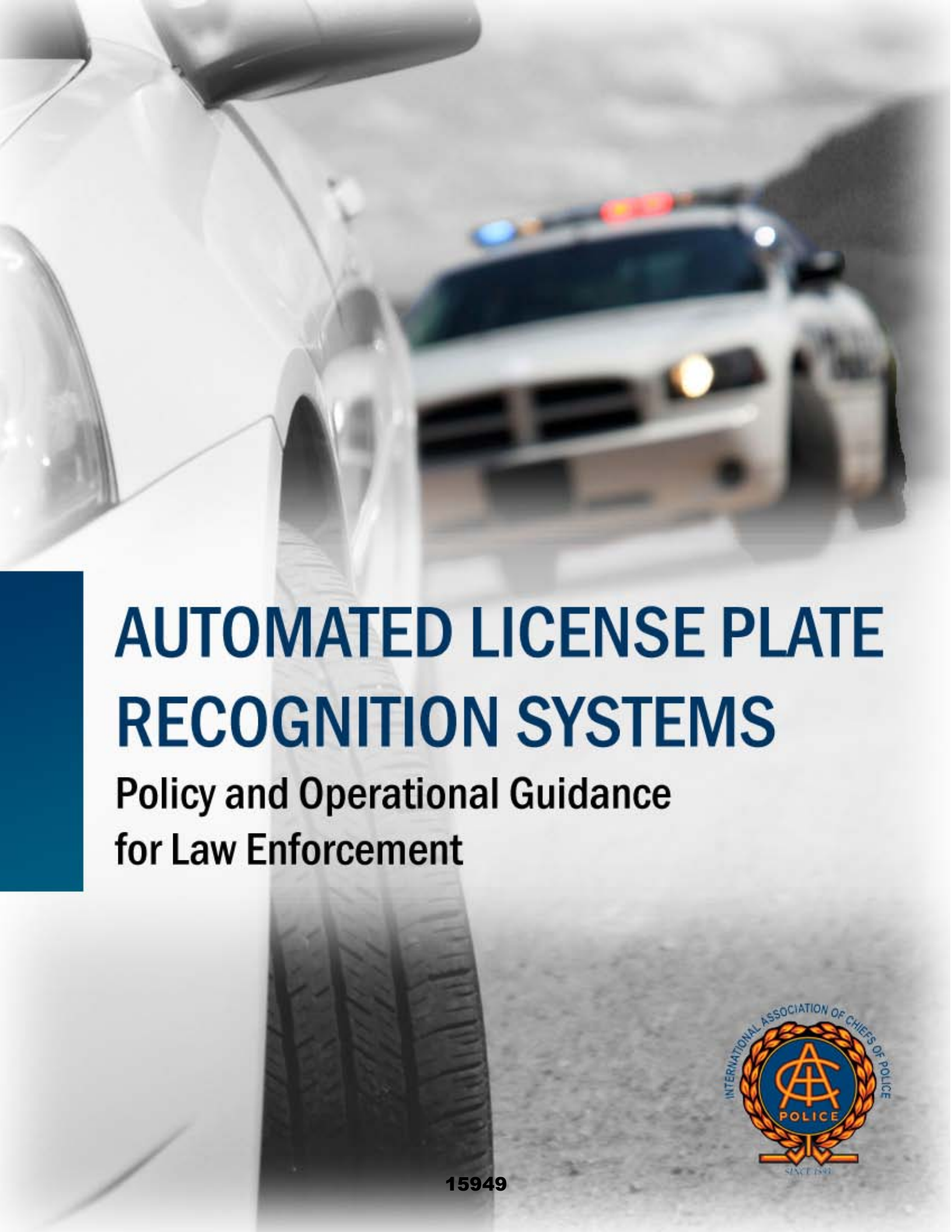
Date Received: **September 2012**

Award Number: **2007-MU-MU-K004**

This report has not been published by the U.S. Department of Justice. To provide better customer service, NCJRS has made this Federally-funded grant final report available electronically in addition to traditional paper copies.

Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

15948



AUTOMATED LICENSE PLATE RECOGNITION SYSTEMS

Policy and Operational Guidance for Law Enforcement

15949

This project, conducted by the International Association of Chiefs of Police (IACP), was supported by Grant No. 2007-MU-MU- K004 from the National Institute of Justice. The National Institute of Justice is a component of the U.S. Department of Justice, Office of Justice Programs, which also includes the Bureau of Assistance; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).

Points of view or opinions contained in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the IACP or the United States Government.

With respect to documentation contained herein, neither the IACP nor the United States Government, nor any of their employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the IACP nor the United States Government nor any of their employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed.

Acknowledgements

IACP Leadership and Project Personnel

Executive Staff

Chief Walt McNeil
President

James McMahon
Deputy Executive Director

Bart R. Johnson
Executive Director

Michael Wagers, Ph.D
State & Provincial Police Director

Project Staff

David Roberts
Senior Program Manager

Meghann Casanova
Project Manager

This report was written by David J. Roberts and Meghann Casanova.

The IACP gratefully acknowledges the contributions of numerous law enforcement practitioners who helped to guide initial discussions of the operational use and value of Automated License Plate Recognition (ALPR) systems, and helped structure the research undertaken in this project. In addition, Dale Stockton, retired Captain, Carlsbad Police Department, provided consulting insight and assisted in site visits, which contributed substantially to our research. We also gratefully acknowledge the law enforcement agencies who participated in the survey and those who accommodated follow-up site visits.

Suggested citation:
David J. Roberts and Meghann Casanova, *Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement,* Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2012.

Table of Contents

Acknowledgements iii
List of Figures vi
List of Tables vii
Executive Summary ix
Introduction 1
Background 3
Police use of license plate data 4
Automated License Plate Recognition (ALPR) Technology 5
An Overview of ALPR 9
Cameras 9
User Interface 10
Software 10
Hot lists 10
Mobile ALPR Systems 11
Fixed and Portable ALPR Systems 12
ALPR Data 13
ALPR Performance 14
Survey of ALPR Use by Law Enforcement 19
ALPR Policies 25
Hot List Management 26
Data Retention 28
Conclusion 35
Endnotes 37
References 49
Appendix A: Sample Agency ALPR Policies 57
Appendix B: IACP ALPR Survey Instrument 105

List of Figures

Figure 1: Examples of Different State License Plate Numbering Schemes 3
Figure 2: Examples of Specialty License Plates for Passenger Vehicles 4
Figure 3: Geographic Distribution of Agencies Using ALPR in 2007 6
Figure 4: Examples of Trunk and Lightbar Mounted Mobile ALPR Cameras 9
Figure 5: An Example of ALPR User Interface 10
Figure 6: Lightbar (left) and Covert (right) Mounted Mobile ALPR Cameras 11
Figure 7: Stationary/Fixed ALPR Cameras on a Bridge and Utility Pole 12
Figure 8: Sample Data and Images Captured by ALPR 14
Figure 9: Sample Plate Designs 15
Figure 10: Poor Image Quality 15
Figure 11: Bent, Dirty, or Damaged Plates 16
Figure 12: Obstructed Plates 16
Figure 13: Geographic Distribution of Survey Respondents 20
Figure 14: ALPR Data Retention Practices in the Washington, D.C. Area 29

List of Tables

Table 1: ALPR Use by Law Enforcement Agencies—LEMAS Survey 2007 Data 6
Table 2: Distribution of LPR use among large and small police agencies 7
Table 3: 'Capture' and 'Read' rates for All United Kingdom (UK) 16
Table 4: 'Capture' and 'Read' rates for All Schengen Community in Isolation of United Kingdom (UK) Number Plates 17
Table 5: Distribution of Agency Size in Survey Sample 19
Table 6: Distribution of ALPR Usage by Agency Size 20
Table 7: Distribution of Agency Size of Sample Respondents: 21
Table 8: Distribution of Agency Type of Survey Respondents 21
Table 9: Types of ALPR Systems Implemented 22
Table 10: Primary Purposes for ALPR Implementation 22
Table 11: Current Uses of ALPR 23
Table 12: Business Value of ALPR 23
Table 13: Regional ALPR Program Participation 24
Table 14: Policy Issues Addressed by Agencies That Have or are Developing ALPR Policies 26
Table 15: Hot List Update Methods 27
Table 16: Hot List Update Frequency 27
Table 17: Hot List Management 27
Table 18: Data Retention Policies of Survey Respondents 29

Executive Summary

Law enforcement officers are often searching for vehicles that have been reported stolen, are suspected of being involved in criminal or terrorist activities, are owned by persons who are wanted by authorities, have failed to pay parking violations or maintain current vehicle license registration, and any of a number of other factors. Law enforcement agencies throughout the nation are increasingly adopting automated license plate recognition (ALPR) technologies, which function to automatically capture an image of the vehicle's license plate, transform that image into alphanumeric characters, compare the plate number acquired to one or more databases of vehicles of interest, and alert the officer when a vehicle of interest has been observed, all within a matter of seconds

This project was designed to assess ALPR implementation among law enforcement agencies in the United States, and to identify emerging implementation practices to provide operational and policy guidance to the field. A random sample of 444 local, state, and tribal law enforcement agencies was surveyed. A total of 305 agencies responded to the initial survey (68.7%). Three-quarters of respondents (235 agencies, 77.0%) indicated that they were not using ALPR, while 70 agencies (23.0%) responded that they were using ALPR. A longer, more detailed survey was sent to the 70 agencies who confirmed they were using ALPR, and 40 agencies (57.1%) responded.

Survey respondents had typically implemented mobile ALPR systems (95%), and were primarily using ALPR for auto theft (69%), vehicle and traffic enforcement (28%), and investigations (25%). Agencies reported increases in stolen vehicle recoveries (68%), arrests (55%), and productivity (50%). Fewer than half (48%) had developed ALPR policies. Over half (53%) updated their ALPR hot lists wirelessly, and nearly half (43%) updated their hot lists once each day. A total of 40% of respondents retain ALPR data for six months or less (n=16). Five respondents (13%) indicated they retain ALPR data indefinitely, while two indicated that retention is based on the storage capacity of the equipment installed.

ALPR technology is a significant tool in the arsenal of law enforcement and public safety agencies. Realizing the core business values that ALPR promises, however, can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all tools and technologies available to law enforcement, ALPR must also be carefully managed. Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered.

Introduction

Law enforcement agencies throughout the nation are increasingly adopting automated license plate recognition (ALPR)[1] technologies to enhance their enforcement and investigative capabilities, expand their collection of relevant data, and expedite the tedious and time consuming process of manually comparing vehicle license plates with lists of stolen, wanted, and other vehicles of interest. Police officers, sheriff's deputies, and other law enforcement practitioners are often on the lookout for vehicles that have been reported stolen, are wanted in connection with a crime or traffic violation, are suspected of being involved in criminal or terrorist activities, are parking violation scofflaws, have failed to maintain current registration or to comply with statutory insurance requirements, or any of a number of other legitimate reasons.

ALPR systems function to automatically capture an image of the vehicle's license plate, transform that image into alphanumeric characters using optical character recognition or similar software, compare the plate number acquired to one or more databases of vehicles of interest to law enforcement and other agencies, and to alert the officer when a vehicle of interest has been observed. The automated capture, analysis, and comparison of vehicle license plates typically occurs within seconds, alerting the officer almost immediately when a wanted plate is observed. Although the ALPR term includes a specific reference to "automated," it should be noted that human intervention is needed insofar as the officer monitoring the equipment must independently validate that the ALPR system has accurately "read" the license plate, that the plate observed is issued from the same state as the one in which it is wanted, and to verify the currency of the alert, i.e., verifying that the reason this vehicle or the owner was wanted or of interest is still valid.

This National Institute of Justice (NIJ)–supported project was designed to assess and document ALPR implementation and operational experiences among law enforcement agencies in the United States, and to identify emerging implementation practices to provide operational and policy guidance to the field. Several data collection techniques were used to gather information for this project, including 1) a survey of law enforcement agencies to assess the scope of the current ALPR implementation, deployment, and operational uses, 2) site visits to interview law enforcement practitioners and observe ALPRs system in operation, and 3) reviewing documents and policies addressing ALPR implementation and use.

This report includes sample ALPR policies from several jurisdictions to assist readers in developing their own policies. Readers are also encouraged to review a supplemental report, "Privacy issues concerning the utilization of automated license plate readers," previously prepared by IACP as part of an effort to develop a privacy impact assessment, in developing ALPR policies for their agencies.

Background

Owners of motorized vehicles driven on public thoroughfares are required by law to annually register their vehicles with their state bureau or department of motor vehicles[2], and to attach license plates that are publicly and legibly displayed.[3] Vehicle license plates generally consist of a series of alpha numeric characters that reference the license plate to the specific vehicle registered (including the make, model, year, and vehicle identification number (VIN)) and the owner and/or lien holder of the vehicle.

New York is credited as the first state to enact legislation requiring vehicle registration on April 25, 1901, with California following in 1902.[4] In Delaware, where numbered license plates were first issued in porcelain in 1909 beginning with a numbering sequence of 1000, the state changed the numbering scheme in 1910, beginning with the number "1", which is reserved for the Governor.[5] Delaware license plates are sold to the owner of the vehicle and can be passed down generation to generation. In 2008, a man and his son paid $675,000 in private auction for license plate number "6"[6] and this figure was matched for Delaware license plate number "11" the following year.[7] Contemporary license plates, which measure 6 x 12 inches in the United States, feature numbering schemes that vary from state to state. States typically use numbers or a combination of letters and numbers in their vehicle license plates. Some states, like Maryland, use stacked letters—one over the other.

Figure 1: Examples of Different State License Plate Numbering Schemes [8]

Connecticut is credited with being the first state to issue vanity plates beginning in 1937, when "motorists with good driving records were allowed to have plates with their initials (2 or 3 letters)."[9] In Texas any person, non-profit organization, or for-profit entity can design a specialty license plate for consideration and potential adoption by the state for an initial deposit of $4,615, which will be refunded to non-profit organizations after 500 of the plates are sold or renewed.[10] A Texas plate with "PORSCHE" recently sold in private auction for $7,500, "AMERICA" for $3,000, and "FERRARI" for $15,000.[11]

Figure 2: Examples of Specialty License Plates for Passenger Vehicles

Texas[12]

New Mexico[13]

Specialty plates generate substantial revenue for states. West Virginia, for example, reports approximately $1.2 million in revenue from the sale of vanity license plates.[14] Texas is estimated to have generated approximately $2.1 million in revenue from the sale of specialty plates through the first 10 months of 2010, Virginia projected potential revenue exceeding $1 million for the sale of specialty plates with company logos, and approximately $600,000 of revenue generated in Nebraska in 2009 from sales of its "Huskers" license plates.[15] The California Legislature recently considered a bill to study the potential use of electronic license plates which would show digital advertisements when the vehicle to which it is attached is stopped for more than four seconds; the vehicle's license plate number would display when the vehicle is in motion.[16]

Police use of license plate data

As noted above, law enforcement practitioners are often searching for vehicles that have been reported stolen, are suspected of being involved in criminal or terrorist activities, are owned by persons who are wanted by authorities, have failed to pay parking violations or maintain current vehicle license registration or insurance, or any of a number of other legitimate reasons. Victims and witnesses are frequently able to provide police with a description of a suspect's vehicle, including in some cases a full or partial reading of their license plate number. Depending on the seriousness of the incident, officers may receive a list of vehicles of interest by their agency at the beginning of their shift, or receive radio alerts throughout the day, providing vehicle descriptions and plate numbers including stolen vehicles, vehicles registered or associated with wanted individuals or persons of interest, vehicles attached to an AMBER[17] or missing persons alert, and "be on the lookout" or "BOLO" alerts.[18] These lists may be sizable depending on the jurisdiction, population size, and criteria for the list, and can present challenges for the patrol officer.

Officers monitor traffic during patrol, searching for vehicles of interest among their other duties. When a potential vehicle of interest is observed, the officer will typically compare characteristics of the observed vehicle and driver with those of the wanted vehicle, including the license plate number, if known. If warranted, the officer may stop the vehicle to further investigate. A license plate check will be run on the vehicle, either by the officer using an in-field computer to initiate

the query, or by radioing dispatch for the query. Results of the query and of the officer's interaction and investigation of the driver will assist the officer in determining next steps.

In addition to spotting vehicles of interest, officers on patrol are also alert to vehicles with expired or missing license plates and annual renewal tags. Failure to maintain current license plate registration may indicate that one or more of several conditions have not been met, including failure to secure vehicle insurance, failing compulsory safety and/or emissions inspections, and simple failure to properly register the vehicle with the state motor vehicle authority. Some jurisdictions may withhold vehicle registration renewal if the owner has unpaid parking or traffic tickets. The lack of a plate or current tags may also indicate that the vehicle has been stolen.

Automated License Plate Recognition (ALPR) Technology

Automated license plate recognition (ALPR) technology was invented in 1976 in the Police Scientific Development Branch (PSDB), Home Office, United Kingdom.[19] The European Secure Vehicle Alliance (ESVA) notes that the "Provisional Irish Republican Army (IRA) terrorist bombings in the City of London resulted in the establishment of the 'ring of steel' in 1993 – a surveillance and security cordon using initially CCTV cameras. In 1997, ANPR cameras, linked to police databases, were fitted at entrances to the ring of steel and gave feedback to monitoring officers within four seconds."[20] Implementation continued over the next several years with forces implementing ANPR systems.

The Home Office Police Standards Unit and the Association of Chief Police Officers (ACPO) began testing dedicated "intercept teams" using ANPR across nine police forces in the multi-phased "Project Laser" beginning 2002.[21] The strategic intent of the ANPR strategy for the Police Services was to "target criminals through their use of the roads."[22] Intercept teams, typically ranged in size of 7 – 12 officers and equipped with ANPR, were designed to enable police to engage criminality on the road and intercept vehicles and drivers wanted in connection with crime, terrorism, and motor vehicle violations. An analysis of the Laser pilot projects, which collectively produced over 46,000 arrests, concluded that "ANPR makes a direct contribution to both national and force objectives and is used on a daily basis to engage criminals. In comparison to a number of other technology-enabled projects in the criminal justice area, its success has been remarkable."[23]

Following success of the Laser pilots, the Police Standards Unit invested £32 million for development of the National ANPR Data Centre (NADC) and a Back Office Facility (BOF), which provide data storage and analytic tools for forces in England and Wales, and support deployment of ANPR at national, regional and local levels. Implementing a single technology platform in forces across the whole of England and Wales has enabled the UK to implement universal business practices and technical and data standards. By the end of the first quarter of 2010, the NADC was receiving approximately 10-12 million license plate reads per day from over 5,000 ANPR cameras, had the capacity to receive up to 50 million reads per day, and maintained a database of more than 7 billion vehicle sightings.[24]

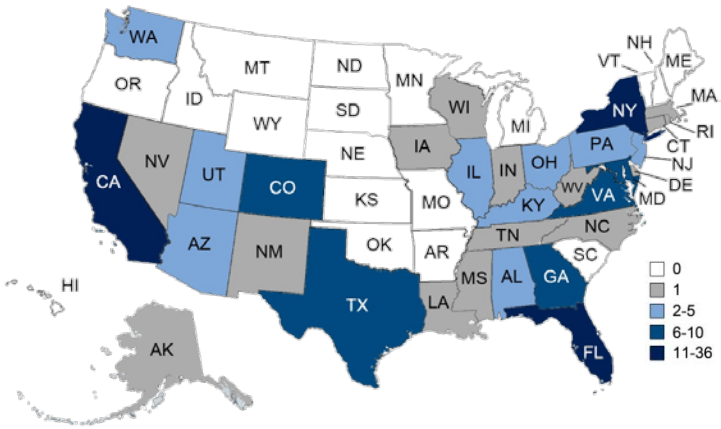
Law enforcement agencies throughout the United States are increasingly implementing ALPR systems. Larger agencies are more likely to have implemented ALPR than smaller agencies, most likely the result of the costs of the technology and the relative sizes of the jurisdictions. The 2007 Law Enforcement Management and Administrative Statistics (LEMAS) survey (the most current LEMAS data available) indicates that as of September 30, 2007, nearly half (48%) of the largest law enforcement agencies (i.e., those with 1,001 or more sworn officers) were regularly using ALPR, as were nearly one-third (32%) of agencies with 500-1,000 sworn officers. In contrast, none of the smallest agencies (i.e., those with fewer than 50 sworn officers) reported regularly using ALPR and only 9% of agencies with 51-100 officers were using it.[25]

Table 1: ALPR Use by Law Enforcement Agencies—LEMAS Survey 2007 Data[26]

Agency Size (Sworn Personnel)	As of September 30, 2007, agency did NOT use license plate readers on a regular basis.	As of September 30, 2007, agency did use license plate readers on a regular basis.	% Using LPR
≤ 50	5	0	0%
51-100	50	2	9%
101-250	450	71	14%
251-500	144	34	19%
501-1000	50	24	32%
1001+	42	39	48%
Total	711	170	19%

In 18 states there were no agencies who reported using ALPR in 2007, and only one agency in each of 15 states. California had the largest concentration of agencies reporting ALPR usage with 36, followed by New York with 31 agencies, and Florida with 16 agencies.

Figure 3: Geographic Distribution of Agencies Using ALPR in 2007 (n=170)[27]



Comparable figures are reported by Lum, et. al., in their 2009 survey of 200 law enforcement agencies drawn from the 2003 LEMAS sample. Their sample was nearly evenly divided between large agencies (≥100 sworn officers) and small agencies (<100 sworn officers).[28]

Table 2: Distribution of LPR use among large and small police agencies [29]

LPR Usage	Small Agencies (n=82)	Large Agencies (n=87)
Use LPR	3 (3.7%)	32 (36.8%)
Do not use LPR	79 (96.7%)	55 (63.2%)

The March 2011 survey by Police Executive Research Forum (PERF), which addressed a variety of technologies, policies and practices, found that nearly three-quarters (71%) of the 70 responding agencies reported using ALPR and 85% plan to acquire or increase their use of the technology over the next five years.[30] Responding agencies were predominantly larger, ranging in size of 10–13,088 sworn officers, with an average of 949 sworn officers (median=336); the average population served among responding agencies was 531,000 (median=183,287).

ALPR also has many applications beyond law enforcement. It is used by departments of transportation to monitor travel time on key roadways for better traffic management (where ALPR captures images of vehicles at two different points on a roadway and calculates travel times between the two points), automated tolling and toll enforcement, access control, and congestion charging, among other things.[31]

An Overview of ALPR

ALPR systems generally consist of a high speed camera with an infrared ("IR") filter or two cameras—one high resolution digital camera and one IR camera—to capture images of license plates; a processor and application capable of performing sophisticated optical character recognition (OCR) to transform the image of the plate into alphanumeric characters; application software to compare the transformed license plate characters to databases of license plates of interest to law enforcement; and a user interface to display the images captured, the results of the OCR transformation, and an alert capability to notify operators when a plate matching an agency's "hot list" is observed. The precise configuration of ALPR systems varies depending on the manufacturer of the equipment and the specific operational deployment.

ALPR systems are able to capture up to 1,800 plates per minute at speeds up to 120-160 miles per hour.[32] Systems range in cost from $10,000 - $22,000, depending on the manufacturer and the specific configuration specified, and agencies have often been able to fund acquisition through federal grant funding sources.

Cameras

Camera hardware is significant to the front-end component of any ALPR system. Since the initial image capture forms a critically important part of the ALPR system and will often determine the overall performance, ALPR systems typically use still or video cameras specialized for the task. Currently, many of the ALPR systems include a set of high resolution digital and IR illuminated cameras which allow the ALPR system to capture images under a variety of light and weather conditions.

Figure 4: Examples of Trunk and Lightbar Mounted Mobile ALPR Cameras

User Interface

In vehicle-mounted ALPR systems, captured images are displayed on a user interface—either a dedicated computer for the ALPR system, or use of the in-field computer already installed in the police vehicle—so the officer can be alerted when a vehicle on one of the hot lists has been observed in the vicinity of the officer.

Figure 5: An Example of ALPR User Interface

The user interface allows the officer to compare the ALPR OCR interpretation of the license plate number to ensure the accuracy of the "read," and to see the larger, contextual image to help the officer in identifying which specific vehicle has the plate of interest. In addition, the user interface also typically enables the officer to manually enter plates on vehicles of interest, manage hot list information, deal with alert queues, and run reports.

Software

As vehicles pass through the field of view of the ALPR camera a picture is taken of license plate and the vehicle. A series of algorithms are performed on the image to isolate the plate and render the alphanumeric characters into an electronically readable format. The sophistication and complexity of each of these algorithms determines the accuracy of the system.

There are six primary algorithms that the software requires for identifying a license plate:

1. *Plate localization* – Finding and isolating the plate on the picture
2. *Plate orientation and sizing* – Compensates for the skew of the plate and adjusts the dimensions to the required size
3. *Normalization* – Adjusts the brightness and contrast of the image
4. *Character segmentation* – Finds the individual characters on the plates
5. *Optical character recognition (OCR)* – Translation of images of text into an electronically readable format
6. *Syntactical/Geometrical analysis* – Check characters and positions against state-specific rules to identify the state of issuance for the license plate

Hot lists

Once the OCR read is obtained, the information is then compared against a database of vehicles of interest, typically known as a "hot list." Hot list information can come from a variety of sources, and is discussed in more detail later in this report. The purpose of these lists is to alert

the officer that a vehicle displaying a license plate number that is included on a hot list has been identified by the ALPR camera.

ALPR systems can be deployed in a variety of ways, including mobile ALPR systems, fixed ALPR systems, and portable ALPR systems.

Mobile ALPR Systems

Mobile ALPR systems use vehicle-mounted cameras to capture license plate data and can be configured in a number of ways to meet specific agency needs. Typically, the processor is located in the trunk of the vehicle and the data is processed locally to notify the officer of a possible hit. ALPR cameras are affixed to a vehicle and can be either hardwired or magnet-mounted for a portable (vehicle to vehicle) configuration. They can be integrated into the light bar, mounted on either the roof or trunk of the vehicle, or within covert housing.

Figure 6: Lightbar (left) and Covert (right) Mounted Mobile ALPR Cameras

System Portability. Mobile ALPR systems can be hardwired to a vehicle or magnet-mounted, for a portable (vehicle to vehicle) configuration. Magnet-mounted set-ups offer more flexibility and allow the agency to relocate the system from one vehicle to another. Consideration should be given, however, to the location of the hardware and connection cables on the various vehicle models and the ease with which they can be transferred. Agencies should weigh the pros and cons of each configuration against the technical and personnel resources of their agency.

Vehicle space availability. Mobile ALPR system components include cameras, processors, an interface screen, and keyboard which need to be added to a vehicle. Consideration should be given to the existing space limitations in both the vehicle cockpit and trunk.

Number of Cameras. Each camera added to the ALPR system on a vehicle provides an additional field of view and increases the amount of data and images the processor must analyze.

Data Transfer. A variety of methods exist to transfer hot list and ALPR data from the vehicle's computer processor. Consideration should be given to whether the agency plans to manually transfer the hot lists and data files using a USB memory stick or automate the transfer using wireless or cellular networks.

Fixed and Portable ALPR Systems

ALPR cameras that are permanently affixed to a structure such as a light pole, bridge, or overhead sign.

Figure 7: Stationary/Fixed ALPR Cameras on a Bridge and Utility Pole

Fixed and portable ALPR systems require an installation design plan that includes infrastructure to support the camera system.[33] This infrastructure includes power for the system and any networking that provides the ability to transmit data between the camera and the command/information center.

Some common considerations for fixed systems are:

- Existing physical infrastructure
- Site location
- Available power
- Available network infrastructure
- Number of cameras
- Dispatch requirements

Existing Physical Infrastructure. A great deal of physical infrastructure already exists at key locations along roadways or potential targets (e.g. sports stadium or power plant). Utilizing established infrastructure can offer a number of advantages such as reduction in costs associated with setting up a site, ease of access, and existing power connections. Consideration should be given however to the agency responsible for the infrastructure as special permits and ongoing maintenance may be required.

Site location. When choosing site locations for fixed and portable ALPR units, consideration should be given to whether officers will be routinely stationed nearby and their possible response times.

Available Power. Fixed and portable systems require power at the location of the camera. The need for power may limit the possible locations for mounting or require additional resources.

Available network infrastructure. Fixed and portable systems require network connectivity between the ALPR system's computer processor (generally located with the camera) and the server receiving database updates. The updates enable the processors at the camera location to identify vehicles of interest that have been recently entered into the databases. Agencies should consider how this network connectivity will be accomplished to ensure successful updates are received and how the information will be secured.

Dispatch requirements. Fixed and portable systems typically provide alert notifications to the communications/operations center. This increases the workload for the dispatch personnel. Depending on the system configuration, the ALPR system may require an additional computer screen for the dispatcher to monitor. Dispatch personnel need to be effectively trained and be able to include the associated actions into their existing responsibilities. It is also important to ensure that the dispatch facility has sufficient power and space for any additional computers or servers the ALPR system may require.

Number of cameras. A fixed system typically requires the installation of one camera for each lane of traffic being monitored. Multiple cameras at one location may improve the ability to locate a suspect or wanted vehicle.

ALPR Data

Collectively referred to as ALPR data, the images and the metadata associated with them are the primary forms of information collected by an ALPR system. The ALPR data may be stored in the individual ALPR units until it is either transferred to another server or discarded.

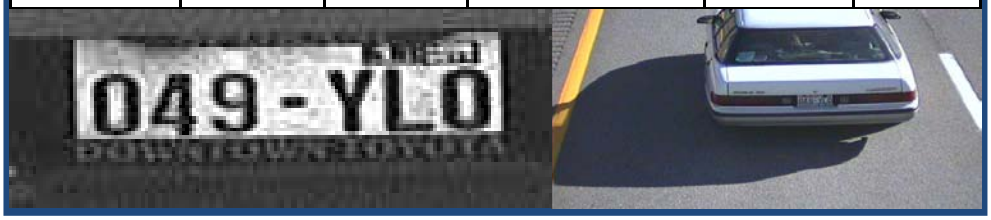
Data files compiled in ALPR systems typically contain the following information:

- Black and white plate image;
- Contextual color image;
- Electronically readable format of plate alphanumeric characters (optical character recognition (OCR)) of license plate numbers;
- Location and GPS coordinates;
- Time and date of image capture;
- Camera identification (mobile cameras may capture officer and vehicle/unit number).

The contextual image, sometimes referred to as an overview image, may capture additional identifying features of the vehicle such as make, model, color, bumper sticker, or damage. Additionally, it may capture the vehicle in the context of the ALPR camera field of vision, and provide information about the area immediately surrounding the vehicle and direction of travel.

Figure 8: Sample Data and Images Captured by ALPR

Site	Device	LPN	Timestamp	Lat.	Lon.
Post Falls PD	McGuire Fast Lane	049YLO	9/29/2010 9:30	47.71116	-116.98



ALPR Performance

A number of factors impact the performance of ALPR systems, and there are several measures that are relevant to the overall performance of the technology.[34]

1. Capture Efficacy – a measure of the effectiveness of ALPR units to capture the license plate information of vehicles that pass through the field of view of ALPR cameras. For example, if 100 cars pass the ALPR unit, what proportion/percentage of vehicles containing license plates are actually captured (i.e., read) by the ALPR units?

2. Read Accuracy – a measure of the accuracy of ALPR system interpretation of captured plates with the actual alphanumeric characters of the plate.

3. Matching Effectiveness – a measure of the effectiveness of ALPR units (really of their underlying software matching algorithms) to accurately match license plates *reads* to records contained in the agency's hot list(s). For example, if the ALPR unit accurately captures or reads only a portion of a vehicle's plate, or misreads one or more characters on a vehicle plate, is the unit (and its software) nevertheless able to match the plate with hotlist records stored or accessed through the device (perhaps with a scoring factor related to the probability of an actual match)? This is more a function of the software supporting the ALPR unit, the calibration of matching algorithms, and a measure of the performance and elasticity of search parameters.

4. Capture/Read Factors – there are a host of factors that may influence the ability of ALPR units to capture and accurately read and match license plates. Capture/Read factors include the following:
    a. Character and/or plate color
    b. Plate design factors (logos, stacked characters, etc.)
    c. State of origin (i.e., the state which issued the plate)
    d. Plate covers or other obstructions (e.g., bent, dirty, trailer hitch obstruction, etc.)
    e. Plate location on the vehicle
    f. Interval between vehicles

g. Vehicle speed
h. Lighting conditions (e.g., day vs. night)
i. Weather conditions (e.g., snow, rain, fog)
j. ALPR equipment (e.g., age and/or ability of the ALPR camera)
k. ALPR implementation (e.g., camera angle)

Plate design. Each state has multiple license plate designs and plates vary substantially from state to state. The shape of the characters, amount of contrast between a particular state's background and the color of the license plate characters, and whether the characters are raised or flat can all impact the accuracy of the OCR read. Some colors, especially reddish tones, may be difficult for ALPR system OCR software to read.

Figure 9: Sample Plate Designs

Poor image resolution. Poor image resolution can result from several factors. License plates can be too far away for the capabilities of the ALPR camera to capture and motion blur can also occur. Poor lighting and low contrast due to overexposure, reflection, adverse weather conditions, or shadows can also result in a poor image quality.

Figure 10: Poor Image Quality

Bent, dirty, damaged, or modified plates. Because many ALPR systems use reflectivity and the contrast created by the alphanumeric characters, plates that are bent, dirty, damaged, or modified may cause the ALPR software to misidentify a character.

Figure 11: Bent, Dirty, or Damaged Plates

Plate location. Occasionally, an object might obscure all or a portion of the license plate and interfere with accurate OCR. Oftentimes the object is a tow bar, dirt on the license plate, or a loaded bike rack; other times the object may be a ALPR circumvention device.

Figure 12: Obstructed Plates

The National Policing Improvement Agency (NPIA) and the Association of Chief Police Officers (ACPO) have specified minimum performance capabilities of ALPR technologies in capturing and reading license plate information for UK and Schengen Community plates.[35]

Table 3: 'Capture' and 'Read' rates for All United Kingdom (UK)[36]

Type of System	Capture Rate	Correct Read Rate	Overall capture & correct read rate
Static ANPR Camera	98%	95%	93.1%
CCTV Integrated ANPR (Dual purpose CCTV and ANPR Camera)	85%	85%	72.0%
Mobile ANPR Camera (Stationary)	98%	95%	93.1%
Mobile ANPR Camera (Moving)	80%	85%	68.0%

Given the fact that in static ALPR implementations the camera capturing the license plate is stationary, where as mobile implementations involve mobile cameras and potentially mobile target vehicles, variations in capture efficacy and read accuracy rates are expected and observed.

Slightly lower performance rates are acceptable for capturing and reading plates of just Schengen member countries.

Table 4: 'Capture' and 'Read' rates for All Schengen Community in Isolation of United Kingdom (UK) Number Plates[37]

Type of System	Capture Rate	Correct Read Rate	Overall capture & correct read rate
Static ANPR Camera	85%	80%	68.0%
CCTV Integrated ANPR (Dual purpose CCTV and ANPR Camera)	85%	80%	68.0%
Mobile ANPR Camera (Stationary)	85%	80%	68.0%
Mobile ANPR Camera (Moving)	75%	80%	60.0%

Law enforcement agencies in the United States must deal with license plates from other states, as well as international jurisdictions, which can pose difficulties if the units are not configured to "read" plates from multiple jurisdictions. ALPR manufacturers are constantly upgrading their equipment and software to address this issue.[38] Minimum performance standards for ALPR in the United States are still at an early stage. IACP is managing an NIJ-funded project to develop technical performance standards for ALPR systems. The goals of the project are to a) identify the specific performance parameters that are critical to ALPR functions, b) develop metrics to accurately measure their performance, and c) establish protocols for the testing of the equipment by an independent laboratory.[39]

Survey of ALPR Use by Law Enforcement

In order to assess the scope of current ALPR implementation, deployment, and operational uses among local, state and tribal law enforcement agencies throughout the United States, a random sample of 444 local, state, and tribal law enforcement agencies was selected from 2003 LEMAS sample agencies.[40]

Table 5: Distribution of Agency Size in Survey Sample

Agency Size (sworn)	Number	Percent
≤50	213	48.0%
51-100	77	17.3%
101-250	65	14.6%
251-500	29	6.5%
501-1000	30	6.8%
1001+	30	6.8%
Total	444	100.0%

The survey, which was administered in September 2009, was conducted in two phases. In the first phase, agencies were contacted to determine whether they were using an ALPR system and if so, to identify a program point of contact for further research. The full questionnaire (a copy of which can be found in Appendix C) was distributed in the second phase to the point of contact in agencies who had indicated they were currently using ALPR. Agencies were given a choice between completing the survey online or by paper. The survey was comprised of 29 questions addressing policy and technical issues, operational practices associated with mobile, fixed and portable deployments, and seeking a brief narrative discussion of lessons learned.

A total of 305 agencies responded to the first phase of the survey, providing a response rate of 68.7%. Of the jurisdictions responding, 235 agencies (77.0%) indicated that they were not using ALPR, while 70 agencies (23.0%) responded that they were using ALPR.

Table 6: Distribution of ALPR Usage by Agency Size (n=305)

	ALPR Use				
No. Sworn	No		Yes		Σ
≤ 50	128	89.5%	15	10.5%	143
51-100	46	79.3%	12	20.7%	58
101-250	28	80.0%	7	20.0%	35
251-500	17	77.3%	5	22.7%	22
501-1000	11	50.0%	11	50.0%	22
1001+	5	20.0%	20	80.0%	25
Total	235	77.0%	70	23.0%	305

As with other research assessing ALPR deployment by law enforcement agencies, this survey demonstrated that larger agencies were more likely to have implemented the technology. This survey, however, found substantially greater adoption of ALPR among smaller agencies than has been observed in earlier research. The 2007 LEMAS data indicate that none of the smallest agencies (50 or fewer sworn officers) had implemented ALPR, and only 7.4% of agencies of 100 or fewer officers having implemented ALRP (2 of 27 agencies). Lum, et. al., found that 3.4% of agencies with 100 or fewer officers had implemented ALPR, while the survey completed for this project shows 13.4% of agencies with 100 or fewer officers had adopted ALPR.

The longer, more detailed phase two survey was sent to the 70 agencies who confirmed they were using ALPR, of which 40 agencies (57.1%) responded.[41] Respondents were broadly arrayed throughout the nation.

Figure 13: Geographic Distribution of Survey Respondents

Nearly one-third (31%) of responding agencies were smaller (less than 100 sworn officers) and over half (53%) were larger agencies, with 500 or more sworn officers. Over half (60%) were municipal police agencies, and nearly one-quarter (23%) were Sheriff's officers.

Table 7: Distribution of Agency Size of Sample Respondents:

Agency Size (sworn)	n	%
25-49	7	18%
40-99	5	13%
100-249	5	13%
250-499	2	5%
500-999	10	25%
1000+	11	28%
Total	40	100%

Table 8: Distribution of Agency Type of Survey Respondents

Agency Type	n	%
Municipal	24	60%
Sheriff	9	23%
State	7	18%
Total	40	100%

The vast majority of agencies (95%) indicated that they had implemented mobile ALPR. Of the seven agencies that have implemented fixed ALPR, five reported using both mobile and fixed ALPR, and each of the five employed 1,000 or more sworn officers. Agencies are generally more likely to implement mobile ALPR deployments since the units can be easily moved from one vehicle to another (depending on the installation options selected by the agency), and by the very nature they can be quickly deployed to specific locations depending on the needs of the agency. Fixed implementations require more costly installation, permits from other agencies or organizations for installation (e.g., utility companies or departments of transportation, depending on the location), infrastructure to provide a continuous power source for the unit, communication channels to securely transmit the ALPR images, and periodic maintenance.

Table 9: Types of ALPR Systems Implemented

Type of ALPR Used	n	%
Mobile	38	95%
Fixed	7	18%
Portable	4	10%

Increasingly, agencies throughout the United States (and certainly in many other jurisdictions globally) are implementing both fixed and mobile ALPR systems. The city of Dallas, for example, recently released a request for proposals (RFP) for ALPR technology that includes 18 mobile systems (two for each of seven substations, two for the auto theft unit (one vehicle and one portable system), and one each for the gang unit and the internet crimes against children unit) and 30-50 fixed systems.[42] The agency indicated that they expect to improve their recovery of "stolen vehicles and identify amber alert vehicles, BOLO vehicles, missing persons, and sex offenders," as well as improve "intelligence gathering activities by providing back office software that allows for administration, data mining, reporting, data sharing, and intelligence gathering activities."[43]

Washington, D.C., has also implemented both fixed and mobile ALPR systems.[44] Although the agency first implemented ALPR in ten auto theft units, they have substantially expanded their program to include mobile, fixed, portable, and covert installations, and they provide real-time access to their ALPR data for other state and federal agencies after negotiating memoranda of understanding.

Locating and recovering stolen vehicles was the primary purpose for ALPR implementation in nearly two-thirds (62%) of responding agencies, followed by vehicle and traffic enforcement (28%) and investigations (25%).

Table 10: Primary Purposes for ALPR Implementation

Primary Purposes for ALPR	n	%
Auto theft	25	63%
Vehicle & traffic enforcement	11	28%
Investigations	10	25%
Identifying vehicles of interest	5	13%
Warrants	2	5%
Intelligence/homeland security	2	5%
Other	5	13%

Many of the agencies indicated that they had expanded their use of ALPR beyond their original purpose after implementation, most notably for auto theft (83%), general investigation (70%), and vehicle and traffic enforcement (50%).

Table 11: Current Uses of ALPR

Current Uses	n	%
Auto theft	33	83%
General investigation	28	70%
Vehicle & traffic enforcement	20	50%
Crime analysis	13	33%
Narcotics	11	28%
Gang Enforcement	8	20%
Smuggling	4	10%

Agencies report a broad range of business value in using ALPR, including increasing their recovery of stolen vehicles (68%), arrests (55%), and officer productivity (50%).

Table 12: Business Value of ALPR

Business Value	n	%
Increase stolen vehicle recoveries	27	68%
Increase in arrests	22	55%
Increase productivity	20	50%
Solving more crimes	14	35%
Other	8	20%

Law enforcement agencies around the world report substantial business and public safety benefits from use of the technology.[45] Montgomery County (MD) Police Department, for example, has indicated that a single officer equipped with ALPR scanned 48,101 plates, resulting in the issuance of 255 traffic citations, the identification of 26 drivers with suspended licenses, 16 vehicle emission violators, 4 stolen and 1 expired license plate tags, and 3 arrests in the course of 96 hours of use over 27 days.[46] The Automated Regional Justice Information Sharing system (ARJIS) reports that in a five day test of ALPR at the US/Mexico border, 780,000 plates crossed the border, and over 1,300 were involved in 4 murders, 14 rapes, 24 robberies, 273 assaults, 128 burglaries, 345 vehicle thefts, 361 weapons, and 241 narcotics cases.[47]

Police forces in the UK report similar business benefits in using ALPR technology:

"In the last financial year, the [North Yorkshire Police] force's ANPR team have seized £1,350,160 worth of stolen property, vehicles and drugs, summonsed 1,588 people to court and have made 88 arrests.

- 1,025 fixed penalty notices have been issued by the team, mainly for motoring offences.
- 523 vehicles have been seized for having no insurance, or because the driver [] did not have a valid licence.
- 88 people were arrested for offences including theft, drugs, burglary, motoring offences and people wanted on warrants.
- Over 700 vehicles or people have been searched."[48]

PERF conducted a randomized experiment to study the effects of LPR devices on auto theft, and concluded that "when LPRs were used, police were able to get over eight times as many checks, over four times as many hits, and about twice as many arrests and vehicle recoveries as when they were not using the LPR devices. The number of hits, arrests and recoveries were not particularly high, which is the result of a number of different factors, including the volume of crime. I also think the results show the difficulty of catching auto thieves in the act. By the time many cars are reported stolen, the thieves have already abandoned them, which poses a challenge."[49]

Fewer than half (43%) of responding agencies are part of a regional ALPR system, and only 40% report sharing ALPR data with any other agencies.

Table 13: Regional ALPR Program Participation

Part of a Regional System	n	%
Yes	17	43%
No	23	58%
Total	40	100%

Cincinnati is helping to build a regional ALPR sharing system known as SOSINK—Southwest Ohio/Southeast Indiana/Northern Kentucky.[50] SOSINK has two primary objectives: 1) increase apprehension of wanted subjects, and 2) collect intelligence and enhance investigations of wanted subjects, drug trafficking, and subjects on terrorist watch lists. They will implement over 80 fixed ALPR cameras on interstate highways in the region to provide alerts when subjects who are wanted, on terrorist watch lists, or suspected of drug trafficking enter or exit the region, as well as provide data regarding traffic patterns for further investigations.

ARJIS reports that they are sharing data with 23 agencies and growing.[51] Maryland is developing a statewide ALPR network, expanding from a base of 105 units implemented in fiscal years 2009-10, to 205 units in fiscal year 2011.[52] The state actually expected to have 242 mobile units and 53 fixed cameras (across seven sites), involving 32 agencies by December 2011.[53]

ALPR Policies

In order to be effective, ALPR technology must be properly implemented and integrated into the daily operations of law enforcement agencies. Developing and enforcing policies defining the strategic objectives of an agency's program, training requirements, deployment options, operating procedures, hot list management, proper use and maintenance of the technology, and data collection, retention, sharing, and access enables law enforcement to effectively manage ALPR.

Agency policies typically:

1. Define the ALPR system and its data as "for official use only" (FOUO),

2. Restrict and audit queries of the ALPR dataset, and

3. Require that all operators of the equipment receive proper training before use.[54]

Essential components of that training include:

1. Ensuring that appropriate hot list information is as current and accurate as possible, and

2. Clear directions that when the ALPR unit matches an observed vehicle's license plate with a record in the hot list and alerts the officer (also known as a "hit"), that the officer must verify
    a. that the ALPR "read" was accurate (i.e., that the ALPR OCR software has properly interpreted the license plate number),
    b. that the issuing State matches the plate on record, and
    c. that the circumstance that triggered the alert is still current, e.g., that the vehicle is still wanted or stolen.

3. If the record in the hot list was created based, not on the status of the vehicle, but rather on the status of the registered owner (e.g., the owner has an outstanding warrant for arrest, or has had their driving privileges suspended or revoked), the officer must also be cognizant of the fact that the driver may not be the registered owner.

4. Additionally, depending on the nature of the alert (e.g., a "hit" on the Terrorist Watch List), the officer may be directed to notify another agency (e.g., the Terrorist Screening Center) and hold the person, surreptitiously watch but not contact the person, or simply document the contact and forward the information to others.[55]

Nearly half of responding agencies (19 agencies, 48%) indicated that they had a policy addressing ALPR use and operations, and six agencies (15%) noted they were in the process of developing or planning one. Among agencies that have or are developing ALPR policies, the policies usually address data access (68%), data retention (48%), and data sharing (44%).

Table 14: Policy Issues Addressed by Agencies That Have or are Developing ALPR Policies (n=25):

Policy Issues	n	%
Data access	17	68%
Data retention	12	48%
Data sharing	11	44%
Deployment	6	24%
Data quality	4	16%
Other	4	16%

Hot List Management

Law enforcement agencies may create, access, and/or maintain any of a variety of lists of vehicles of interest, and these lists are universally known as "hot lists." Hot lists may include the license plate numbers of stolen vehicles, stolen license plates, vehicles owned or associated with wanted or missing persons, vehicles suspected of being involved in criminal or terrorist activities, owned by persons whose driver license has been suspended or revoked, and for any of a host of other legitimate purposes.[56]

Hot list information can come from a variety of sources, including stolen vehicle information from the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. Departments of Motor Vehicles can provide lists of expired registration tags and law enforcement agencies can also interface their own, locally-compiled hot lists (e.g., persons of interest, vehicles registered to wanted individuals) to the ALPR system. The purpose of these lists is to alert the law enforcement officer or system operator that a vehicle displaying a license plate number that is included on a hot list has been observed by an ALPR camera.

Information regarding hot list use and maintenance was gathered in our survey of law enforcement agencies. Over half (53%) of responding agencies indicated that their hot lists were updated wirelessly, either via cellular networks (28%) or using Wi-Fi/hotspots (25%). Over one-third (38%) of agencies use USB drives to upload hot list information to their mobile ALPR systems. Nearly half (43%) of agencies update their hot lists once each day, while over a quarter (28%) update their hot lists two or three times per day, or at each shift change.

Table 15: Hot List Update Methods

Hot List Updated by	n	%
USB drive	15	38%
Wi-Fi/Hotspot	10	25%
Cellular	11	28%
Other	4	10%

Table 16: Hot List Update Frequency

Hot List Updated	n	%
Once a day	17	43%
Twice a day	5	13%
Three times a day	2	5%
Each shift	4	10%
Multiple times per shift	6	15%
As needed	1	3%
No response	5	13%

What data sources agencies use for building and managing their hot lists varies widely, and depends in some measure on the operational objectives of the agency's ALPR deployment. Stolen vehicles and vehicle license plates are the most obvious and frequent sources of data contained in law enforcement hot lists (88% and 83%, respectively among agencies responding to our survey). Vehicles owned or operated by wanted persons, those associated with AMBER alerts, and those registered to drivers who have had their driving privileges suspended or revoked, or who have no valid insurance, also figure prominently in hot lists created or accessed by law enforcement.[57]

Table 17: Hot List Management

Hot List Content	n	%
Stolen vehicles	35	88%
Stolen plates	33	83%
Wanted persons	24	60%
AMBER alerts	18	45%
Suspend/Revoked Drivers	12	30%
No insurance	10	25%
Parking scofflaws	8	20%
Other	17	43%

Data Retention

ALPR systems store data regarding vehicle license plates they have read. As previously noted, license plate "read" records typically include information identifying the agency operating the technology, the camera which captured the read, the OCR interpretation of the license plate read, the date and time of the image capture, GPS coordinates (the latitude and longitude) of the vehicle plate at capture, and digital images of the license plate and a contextual photo of the vehicle.[58]

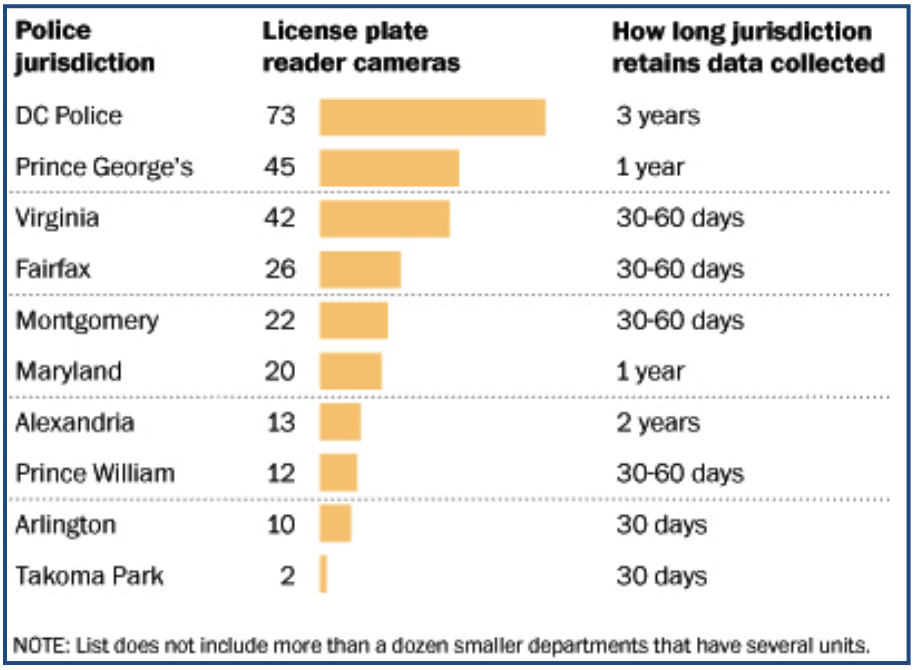
In addition to providing real-time alerts to officers and agencies when a vehicle on a hot list is identified, ALPR data are also a rich source of information for a variety of investigative operations. Depending on a jurisdiction's specific deployment of the technology, authorized law enforcement users could search ALPR records to identify vehicles that were recorded in a specific geographic region within a defined date and time range, or whether a particular vehicle was "observed" entering or leaving a geographic region. Police will often deploy ALPR-equipped vehicles to the scene of a crime, where they will canvas the surrounding neighborhood, scanning and recording vehicles which may help in identifying potential suspects and witnesses.

In addition to deploying ALPR-equipped units to geographic areas where crimes or other incidents of interest have occurred, law enforcement also use ALPR captured data to determine whether a vehicle of interest has been observed within a region covered by the technology. In one instance, local law enforcement was notified that an older, mentally ill citizen was missing. Combing though ALPR records captured during the week prior to the person's disappearance, the agency was able to identify numerous sightings of a vehicle that was registered as belonging to the missing citizen within a specific and narrow geographic region of the city. Officers were deployed to that region and quickly found the person, who was severely dehydrated and transported for medical attention.[59]

New York City deployed 238 ALPR systems (130 of which were mobile) by early 2011.[60] Washington D.C. and its suburbs have deployed over 250 ALPR cameras by late 2011.[61] Maryland is implementing a statewide ALPR program that was to include 242 mobile and 53 fixed ALPR units spread across 32 agencies by the end of 2011.[62] Dallas is currently (May 2012) in the process of procuring 18 mobile ALPR systems, and 30-50 fixed ALPR units.[63] The UK, as previously noted, has over 5,000 ALPR units deployed, capturing and reading approximately 10-12 million license plates per day, feeding a centralized data repository containing over 7 billion records.[64]

Jurisdictions vary widely in their ALPR data retention policies. Canada retains "hits" for two years, but limits retention of "non-hits" to no more than 90 days.[65] New Jersey allows retention of ALPR data for five years,[66] while Maine limits it to 21 days.[67] Law enforcement agencies in the Washington, D.C. region show similar diversity in their retention schedules, ranging from 30 days to 3 years.

Figure 14: ALPR Data Retention Practices in the Washington, D.C. Area[68]



Respondents to our survey demonstrated comparable diversity in their ALPR data retention policies.

Table 18: Data Retention Policies of Survey Respondents

Data Retention	n	%
No storage	2	5%
30 days or less	7	18%
2-6 months	7	18%
1 year	2	5%
2 years	2	5%
3-5 years	3	8%
Indefinitely	5	13%
Based on capacity	2	5%
In development	2	5%
Unknown	2	5%
No answer	6	15%
Total	40	100%

A total of 40% of respondents indicated they retain ALPR data for six months or less (n=16). Five respondents (13%) indicated they retain ALPR data indefinitely, while two indicated that retention is based on the storage capacity of the equipment they had installed.

Privacy concerns surrounding law enforcement use and retention of ALPR data have surfaced in many venues in recent years.[69] One of the key concerns is the fact that ALPR systems capture and record license plate information on all vehicles, regardless whether the driver is suspected of a crime or other violation. As Donna Lieberman, Executive Director, New York Civil Liberties Union, has noted, "It's one thing to have information about cars that are stopped for suspicious activity, but it's something else to basically maintain a permanent database of where particular cars go when there is nothing happening that is wrong and there is no basis for suspicion."[70]

One key issue is whether license plate data is considered "personally identifiable information" (PII). PII has been defined as "…any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, education, financial, and employment information."[71] McCallister, *et. al.,* define "linked" information as "information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual."[72]

The IACP completed a privacy impact assessment (PIA) of ALPR and concluded that ALPR data is not personally identifiable information.

> A license plate number identifies a specific vehicle, not a specific person. Although a license plate number may be linked or otherwise associated with an identifiable person, this potential can only be realized through a distinct, separate step (e.g., an inquiry to a Secretary of State or Department of Motor Vehicles data system). Absent this extra step, the license plate number and the time and location data attached to it are not personally identifying. Thus, even though LPR systems automate the collection of license plate numbers, it is the investigative process that identifies individuals.[73]

Although license plates function primarily to uniquely identify automobiles, many of the uses of ALPR necessarily involve acquiring information regarding the identity of the registered owner of the vehicle. The UK classifies ALPR data as "personal data" and follows the eight data protection principles articulated in their Data Protection Act.[74]

ALPR systems are typically deployed in public venues—on public streets, roadways, highways, and in public parking lots. As such, there is little "expectation of privacy" associated with observing a vehicle and its license plate numbers at a specific location, date and time.[75] Law enforcement is free to observe and even record information regarding a person's or a vehicle's movements in public venues. There are, however, key issues that may emerge when ALPR data is systematically collected and retained.

In *United States v. Jones*[76], which dealt with police attaching a global positioning system (GPS) tracking device to the defendant's vehicle in order to track his movements over the course of 28 days, the U.S. Supreme Court concluded that attaching the device to the defendant's vehicle was a "search" within the scope of the Fourth Amendment and, absent a warrant, the evidence obtained was inadmissible. Police had actually obtained a warrant, but they installed the device one day after the 10 day warrant had expired and in another jurisdiction (Maryland, instead of Washington, DC). Although the Court decided the case on the fairly narrow issue that by attaching the GPS tracking device to the undercarriage of Jones' vehicle, "[t]he Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[77] Justice Alito's concurring opinion (which was joined by Justices Ginsburg, Breyer, and Kagan) argues that the case should have been decided on whether Jones' "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[78]

Justice Sotomayor's concurring opinion discussed the evolving nature of technology and privacy expectations. "With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. [] In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance…. [T]he same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations."[79]

Although *Jones* dealt specifically with GPS tracking devices, the separate concurring opinions of five of the Justices reference the variety of evolving technologies that increasingly enable law enforcement to track and record the movement of persons and vehicles without requiring the installation of special tracking technologies. As jurisdictions expand their deployment of fixed and mobile ALPR systems, and build regional and statewide ALPR information sharing networks, they can rapidly amass a significant volume of data. Such expansive deployment and sharing of ALPR data retained for extended periods of time may well enable agencies to systematically track the movement of vehicles throughout a jurisdiction and beyond. Although there may be no reasonable expectation of privacy in any particular sighting of a vehicle traveling on a public roadway, the systematic capture, storage, and retrieval of ALPR data may nevertheless raise important privacy concerns.

In *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*[80], the U.S. Supreme Court recognized a difference between public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a centralized clearinghouse of information. The Court ruled that the electronic compilation of otherwise publicly available but difficult to obtain records, altered the privacy interest implicated by disclosure of that compilation.[81] Automation overwhelms what the Court referred to as the *practical obscurity*[82] associated with manually collecting and concatenating the individual public records associated with a particular person into a comprehensive, longitudinal criminal history record.

ALPR records may be implicated when agencies systematically capture and record these independent public records and assemble them into a longitudinal file or provide the ability to analyze them as such. The technological convergence that enables the systematic collection, concatenation, and analysis of such massive datasets may challenge established concepts of what is public, what is private, and what is a "reasonable expectation of privacy." What ALPR data is collected, how the data is collected, how long the data are retained, who can access the data and for what purposes, and what kind of analytic tools and methodologies are available to query and analyze ALPR data are all critical issues that may impact public acceptance and legal approval.[83]

Creating and enforcing a comprehensive agency policy, which addresses ALPR objectives, deployment, records management, data quality, hot list management, systems security, data retention and purging, access and use of stored ALPR data, information sharing, accountability, and sanctions for non-compliance can help to ensure that data are properly collected, used, and managed. New Jersey, which retains data for five years, has a comprehensive ALPR policy "to ensure that ALPRs are used only for *bona fide* law enforcement purposes, and that the data collected by these devices are used in accordance with substantive standards and procedural safeguards that appropriately balance the need for law enforcement agencies to prevent and respond to terrorism and other forms of crime against the legitimate privacy interests of persons operating motor vehicles on the roadways of this State."[84] The state differentiates between "positive alert data" and "non-alert data," and specifically restricts and audits access to non-alert data.[85]

Relatively short data retention periods were once necessitated by physical storage constraints. Technological advances, declining costs, and new computing paradigms have vastly expanded the digital storage capacity of modern computers and information systems.[86] Whether to retain a piece of information or an entire dataset for a month, a year, five years, or indefinitely is now more a matter of policy than physical limitations of technology. As a consequence, developing data retention policies requires consideration of a variety of factors, including privacy concerns associated with ALPR data.

There is no established formula for determining how long ALPR data should be retained, nor have national standards or guidelines been established that agencies can refer to as they develop ALPR data retention policies. The IACP has developed a *Model Policy: License Plate Readers*[87], but given the disparity between agencies and jurisdictions in ALPR data retention policies and practices, the model policy does not recommend a specific data retention schedule. Given the lack of professional standards in this area, and the broad diversity in ALPR data retention policies and practices observed throughout the nation, IACP has developed some general points for consideration that agencies should review in developing ALPR policies. These points of consideration are based on input from a host of operational practitioners, as well as site visits to 10 law enforcement agencies that had implemented and used ALPR for one or more years as part of this project.[88]

State and local data retention schedules. State and local data retention schedules supersede retention periods established by individual entities. Even where there are no state or local guidelines directly focused on ALPR, existing guidelines related to comparable forms of electronic data and imaging systems may be applicable to ALPR systems.

System type. The type of ALPR system an agency uses may also play a factor in determining retention policies. Fixed ALPR systems, for example, typically capture more license plate reads in a day than mobile or portable ALPR systems. As a consequence, some agencies that use more than one system type establish different retention schedules for each type of deployment, with longer retention periods for mobile and/or portable ALPR systems and shorter periods for fixed ALPR systems.

Situational realities. Political, social, technical, and financial realities are different in every jurisdiction, and each must be weighed against the other and combined with the business needs and priorities of the agency. Where the social and political climate is more favorable to law enforcement's use of ALPR systems, a longer retention period may be possible. Longer retention periods generally require more technical and financial resources for support, however, and agency objectives and priorities in the use of ALPR data should substantively contribute to decisions regarding retention duration.

Loss of value over time. Historical data may lose value over time due to the sale and transfer of automobiles or the ability to obtain information from other governmental departments.

Statutes of limitations. Consideration should also be given to the mission of the agency and to the operational objectives of the ALPR deployment. If the ALPR data are associated with a crime that is subject to a statute of limitations, then an agency may want to set a retention period relative to that statute.

Potential evidentiary value. Potential evidentiary value may not only affect the length of retention but *how* the data are retained. For example, during an investigation it may be determined that the ALPR data could be valuable at a later point. In such a case, a query for all ALPR data within a certain time frame relative to the incident could be run, and the results saved to a CD or thumb drive and placed in the case file so they are available at a later date even if the original data have already been discarded. In this case, while saved ALPR data are no longer subject to the original retention period, they may still be subject to policies regarding evidentiary practices. All ALPR confirmation paperwork (hardcopy and/or electronic) that initiates law enforcement action should be retained until all possible court action has been exhausted, including criminal and civil appeal processes.

Appendix A includes sample ALPR policies from several jurisdictions. These sample policies address a broad range of ALPR implementation, training, technical support, operational uses, data quality and security, data accessibility and use, and data retention practices.

In addition to sample agency policies, a supplemental report, *Privacy issues concerning the utilization of automated license plate readers*[89], previously prepared by IACP as part of the privacy impact assessment for ALPR, may also provide guidance in developing policies governing ALPR operations. Readers are encouraged to review and address questions posed in the report in developing ALPR policies for their agencies.

Conclusion

ALPR technology is a significant tool in the arsenal of law enforcement and public safety agencies. It automates a tedious, distracting, and manual process that officers regularly complete in their daily operations, and vastly improves their efficiency and effectiveness in identifying vehicles of interest among the hundreds or thousands they observe in routine patrol. Moreover, it generates a rich and enduring record of vehicle sightings, complete with time, date, and geographic location information for each observation. This data can substantially enhance the investigative capacity of law enforcement, and greatly contribute to intelligence collection and analysis functions.

Realizing the core business values that ALPR promises, however, can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all tools and technologies available to law enforcement, ALPR must also be carefully managed. Agencies must clearly articulate their strategic goals and tactical objectives for the technology, and this strategy should be tightly aligned with the broader strategic plans of the agency. Thorough and ongoing training is required to ensure that the technology performs effectively, and that users are well versed in the operational policies and procedures defined and enforced by the agency.

Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system, and reassure the public that their privacy interests are recognized and respected.

Endnotes

[1] Automated license plate recognition (ALPR) technology is variously referred to as license plate readers (LPR), automatic number plate recognition (ANPR, primarily in the UK), automatic vehicle identification (AVI), and car plate recognition (CPR). ALPR is fairly commonly used throughout the United States, however, and for purposes of this report it will be used throughout.

[2] Depending on the state, the central government office registering motor vehicles and issuing license plates may be a separate bureau, division, department, or other office, or they may be part of a larger governmental agency (e.g., Florida Department of Highway Safety and Motor Vehicles).

[3] In Virginia, for example, the Code of Virginia, §46.2-600, specifies: "Except as otherwise provided in this chapter every person who owns a motor vehicle, trailer or semitrailer, or his authorized attorney-in-fact, shall, before it is operated on any highway in the Commonwealth, register with the Department and obtain from the Department the registration card and certificate of title for the vehicle. Individuals applying for registration shall provide the Department with the residence address of the owner of the vehicle being registered. A business applying for registration shall provide the Department with the street address of the owner or lessee of the vehicle being registered." Code of Virginia §46.2-716, A specifies that plates must be "securely fastened to the motor vehicle, trailer, or semitrailer…1. So as to prevent the plate from swinging, 2. In a position to be clearly visible, and 3. In a condition to be clearly legible." The code goes on to specify that "No colored glass, colored plastic, bracket, holder, mounting, frame, or any other type of covering shall be placed, mounted, or installed on, around, or over any license plate if such glass, plastic, bracket, holder, mounting, frame, or other type of covering in any way alters or obscures (i) the alpha-numeric information, (ii) the color of the license plate, (iii) the name or abbreviated name of the state wherein the vehicle is registered, or (iv) any character or characters, decal, stamp, or other device indicating the month or year in which the vehicle's registration expires. No insignia, emblems, or trailer hitches or couplings shall be mounted in such a way as to hide or obscure any portion of the license plate or render any portion of the license plate illegible." Code of Virginia §46.2-716, B.

Currently 31 states and the District of Columbia require vehicles to display two license plates—one on the front of the vehicle and one on the back; 19 states (Alabama, Arizona, Arkansas, Delaware, Florida, Georgia, Indiana, Kansas, Kentucky, Louisiana, Michigan, Mississippi, New Mexico, North Carolina, Oklahoma, Pennsylvania, South Carolina, Tennessee, and West Virginia) mandate only a single plate on the rear of the vehicle. http://dmvanswers.com/questions/354/Am-I-required-to-have-license-plates-on-the-front-and-back-of-my-car accessed June 4, 2012.

[4] http://deldot.gov/information/media_gallery/2008/centennial_plates/license_plate_history.shtml, accessed June 4, 2012. It has been noted elsewhere that "these plates were made by individual owners (with the owner's initials) rather than state-issued plates." Massachusetts is credited with being the first state to actually issue license plates to vehicle owners in 1903. http://history1900s.about.com/od/1900s/qt/licenseplates.htm, accessed June 4, 2012.

[5] http://deldot.gov/information/media_gallery/2008/centennial_plates/de_license_plate_history.shtml, accessed June 4, 2012.

[6] Nancy Keates, "What Drives People to Take a Creative License?" *Wall Street Journal*, June 23, 2011, at http://online.wsj.com/article/SB10001424052702303745304576359910386002034.html?mod=WSJ_hpp_MIDDLE_Video_Top, accessed June 4, 2012.

[7] http://www.cbsnews.com/2100-18563_162-3994634.html, accessed June 4, 2012.

[8] Plate images acquired from http://www.15q.net/usindex.html, accessed June 4, 2012.

[9] http://ctplates.info/ct_vanity.php, accessed June 4, 2012.

[10] http://ftp.txdmv.gov/pub/txdot-info/vtr/slp_brochure.pdf accessed June 4, 2012.

[11] Nancy Keates, "What Drives People to Take a Creative License?", *Wall Street Journal*, June 23, 2011, at http://online.wsj.com/article/SB10001424052702303745304576359910386002034.html?mod=WSJ_hpp_MIDDLE_Video_Top, accessed June 4, 2012. For more detail regarding state statutes addressing licensing and specialty plates, see Bill Kenworthy, "State-by-state statutes governing license plates," January 20, 2006, at http://archive.firstamendmentcenter.org/analysis.aspx?id=16337, accessed June 4, 2012.

[12] Images retrieved from http://www.myplates.com/, accessed June 4, 2012.

[13] Images retrieved from http://www.mvd.newmexico.gov/Vehicles/Pages/License-Plates.aspx#Personalized, accessed June 4, 2012.

[14] Travis Crum, "Special license plates bring in $1.2 million for State Road Fund," *The Charleston Gazette*, May 29, 2011, at http://wvgazette.com/News/201105291075, accessed June 4, 2012.

[15] Katharine Lackey, "States look at corporate plates to help with deficits," *USA Today*, at http://www.usatoday.com/news/nation/2010-11-04-license-plates_N.htm, accessed June 4, 2012.

[16] Robin Hindery, "Calif. License plates might go digital, show ads for revenue," Associated Press, *USA Today*, at http://www.usatoday.com/tech/news/2010-06-22-calif-license-plates_N.htm, accessed June 4, 2012.

[17] The America's Missing: Broadcast Emergency Response (AMBER) system was created in 1996 as an early warning system designed to help immediately broadcast information on missing and abducted children. http://www.amberalert.gov/ accessed June 4, 2012.

[18] Be on the lookout, or BOLO alerts, provide the names and indentifying information on individuals who are of investigative interest to law enforcement agencies. http://www.fbi.gov/news/testimony/terrorism-preparedness-2, accessed June 4, 2012.

[19] Many references indicate that PSDB developed ANPR in 1976 (see, e.g., Ch. Jaya Lakshmi, A. Jhansi Rani, K. Sri Ramakrishna, and M. KatiKiran, "A Novel Approach for Indian License Plate Recognition System," 6 *International Journal of Advanced Engineering Sciences and Technologies*, 10-14, 2011, at http://ijaest.iserp.org/archieves/9.2-A16-30-11/Vol-No.6-Issue-No.1/3.IJAEST-Vol-No-6-Issue-No-1-A-Novel-Approach-for-Indian-License-Plate-Recognition-System-010-014.pdf, accessed June 4, 2012; "Drivers on police files for life," *This is Cornwall*, June 30, 2009, at http://www.thisiscornwall.co.uk/Drivers-police-files-life/story-11398048-detail/story.html, accessed April 30, 2012), though these and many others appear to quote liberally the brief developmental history of ALPR posted on Wikipedia: "ANPR was invented in 1976 at the Police Scientific Development Branch in the UK. Prototype systems were working by 1979, and contracts were let to produce industrial systems, first at EMI Electronics, and then at Computer Recognition Systems (CRS) in Wokingham, UK. Early trial systems were deployed on the A1 road and at the Dartford Tunnel. The first arrest through detection of a stolen car was made in 1981." http://en.wikipedia.org/wiki/ANPR#Development_history, accessed June 4, 2012.

[20] Protection of Freedoms Bill, Memorandum Submitted by the European Secure Vehicle Alliance (ESVA) (PF 11), Session 2010-11, at http://www.publications.parliament.uk/pa/cm201011/cmpublic/protection/memo/pf11.htm, accessed June 4, 2012, referencing John Coaffee "Rings of Steel, Rings of Concrete and Rings of Confidence: Designing out Terrorism in Central London pre- and post September 11th," *International Journal of Urban and Regional Research*, Vol 28, Number 1, 2004.

[21] PA Consulting Group, *Police Standards Unit: Thematic review of the use of automatic number plate recognition within police forces*, December 2006, at http://gemini.gmu.edu/cebcp/LPR/Thematic_Review_of_ANPR_v2[1].pdf, accessed June 4, 2012.

[22] ACPO, *ANPR Strategy for the Police Service – 2010-2013*, at http://www.acpo.police.uk/documents/crime/2010/201010CRIANP01.pdf, p. 6, accessed June 4, 2012. This strategic intent has changed only slightly from the original intent, which was announced in 2005 as "Denying Criminals the Use of the Roads," ACPO ANPR Steering Group, *ANPR Strategy for the Police Service – 2005/2008,* March 2005.

[23] PA Consulting Group, *Police Standards Unit: Thematic review of the use of automatic number plate recognition within police forces*, December 2006, at http://gemini.gmu.edu/cebcp/LPR/Thematic_Review_of_ANPR_v2[1].pdf, accessed June 4, 2012, at p. 59.

[24] ACPO, *ANPR Strategy for the Police Service—2012-2013*, (2010) at http://www.acpo.police.uk/documents/crime/2010/201010CRIANP01.pdf, pp. 9 and 11, accessed June 4, 2012.

[25] The Law Enforcement Management and Administrative Statistics (LEMAS) survey is conducted every 3-4 years by the Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice. LEMAS "collects data from over 3,000 state and local law enforcement agencies, including all those that employ 100 or more sworn officers and a nationally representative sample of smaller agencies. Data are obtained on the organization and administration of police and sheriffs' departments, including agency responsibilities, operating expenditures, job functions of sworn and civilian employees, officer salaries and special pay, demographic characteristics of officers, weapons and armor policies, education and training requirements, computers and information systems, vehicles, special units, and community policing activities." *See*: http://bjs.ojp.usdoj.gov/index.cfm?ty=dcdetail&iid=248, accessed June 4, 2012.

[26] These figures were tabulated online from the LEMAS 2007 dataset (Section VI-Equipment, question 32, LPREADER) accessible through the National Archive of Criminal Justice Data. http://www.icpsr.umich.edu/icpsrweb/NACJD/series/92, accessed June 4, 2012.

[27] This map was generated based on the analysis of the LEMAS 2007 dataset, as noted above.

[28] Cynthia Lum, Linda Merola, Julie Willis, and Breanne Cave, *License Plate Recognition Technology (LPR): Impact Evaluation and Community Assessment*, (Fairfax, VA: George Mason University Center for Evidence-Based Crime Policy, September 2010), http://gemini.gmu.edu/cebcp/LPR_FINAL.pdf, accessed June 4, 2012. 2007 LEMAS data were not available at the time of their study.

[29] *Id*, at p. 19.

[30] PERF, *Critical Issues in Policing Series. How Are Innovations in Technology Transforming Policing?* Washington, DC: PERF), January 2012. http://policeforum.org/library/critical-issues-in-policing-series/Technology_web.pdf, and PERF, *Use of Technology in Policing: The Chief's Perspective*, Washington, DC: PERF), April 4, 2011, http://www.policeforum.org/library/critical-issues-in-policing-series/perfpresentation.pdf, accessed June 4, 2012.

[31] See, e.g., Declan *Measuring Cross-Border Travel Times for Freight: Otay Mesa International Border Crossing*, March 31, 2008, at http://www.ops.fhwa.dot.gov/publications/fhwahop10051/index.htm; Virginia Department of Transportation, *Tolling Facilities Report, HB 3302 (2007)*, at http://virginiadot.org/projects/resources/TollingReportforVDOTwebsite.pdf; Apex Design, *Draft Concept of Operations for the US 36 Managed Lane*, August 4, 2011, at http://www.coloradodot.info/programs/high-performance-transportation-enterprise-hpte/projects/us-36-hpte-projects/us-36-managed-lanes/IGA%20Phase%20I%20US%2036%20Project%20Executed%20with%20Exhibits.pdf,; Andrew Eberline, *Cost/Benefit Analysis of Electronic License Plates, Final Report 637*, June

2008, at http://www.azdot.gov/TPD/ATRC/publications/project_reports/PDF/AZ637.pdf; Department for Transport, Case Study: London Congestion Charging, June 2, 2010, at http://www.dft.gov.uk/itstoolkit/CaseStudies/london-congestion-charging.htm; Fran Spielman, "O'Hare upgrade would let you find and pay for parking with your phone," *Chicago Sun Times*, May 4, 2012 at http://www.suntimes.com/news/12318425-418/ohare-upgrade-would-let-you-find-and-pay-for-parking-with-your-phone.html, "Uninsured Drivers Targeted," *Mearns Leader*, April 13, 2012, at: http://www.mearnsleader.co.uk/community/uninsured-drivers-targeted-1-2230630#; "Uninsured drivers targeted in police crackdown," *Banffshire Journal*, UK, April 5, 2012, at http://www.banffshire-journal.co.uk/News/Uninsured-drivers-targeted-in-police-crackdown-05042012.htm, all accessed June 4, 2012.

[32] http://www.elsag.com/faqs.htm, http://pipstechnology.com/news/faq/, http://www.vigilantvideo.com/index.html, accessed June 4, 2012

[33] For a detailed overview and presentation on fixed ALPR, see Chris Morgan, John Gaw, Sam Paul, *Fixed ALPR "Best Practices"*, presentation at the 2011 IACP LEIM Conference, San Diego, California, June 15, 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/Fixed_ALPR_Best_Practice-Final.pdf, accessed June 4, 2012.

[34] Jim Kennedy, "Step up to the plate," *Thinking Highways*, Vol. 4, No. 1, pp. 40-42, 2009 at http://thinkinghighways.com/Pages/View-issue/View-issue-page.aspx?id=cbd7c667-4536-469b-8670-854bfd3ac23b, accessed June 4, 2012. Also see, Space and Naval Warfare Systems Center Atlantic, System Assessment and Validation for Emergency Responders (SAVER), *Mobile License Plate Recognition Systems Assessment Report*, (Washington, DC: Department of Homeland Security, September 2009, Revision 1).

[35] National Policing Improvement Agency (NPIA), *National ACPO ANPR Standards (NAAS),* version 4.12, November 2011, at http://www.acpo.police.uk/documents/crime/2011/201111CBANAAS412.pdf, accessed June 4, 2012. For more information regarding Schengen, and the 25 members countries, see http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm, accessed June 4, 2012.

[36] *Id*, at p. 12.

[37] *Id*, at p. 13.

[38] *See, e.g.,* Tim Dees, "New Development in ALPR," *Police Magazine*, February 2011, at http://www.policemag.com/Channel/Technology/Articles/Print/Story/2011/02/New-Developments-In-ALPR.aspx, accessed June 4, 2012.

[39] In addition to ALPR technology, the project also supports the development of performance standards for interview-room video technology. IACP Video Standards for Law Enforcement, Project number 2009-IJ-CX-K009.

[40] Although the initial sample was 500 agencies, agency size was not known in 56 of the agencies, who were subsequently dropped from the sample.

[41] It should be noted that in follow-up conversations, many of the 30 agencies that had indicated they had implemented ALPR but did not respond to the phase two survey, explained that they had only recently begun to use ALPR.

[42] The City of Dallas, Texas, *Request for Competitive Sealed Proposal, BHZ1217, DPD Mobile and Fixed Automatic License Plate Recognition (ALPR System),* http://www.scribd.com/doc/88124473/Rfcsp-Dpd-Alpr-System-Ver1-0#outer_page_3, accessed June 4, 2012

[43] *Id*., at p. 96.

[44] Lisa Sutter, *The Metropolitan [DC] Police Department: Our LPR Experience,* presentation at the 2011 IACP LEIM Conference, San Diego, California, June 15, 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/District-of-Columbia-Metropolitan-Police-Department-Presentation_6-15-11.pdf, accessed June 4, 2012

[45] "Travelling criminals hit hard by ANPR team," North Yorkshire Police, UK, April 20, 2012, accessed at http://www.northyorkshire.police.uk/index.aspx?articleid=8593. Robert Wilonsky, "Dallas PD intends to use license-plates [sic] readers to catch criminal now and gather 'information' for use later," *The Dallas Morning News,* April 5, 2012, accessed June 4, 2012 at http://crimeblog.dallasnews.com/archives/2012/04/dallas-pd-intends-to-use-licen.html; Jay Boreham, "Snapped and nabbed," Manukau Courier, AU, April 17, 2012, accessed June 4, 2012 at http://www.stuff.co.nz/auckland/local-news/manukau-courier/6754667/Snapped-and-nabbed.

[46] Sebastian Montes, "MCPD Wants to Keep License Plate Data Indefinitely," Wheaton Patch, April 11, 2012, at http://wheaton-md.patch.com/articles/mcpd-wants-to-keep-license-plate-data-indefinitely-76216f6d, accessed June 4, 2012.

[47] Julio Valcarcel and Dale Stockton, *ARJIS Regional License Plate Reader Sharing,* presentation at the 2011 IACP Law Enforcement Information Management (LEIM) Annual Conference, San Diego, California June 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/ARJIS_LEIM2011.pdf, accessed June 4, 2012.

[48] North Yorkshire Police (UK), "Travelling criminals hit hard by ANPR Team," April 20, 2012, accessed June 4, 2012 at http://www.northyorkshire.police.uk/index.aspx?articleid=8593

[49] Comments by Christopher Koper, PERF, *Critical Issues in Policing Series: "How Are Innovations in Technology Transforming Policing?"* (Washington, D.C.: PERF, 2012), p. 30, at http://policeforum.org/library/critical-issues-in-policing-series/Technology_web.pdf, accessed June 4, 2012. For a report of the actual study, see Bruce Taylor, Christopher Koper, Daniel Woods, "Combating Vehicle Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology," *Criminal Justice Review*, November 14, 2011, at http://cjr.sagepub.com/content/early/2011/11/09/0734016811425858, accessed June 4, 2012.

[50] Russell A. Neville, "Cincinnati Regional Automatic License Plate Recognition Technology Project," *The Police Chief Magazine,* vol. LXXVI, no. 6, June 2009, at http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1823&issue_id=62009, accessed June 4, 2012

[51] Dale Stockton and Dan Gomez, *Automated License Plate Recognition: Interoperability and Policy and Procedures,* presentation at the 2011 IACP LEIM Annual Conference, San Diego, California June 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/LEIM-2011-San-Diego-Final.pdf, accessed June 4, 2012

[52] State of Maryland, *Automated License Plate Reader Technology Security Integration Strategy,* August 2010, at http://www.governor.maryland.gov/documents/100804LPRPlan.pdf, p. 5, accessed June 4, 2012

[53] Julio Valcarcel, *Maryland's LPR Program and Policy Overview,* presentation presented at the 2011 IACP LEIM Conference, June 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/Maryland's-LPR-Program-and-Policy-Overview.pdf, at slide 5, accessed June 4, 2012

[54] See, e.g., South Portland Police Department, *Standard Operating Procedures: Automated License Plate Reader (ALPR),* Policy # 8-82-F, September 20, 2010, http://www.maine.gov/sos/SPPD-SOP.pdf; New York State Division of Criminal Justice Services, *Operation of License Plate Readers for Law Enforcement Agencies in New York State: Suggested Guidelines*, June 2007 http://www.elsag.com/media/content/NYDCJS%20LPR%20Policy.pdf; New York State Division of Criminal Justice Services, *Suggested Guidelines: Operation of License Plate Reader Technology*, 2011, http://criminaljustice.state.ny.us/ofpa/pdfdocs/finallprguidelines01272011a.pdf; Campbell Police Department, *Automated License Plate Readers: Policy 462*, 2010. http://www.ci.campbell.ca.us/AgendasMinutes/2010/ca04062010/Item%2008.pdf; Charlotte-Mecklenburg Police Department, *Standard Operating Procedure: License Plate Reader*, April 29, 2011, http://gemini.gmu.edu/cebcp/Charlotte-Mecklenberg%20SOP.pdf; International Association of Chiefs of Police, *Model Policy: License Plate Readers*, August 2011 http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223; Paula T. Dow, *Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data*, Directive No. 2010-5, December 3, 2010, at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf; and Kent Police, *G10 Automatic Number Plate Recognition (ANPR),* July 2010, http://www.kent.police.uk/about_us/policies/g/g10.html, all accessed June 4, 2012.

[55] The different types of law enforcement response described here are discussed in the Charlotte-Mecklenburg Police Department SOP, *op. cit.*, at p. 4, for three levels of Terrorist identified by Terrorist Screening Center in their Terrorist Watch List. In addition, officers are instructed to contact the Terrorist Screening Center by telephone, not by radio.

[56] The South Portland (ME) Police Department, for example, identifies the following sources of hot list information:

"a) NCIC Stolen Vehicle files, as available; b) NCIC Stolen plates and Stolen Canadian plates, as available; c) NCIC Wanted persons, as available; d) NCIC Missing or Endangered person files, as available; e) NCIC Federal Immigration Violators, as available; f) NCIC Supervised Release (Federal Probationers), as available; g) NCIC Nationwide Domestic Violence Protection Orders, as available; h) NCIC Violent Gang and Terrorist Organization File, as available; i) NCIC Sexual Offender; j) BMV records of Suspended Drivers / Habitual Offenders and / or Suspended Registrations, as available; k) and Official BOLOs or alerts, based on specific and articulable facts of a concern for safety, wrongdoing or a criminal investigation, or pursuant to a civil order (e.g., PFA or PHA) or official law enforcement bulletin or teletype (e.g., vehicles associated with crime incidents, suicidal, homicidal, missing or wanted persons, AMBER ALERTS, stolen vehicles, or similar vehicles of interest)." South Portland Police Department, *Standard Operating Procedures, ALPR, Policy # 8-82-F*, September 20, 2010, at p. 8-82-F-2, at http://www.maine.gov/sos/SPPD-SOP.pdf, accessed June 4, 2012.

[57] For examples of the types of files and data included in other agency hot lists, see Norm Gaumont and Dave Babineau, "The Role of Automatic License Plate Recognition Technology in Policing: Results from the Lower Mainland of British Columbia," *Police Chief Magazine*, vol. LXXV, no. 11, November 2008; Washington Association of Sheriffs and Police Chiefs, *Guidelines for Washington State Law Enforcement: Operation of Automated License Plate Readers*, September 2008, p. 5; Russell Neville, "Cincinnati Regional Automatic License Plate Recognition Technology Project," *The Police Chief Magazine*, vol. LXXVI, no. 6, June 2009.

[58] National Policing Improvement Agency (UK), *National ACPO ANPR Standards (NAAS),* version 4.12, November 2011, also identifies these data elements as part of the ANPR data output, as well as possibly a confidence level of the accuracy of the 'read' (similar to AFIS systems), and the CCTV (closed-circuit television) preset value (for CCTV ANPR systems). http://www.acpo.police.uk/documents/crime/2011/201111CBANAAS412.pdf, p. 14, accessed June 4, 2012.

[59] Personal correspondence with Daniel J. Murray, Deputy Chief of Police, Arlington County (VA) Police Department, July 8, 2010. "Missing Endangered Adult, Found/ 10070xxxx/ At 1750 hours Detective [XXXX] broadcast for a missing adult, 67 years of age, suffering from mental illness. An associated vehicle was also broadcast. Detective [XXXX] of the Auto [Theft] unit ran the registration through the LPR system history and discovered that the tag was read 6 times in the last few days in the XXXX block of S. XXXX St. He notified Officer [XXXX] who began to search the area. The victim was located in front of Fire Station #[XXXX] and was in a severe state of dehydration. He was transported to VHS and family was notified. (XXXX, XXXX, XXXX)."

[60] Al Baker, "Camera Scans of Car Plates are Reshaping Police Inquiries," *The New York Times,* April 11, 2011, at http://www.nytimes.com/2011/04/12/nyregion/12plates.html?pagewanted=all, accessed June 4, 2012.

[61] Allison Klein and Josh White, "License plate readers: A useful tool for police comes with privacy concerns," *The Washington Post*, November 19, 2011, at http://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html, accessed June 4, 2012

[62] Julio Valcarcel, *Maryland's LPR Program and Policy Overview,* presentation presented at the 2011 IACP LEIM Conference, June 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/Maryland's-LPR-Program-and-Policy-Overview.pdf, at slide 5, accessed June 4, 2012.

[63] The City of Dallas, Texas, *Request for Competitive Sealed Proposal, BHZ1217, DPD Mobile and Fixed Automatic License Plate Recognition (ALPR System),* http://www.scribd.com/doc/88124473/Rfcsp-Dpd-Alpr-System-Ver1-0#outer_page_3, accessed June 4, 2012.

[64] ACPO, *ANPR Strategy for the Police Service—2012-2013*, (2010) at http://www.acpo.police.uk/documents/crime/2010/201010CRIANP01.pdf, pp. 9 and 11, accessed June 4, 2012.

[65] Gaumont, *op. cit.*

[66] *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored Data,* (Trenton, NJ: Office of the Attorney General), Issued December 3, 2010; Effective January 18, 2011, at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf, accessed June 4, 2012.

[67] Me. Rev. Stat. Ann. tit. 29-A, §2117-A (Use of automated license plate recognition systems), at http://www.mainelegislature.org/legis/statutes/29-A/title29-Asec2117-A.html, accessed June 4, 2012

[68] Klein and White, *op. cit.*, at http://www.washingtonpost.com/local/2011/11/05/gIQAoWGdqM_graphic.html, accessed June 4, 2012.

[69] David Riley, "License plate readers help police, worry privacy groups," Taunton Daily Gazette, July 6, 2011, at http://www.tauntongazette.com/news/x1860262823/License-plate-readers-help-Mass-police-worry-privacy-groups; John Lender, "As Use of License Plate Scanners Spreads, Privacy Concerns Deepen" (Harford Courant, April 21, 2012), at:http://www.courant.com/news/politics/hc-lender-column-plate-scanners-0422-20120421,0,7896326.column; Ontario Information and Privacy Commissioner, Privacy Investigation: The Toronto Police Service's use of Mobile License Plate Recognition Technology to Find Stolen Vehicles, (Toronto, Ontario: Information and Privacy Commissioner), April 29, 2003, at http://www.ipc.on.ca/images/Findings/up-mc_030023_1.pdf; Basich, op. cit.; and Klein and White, op. cit., all accessed June 4, 2012.

[70] Quoted in Baker, op. cit. Similar concerns have been expressed in other geographies addressing ALPR, including by the Office of the Victorian (Australia) Privacy Commissioner:

"Other concerns about ANPR centre on the aggregation of data in large, consolidated ANPR networks. The UK National ANPR Data Centre for example has faced criticism because it will centralise ANPR data from 43 police forces in England and Wales, drawing on several thousand cameras. A database in north London will hold the details of millions of British drivers' journeys as recorded by thousands of ANPR camera systems seeded on motorways across the country. City-centre and filling station cameras are also being integrated into the system. The database is stored in a National ANPR Data Centre next to the Metropolitan Police training centre in Hendon. Some 35 million number plates will be recorded each day with details of the time and location. This provides authorities with the time, date and precise location of vehicles as camera sites are also linked to global positioning satellites.[] This will mean that it will no longer be possible to travel on a road anywhere in Britain without being surveilled." Office of the Victorian [Australia] Privacy Commissioner, Travelsafe Committee Inquiry into Automatic Number Plate Recognition Technology, January 2008, p. 3, citation omitted, at http://www.privacy.vic.gov.au/privacy/web2.nsf/files/travelsafe-committee-inquiry-into-number-plate-recognition-technology-2008, accessed June 4, 2012.

[71] Government Accountability Office (GAO), Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, (Washington, D.C.: GAO, May 2008), p. 1, at http://www.gao.gov/new.items/d08536.pdf, accessed June 4, 2012.

[72] Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology,* (Gaithersburg, MD: NIST, April 2010), p. 2-1, at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf, accessed June 4, 2012. McCallister, *et. al.,* go on to describe *linked* and *linkable* information: "For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable." *Id.*

[73] International Association of Chiefs of Police (IACP), *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, (Alexandria, VA: IACP, September 2009), p. 10. Also, see *State v. Donis*, 157 N.J. 44 (1998), in which the Supreme Court of New Jersey approved a comparable two-step process for officers randomly checking license plates through a mobile data terminal (MDT). If the license plate MDT inquiry "disclosed that the car was unregistered, reported stolen or that the registered owner was not properly licensed, that information would then justify the police officer accessing the 'personal information' from the MDT. The ability of law enforcement officers under step-two to access full information indentifying motorists will help protect those officers from danger as they stop and approach motor vehicles." *Id.,* at http://caselaw.findlaw.com/nj-supreme-court/1309504.html

[74] Association of Chief Police Officers (ACPO) and National Policing Improvement Agency (NPIA), *Practice Advice on the Management and Use of Automatic Number Plate Recognition*, (UK, 2009), pp. 19-21, at http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf, accessed June 4, 2012. For information regarding the UK Data Protection Act, see http://www.legislation.gov.uk/ukpga/1998/29/contents, accessed June 4, 2012.

[75] Justice Harlan first articulated a "constitutionally protected reasonable expectation of privacy" in *Katz v. United States*, 389 U.S. 347 (1967), at 361. Justice Harlan's two-fold test is "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.*

[76] No. 10-1259, Argued November 8, 2011—Decided January 23, 2012, at http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf, accessed June 4, 2012.

[77] *Id.,* at p. 4.

[78] *Id.*, Justice Alito, with whom Justice Ginsburg, Justice Breyer, and Justice Kagan join, concurring in the judgment, p. 2.

[79] *Id.,* Justice Sotomayor concurring opinion, pp. 2-3. Citations omitted.

[80] 489 U.S. 749 (1989).

[81] "…the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.,* at p. 764.

[82] "…the privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap-sheet is a private citizen, and when the information is in the Government's control as a compilation, rather than as a record of 'what the Government is up to,' the privacy interest … is, in fact, at its apex, while the FOIA-based public interest in disclosure is at its nadir." *Id.,* at 780. The Society of American Archivists defines practical obscurity as: "The principle that private information in public records is effectively protected from disclosure as the result of practical barriers to access." at http://www.archivists.org/glossary/term_details.asp?DefinitionKey=3053, accessed June 4, 2012.

[83] Lum, et. al., surveyed residents of Fairfax County, Virginia, to assess public perceptions of ALPR technology and police legitimacy. Lum, et. al., *op. cit.,* at pp. 78-99. Also see, Anthony Abdalla, *Policy Issues Regarding Automated License Plate Recognition Technology,* no date, at http://www.police-writers.com/articles/policy_automated_license_plate_recognition_technology.html, accessed June 4, 2012.

[84] Paula T. Dow, Attorney General, *Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data,* (Trenton, NJ: Office of the Attorney General), December 3,

2010, p. 2, at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf, accessed June 4, 2012.

[85] *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored Data,* (Trenton, NJ: Office of the Attorney General), Issued December 3, 2010; Effective January 18, 2011, pp. 9-14, *Id.*

[86] Gordon Moore observed in 1965 that the number of components in integrated circuits doubled every year from 1958 – 1965, and predicted that it would continue for at least the next ten years. Gordon E. Moore, "Cramming more components unto integrated circuits," *Electronics,* Volume 38, Number 8, April 19, 1965, at ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf , accessed June 4, 2012. Processing speed and storage capacity of computers have continued to advance, doubling every 12-18 months, which has also significantly reduced data storage costs. New computing paradigms, such as cloud computing, offer mass storage at commodity pricing. "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing,* (Gaithersburg, MD: National Institute of Standards and Technology), September 2011, p. 2, at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed June 4, 2012.

[87] IACP, *Model Policy: License Plate Readers,* available at http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223, accessed June 4, 2012. In addition, IACP also published a companion report, *License Plate Readers: Concepts and Issues Paper*, August 2010, which provides background information and additional discussion of key issues, including data retention.

[88] Site visits were conducted as part of this project at Boston (MA) Police Department, Broward County (FL) Sheriff's Department, Escondido (CA) Police Department, Jefferson Parish (LA) Sheriff's Office, Kent (WA) Police Department, Long Beach (CA) Police Department, Long Beach (NY) Police Department, Los Angeles (CA) Sheriff's Department, Minnesota State Patrol, Norfolk (VA) Police Department, and Seattle (WA) Police Department.

[89] International Association of Chiefs of Police (IACP), *Privacy Issues Concerning the Utilization of Automated License Plate Readers,* (Alexandria, VA: IACP), March 24, 2009, published as Appendix 2, in *Privacy Impact Assessment Report for the Utilization of License Plate Readers,* at http://www.theiacp.org/LinkClick.aspx?fileticket=N%2bE2wvY%2f1QU%3d&tabid=87, accessed June 4, 2012.

References

Abdalla, Anthony. *Policy Issues Regarding Automated License Plate Recognition Technology,* no date, at http://www.police-writers.com/articles/policy_automated_license_plate_recognition_technology.html, accessed June 4, 2012.

America's Missing: Broadcast Emergency Response (AMBER) system, at http://www.amberalert.gov/ accessed June 4, 2012.

Association of Chief Police Officers (ACPO), *ANPR Strategy for the Police Service – 2010-2013*, at http://www.acpo.police.uk/documents/crime/2010/201010CRIANP01.pdf, accessed June 4, 2012.

Association of Chief Police Officers (ACPO) and National Policing Improvement Agency (NPIA), *Practice Advice on the Management and Use of Automatic Number Plate Recognition*, (UK, 2009), at http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf, accessed June 4, 2012.

Apex Design, *Concept of Operations for the US 36 Managed Lane*, August 4, 2011, at http://www.coloradodot.info/programs/high-performance-transportation-enterprise-hpte/projects/us-36-hpte-projects/us-36-managed-lanes/IGA%20Phase%20I%20US%2036%20Project%20Executed%20with%20Exhibits.pdf, accessed June 4, 2012.

Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored Data, (Trenton, NJ: Office of the Attorney General), Issued December 3, 2010; Effective January 18, 2011, at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf, accessed June 4, 2012.

Baker, Al. "Camera Scans of Car Plates are Reshaping Police Inquiries," *The New York Times,* April 11, 2011, at http://www.nytimes.com/2011/04/12/nyregion/12plates.html?pagewanted=all, accessed June 4, 2012.

Boreham, Jay. "Snapped and nabbed," *Manukau Courier*, AU, April 17, 2012, at http://www.stuff.co.nz/auckland/local-news/manukau-courier/6754667/Snapped-and-nabbed, accessed June 4, 2012.

Campbell Police Department, *Automated License Plate Readers: Policy 462*, 2010. http://www.ci.campbell.ca.us/AgendasMinutes/2010/ca04062010/Item%2008.pdf, accessed June 4, 2012.

City of Dallas, Texas, *Request for Competitive Sealed Proposal, BHZ1217, DPD Mobile and Fixed Automatic License Plate Recognition (ALPR System),* http://www.scribd.com/doc/88124473/Rfcsp-Dpd-Alpr-System-Ver1-0#outer_page_3, accessed June 4, 2012.

Crum, Travis. "Special license plates bring in $1.2 million for State Road Fund," *The Charleston Gazette*, May 29, 2011, at http://wvgazette.com/News/201105291075, accessed June 4, 2012.

Charlotte-Mecklenburg Police Department, *Standard Operating Procedure: License Plate Reader*, April 29, 2011, http://gemini.gmu.edu/cebcp/Charlotte-Mecklenberg%20SOP.pdf, accessed June 4, 2012.

Declan *Measuring Cross-Border Travel Times for Freight: Otay Mesa International Border Crossing*, March 31, 2008, at http://www.ops.fhwa.dot.gov/publications/fhwahop10051/index.htm, accessed June 4, 2012.

Dees, Tim. "New Development in ALPR," *Police Magazine*, February 2011, at http://www.policemag.com/Channel/Technology/Articles/Print/Story/2011/02/New-Developments-In-ALPR.aspx, accessed June 4, 2012.

Department for Transport, *Case Study: London Congestion Charging*, June 2, 2010, at http://www.dft.gov.uk/itstoolkit/CaseStudies/london-congestion-charging.htm, accessed June 4, 2012.

Dow, Paula T. Attorney General, *Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data,* (Trenton, NJ: Office of the Attorney General), December 3, 2010, p. 2, at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf, accessed June 4, 2012.

"Drivers on police files for life," *This is Cornwall*, June 30, 2009, at http://www.thisiscornwall.co.uk/Drivers-police-files-life/story-11398048-detail/story.html, accessed June 4, 2012.

Eberline, Andrew. *Cost/Benefit Analysis of Electronic License Plates, Final Report 637*, June 2008, at http://www.azdot.gov/TPD/ATRC/publications/project_reports/PDF/AZ637.pdf, accessed June 4, 2012.

Gaumont, Norm and Dave Babineau. "The Role of Automatic License Plate Recognition Technology in Policing: Results from the Lower Mainland of British Columbia," *Police Chief Magazine*, vol. LXXV, no. 11, November 2008.

Government Accountability Office (GAO), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, (Washington, D.C.: GAO, May 2008), p. 1, at http://www.gao.gov/new.items/d08536.pdf, accessed June 4, 2012.

Hindery, Robin. "Calif. License plates might go digital, show ads for revenue," Associated Press, *USA Today*, at http://www.usatoday.com/tech/news/2010-06-22-calif-license-plates_N.htm, accessed June 4, 2012.

International Association of Chiefs of Police (IACP), *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, (Alexandria, VA: IACP), September 2009.

International Association of Chiefs of Police (IACP), *Privacy Issues Concerning the Utilization of Automated License Plate Readers,* (Alexandria, VA: IACP), March 24, 2009, published as Appendix 2, in *Privacy Impact Assessment Report for the Utilization of License Plate Readers.*

International Association of Chiefs of Police, *Model Policy: License Plate Readers*, August 2010 http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223;

Katz v. United States, 389 U.S. 347 (1967).

Keates, Nancy. "What Drives People to Take a Creative License?" *Wall Street Journal*, June 23, 2011, at http://online.wsj.com/article/SB10001424052702303745304576359910386002034.html?mod=WSJ_hpp_MIDDLE_Video_Top, accessed June 4, 2012.

Kennedy, Jim. "Step up to the plate," *Thinking Highways,* Vol. 4, No. 1, pp. 40-42, 2009 at http://thinkinghighways.com/Pages/View-issue/View-issue-page.aspx?id=cbd7c667-4536-469b-8670-854bfd3ac23b, accessed June 4, 2012.

Kent Police, *G10 Automatic Number Plate Recognition (ANPR),* July 2010, http://www.kent.police.uk/about_us/policies/g/g10.html, accessed June 4, 2012.

Kenworthy, Bill. "State-by-state statutes governing license plates," January 20, 2006, at http://archive.firstamendmentcenter.org/analysis.aspx?id=16337, accessed June 4, 2012.

Klein. Allison and Josh White. "License plate readers: A useful tool for police comes with privacy concerns," *The Washington Post*, November 19, 2011, at http://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_story.html, accessed June 4, 2012.

Koper, Christopher. PERF, *Critical Issues in Policing Series: "How Are Innovations in Technology Transforming Policing?"* (Washington, D.C.: PERF, 2012), p. 30, at http://policeforum.org/library/critical-issues-in-policing-series/Technology_web.pdf, accessed June 4, 2012.

Lackey, Katharine . "States look at corporate plates to help with deficits," *USA Today*, at http://www.usatoday.com/news/nation/2010-11-04-license-plates_N.htm, accessed June 4, 2012.

Lakshmi, Ch. Jaya. A. Jhansi Rani, K. Sri Ramakrishna, and M. KatiKiran, "A Novel Approach for Indian License Plate Recognition System," 6 *International Journal of Advanced Engineering Sciences and Technologies*, 10-14, 2011, at http://ijaest.iserp.org/archieves/9.2-A16-30-11/Vol-No.6-Issue-No.1/3.IJAEST-Vol-No-6-Issue-No-1-A-Novel-Approach-for-Indian-License-Plate-Recognition-System-010-014.pdf, accessed June 4, 2012.

Lender, John "As Use of License Plate Scanners Spreads, Privacy Concerns Deepen," *Harford Courant*, April 21, 2012, at: http://articles.courant.com/2012-04-21/news/hc-lender-column-plate-scanners-0422-20120421_1_license-plate-data-license-plate-scanners-surveillance-camera, accessed June 4, 2012.

Lum, Cynthia, Linda Merola, Julie Willis, and Breanne Cave, *License Plate Recognition Technology (LPR): Impact Evaluation and Community Assessment*, (Fairfax, VA: George Mason University Center for Evidence-Based Crime Policy, September 2010), http://gemini.gmu.edu/cebcp/LPR_FINAL.pdf, accessed June 4, 2012.

Me. Rev. Stat. Ann. tit. 29-A, §2117-A (Use of automated license plate recognition systems), at http://www.mainelegislature.org/legis/statutes/29-A/title29-Asec2117-A.html, accessed June 4, 2012.

McCallister, Erika, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology,* (Gaithersburg, MD: NIST, April 2010), p. 2-1, at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf, accessed June 4, 2012.

Mell, Peter and Timothy Grance, *The NIST Definition of Cloud Computing,* (Gaithersburg, MD: National Institute of Standards and Technology), September 2011, p. 2, at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed June 4, 2012

Montes, Sebastian . "MCPD Wants to Keep License Plate Data Indefinitely," *Wheaton Patch*, April 11, 2012, at http://wheaton-md.patch.com/articles/mcpd-wants-to-keep-license-plate-data-indefinitely-76216f6d, accessed June 4, 2012.

Moore, Gordon E. "Cramming more components unto integrated circuits," *Electronics,* Volume 38, Number 8, April 19, 1965, at ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf , accessed June 4, 2012

Morgan, Chris, John Gaw, Sam Paul, *Fixed ALPR "Best Practices",* presentation at the 2011 IACP LEIM Conference, San Diego, California, June 15, 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/Fixed_ALPR_Best_Practice-Final.pdf, accessed June 4, 2012.

National Policing Improvement Agency (NPIA), *National ACPO ANPR Standards (NAAS),* version 4.12, November 2011, at http://www.acpo.police.uk/documents/crime/2011/201111CBANAAS412.pdf, accessed June 4, 2012.

Neville, Russell A. "Cincinnati Regional Automatic License Plate Recognition Technology Project," *The Police Chief Magazine,* vol. LXXVI, no. 6, June 2009, at http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1823&issue_id=62009, accessed June 4, 2012.

New York State Division of Criminal Justice Services, *Operation of License Plate Readers for Law Enforcement Agencies in New York State: Suggested Guidelines*, June 2007 http://www.elsag.com/media/content/NYDCJS%20LPR%20Policy.pdf, accessed June 4, 2012.

New York State Division of Criminal Justice Services, *Suggested Guidelines: Operation of License Plate Reader Technology, 2011,* http://criminaljustice.state.ny.us/ofpa/pdfdocs/finallprguidelines01272011a.pdf, accessed June 4, 2012.

North Yorkshire Police (UK), "Travelling criminals hit hard by ANPR Team," April 20, 2012, at http://www.northyorkshire.police.uk/index.aspx?articleid=8593, accessed June 4, 2012.

Office of the Victorian Privacy Commissioner, *Submission to the Queenland Parliament's Travelsafe Committee Inquiry into Automatic Number Plate Recognition Technology* (Victoria, AU: Office of the Victorian Privacy Commissioner, January 2008), pp. 3-4, at http://www.privacy.vic.gov.au/privacy/web2.nsf/files/travelsafe-committee-inquiry-into-number-plate-recognition-technology-2008/$file/submission_01_08.pdf, accessed June 4, 2012.

Ontario Information and Privacy Commissioner, *Privacy Investigation: The Toronto Police Service's use of Mobile License Plate Recognition Technology to Find Stolen Vehicles,* (Toronto, Ontario: Information and Privacy Commissioner), April 29, 2003, at http://www.ipc.on.ca/images/Findings/up-mc_030023_1.pdf, accessed June 4, 2012.

Protection of Freedoms Bill, Memorandum Submitted by the European Secure Vehicle Alliance (ESVA) (PF 11), Session 2010-11, at http://www.publications.parliament.uk/pa/cm201011/cmpublic/protection/memo/pf11.htm, accessed June 4, 2012.

PA Consulting Group, *Police Standards Unit: Thematic review of the use of automatic number plate recognition within police forces*, December 2006, at http://gemini.gmu.edu/cebcp/LPR/Thematic_Review_of_ANPR_v2[1].pdf, accessed June 4, 2012.

PERF, *Critical Issues in Policing Series. How Are Innovations in Technology Transforming Policing?* (Washington, DC: PERF), January 2012. http://policeforum.org/library/critical-issues-in-policing-series/Technology_web.pdf, accessed June 4, 2012.

PERF, *Use of Technology in Policing: The Chief's Perspective*, (Washington, DC: PERF), April 4, 2011, http://www.policeforum.org/library/critical-issues-in-policing-series/perfpresentation.pdf, accessed June 4, 2012.

Reaves, Brian A. *Local Police Departments, 2007* (Washington, DC: Bureau of Justice Statistics) December 2012, NCJ-231174, p. 22, at http://bjs.ojp.usdoj.gov/content/pub/pdf/lpd07.pdf, accessed June 4, 2012.

Riley, David. "License plate readers help police, worry privacy groups," *Taunton Daily Gazette,* July 6, 2011, at http://www.tauntongazette.com/news/x1860262823/License-plate-readers-help-Mass-police-worry-privacy-groups, accessed June 4, 2012.

Spielman, Fran "O'Hare upgrade would let you find and pay for parking with your phone," *Chicago Sun Times*, May 4, 2012 at http://www.suntimes.com/news/12318425-418/ohare-upgrade-would-let-you-find-and-pay-for-parking-with-your-phone.html, accessed June 4, 2012.

South Portland Police Department, *Standard Operating Procedures, ALPR, Policy # 8-82-F*, September 20, 2010, at p. 8-82-F-2, at http://www.maine.gov/sos/SPPD-SOP.pdf, accessed June 4, 2012.

Space and Naval Warfare Systems Center Atlantic, System Assessment and Validation for Emergency Responders (SAVER), *Mobile License Plate Recognition Systems Assessment Report*, (Washington, DC: Department of Homeland Security, September 2009, Revision 1).

State of Maryland, *Automated License Plate Reader Technology Security Integration Strategy,* August 2010, at http://www.governor.maryland.gov/documents/100804LPRPlan.pdf, p. 5, accessed June 4, 2012.

State v. Donis, 157 N.J. 44 (1998)

Stockton, Dale and Dan Gomez, *Automated License Plate Recognition: Interoperability and Policy and Procedures,* presentation at the 2011 IACP LEIM Annual Conference, San Diego, California June 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/LEIM-2011-San-Diego-Final.pdf, accessed June 4, 2012.

Sutter, Lisa *The Metropolitan [DC] Police Department: Our LPR Experience,* presentation at the 2011 IACP LEIM Conference, San Diego, California, June 15, 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/District-of-Columbia-Metropolitan-Police-Department-Presentation_6-15-11.pdf, accessed June 4, 2012.

"Travelling criminals hit hard by ANPR team," North Yorkshire Police, UK, April 20, 2012, accessed at http://www.northyorkshire.police.uk/index.aspx?articleid=8593, accessed June 4, 2012.

Taylor, Bruce, Christopher Koper, Daniel Woods, Combating Vehicle Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology, *Criminal Justice Review*, November 14, 2011, at http://cjr.sagepub.com/content/early/2011/11/09/0734016811425858, accessed June 4, 2012.

"Uninsured Drivers Targeted," *Mearns Leader*, April 13, 2012, at http://www.mearnsleader.co.uk/community/uninsured-drivers-targeted-1-2230630#; accessed June 4, 2012.

"Uninsured drivers targeted in police crackdown," *Banffshire Journal*, UK, April 5, 2012, at http://www.banffshire-journal.co.uk/News/Uninsured-drivers-targeted-in-police-crackdown-05042012.htm, accessed June 4, 2012.

U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

United States v. Jones, No. 10-1259, Argued November 8, 2011—Decided January 23, 2012, at http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf, accessed June 4, 2012.

Valcarcel, Julio. *Maryland's LPR Program and Policy Overview,* presentation presented at the 2011 IACP LEIM Conference, June 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/Maryland's-LPR-Program-and-Policy-Overview.pdf, accessed June 4, 2012

Valcarcel, Julio and Dale Stockton, *ARJIS Regional License Plate Reader Sharing,* presentation at the 2011 IACP Law Enforcement Information Management (LEIM) Annual Conference, San Diego, California June 2011, at http://www.theiacp.org/Portals/0/pdfs/LEIM/2011Presentations/ARJIS_LEIM2011.pdf, accessed June 4, 2012.

Virginia Department of Transportation, *Tolling Facilities Report, HB 3302 (2007)*, at http://virginiadot.org/projects/resources/TollingReportforVDOTwebsite.pdf, accessed June 4, 2012.

Washington Association of Sheriffs and Police Chiefs, *Guidelines for Washington State Law Enforcement: Operation of Automated License Plate Readers*, September 2008.

Wilonsky, Robert "Dallas PD intends to use license-plates [sic] readers to catch criminal now and gather 'information' for use later," *The Dallas Morning News,* April 5, 2012, http://crimeblog.dallasnews.com/archives/2012/04/dallas-pd-intends-to-use-licen.html, accessed June 4, 2012.

Appendix A: Sample Agency ALPR Policies

Note: These sample agency ALPR policies have been downloaded from agency websites. Readers should review and verify the currency of agency policies.

I. PURPOSE

To establish guidelines for CMPD employees for the deployment, maintenance, training, data storage, and associated uses of license plate readers (LPR) used by CMPD. It is the purpose of these procedures to serve as a guide for the use of LPRs which collect and store large amounts of data (license plates, dates, times, and locations of vehicles) for future records management, analysis and dataset linking.

II. POLICY

LPR technology automates a process that, in the past, was conducted manually by officers, tag by tag, with much discretion. LPR is an information technology system with the capability for quick scanning and matching capabilities. In addition to recovering stolen vehicles, LPR data can be used to confirm a suspect's alibi or whereabouts at a particular date and time. Data may also be used for predictive purposes, i.e., to scan and record vehicular activity in high risk/crime locations and unusual patterns of traffic by one or multiple vehicles resulting in a heightened risk or concern that emerges from analyzing the data.

III. DEFINITIONS

A. License Plate Recognition (LPR) system: Equipment consisting of camera(s), computer, and computer software used to automatically recognize and interpret the characters on vehicle license plates. The LPR can scan and read over 3,000 license plates per hour. Digital images captured by the cameras are converted into data, which is processed through the LPR system. This data is then compared against a list of license plates bearing some significance to the CMPD. If the information supplied via the LPR system alerts LPR Operators to an offense or relevant intelligence on a vehicle, the vehicles may be stopped to allow further investigation. Stored data may also be analyzed at a further date for investigative purposes.

B. LPR Manager: Command staff level employee designated by the Chief of Police or designee who is responsible for the management of the LPR program including its administration, troubleshooting, training, repairing and coordinating all aspects of the LPR system.

C. LPR-Generated Data: All information including GPS coordinates, date and time of a license plate reading, the optical character recognition interpreted data, and any LPR-generated digital photographic image(s) of the license plate and vehicle generated entirely through the use of and by the LPR equipment.

D. LPR Operator: A sworn employee properly trained in the use of the CMPD LPR system.

E. Download: The transfer of hot list data from NCIC, KBCOPS, or other data sources consisting of license plates and associated data.

F. External Hot List: A database populated with items of specific concern to the investigative and/or enforcement interests within the CMPD's jurisdiction. External hot lists originate from sources other than CMPD such as NCIC data.

G. Local Hot List: An addition to the LPR server database that is appended to the External Hot List. The local hot list consists of license plates of local investigative significance entered into the server hot list from sources such as KBCOPS or GangNet.

H. Alert: A positive indication, by visual and/or audible signal, of a potential match between data on the hot list and a license plate scanned by the LPR system. An alert is not conclusive confirmation that a license plate is wanted. Additional investigation is always warranted when an alert is indicated.

IV. DAILY CHECKLIST and PATROL PROCEDURES

A. Daily Checklist

1. Officers will visually inspect the exterior cameras to ensure the lenses are clear and the cameras have not been altered in any way.

2. Download the most current data file of stolen and "of interest" vehicles containing all of the current NCIC information.

3. Manually add any license plate numbers of interest that warrant a law enforcement related alert.

4. LPR Operators should leave the LPR system operational while patrolling during the duration of the shift. The LPR screen can be minimized in the background and can be constantly operational even when on other calls or conducting preventative patrol.

5. LPR Operators can adjust the manner in which they drive to maximize the number of tags being read.

   a. The front facing camera allows for the tags to be read in close proximity to the right front of the police vehicle.

   b. The rear facing allows for tags to be read at a further distance in relation to the camera and is designed to capture tags on vehicles traveling the opposite direction of the police vehicle.

   c. The side facing camera allows for tags to be read on vehicles in a parked position. This function is best utilized when driving in parking lots with a high volume of vehicles.

6. Officers must upload LPR data to the computer server at the end of each shift and confirm that the data transfer is complete.

B. Patrol Procedures

1. Use crime analysis to accurately target patrols in areas specifically related to crime trends where the collection of this data will benefit future and current investigations.

2. Target areas should be small enough (usually less than a half mile wide) for patrol units to drive through every street within the hotspot in less than 30 minutes.

3. Staying in strategic locations for 30 minutes or less LPR Operators would be more effective in deterring criminal activity.

4. LPR Operators should be given 3-5 small crime strategic locations to patrol in a shift.

5. To maximize effectiveness, LPR Operators should move from strategic location to strategic location in a completely random fashion.

6. LPR Operators should use "sweep and sit" scheme.

7. "Sweep" each strategic location at least once for parked and moving vehicles.

8. "Sit" at certain locations, at the discretion of the LPR Operator, in which the probability of a suspect vehicle traveling by would be the greatest.

V. Responsibilities

A. LPR Operators shall receive formal training prior to using the LPR system.

B. LPR Operators shall exercise safety when operating the LPR system.

1. Use of any device during the operation of a motor vehicle must comply with current State law including CMPD Policies and Directives.

2. LPR Operators will pay careful attention to driving and will not use the LPR system in any manner that would endanger or distract them, resulting in an accident.

C. It shall be the responsibility of each LPR Operator to ensure the download of the most recent hot list occurs on the mobile computer prior to deployment of the LPR equipment.

D. When using an LPR-equipped vehicle, LPR Operators should have the system in operation to include a connection to the LPR server so as to maximize the opportunity to scan vehicles, compare them to the hot list and collect LPR data in a central repository.

E. Upon receiving an alert, the LPR Operator will use the displayed information to determine the accuracy and nature of the alert. The LPR Operator will visually verify that the subject tag and the actual read on the LPR screen are the same (i.e. correct letters, numbers, state and any other information that can be matched).

F. Once the LPR Operator has confirmed that the alert is valid, he or she shall take appropriate action based on the type of alert in accordance with training.

1. If the alert is for a stolen or felony vehicle, the LPR Operator will confirm the alert is still active by running a check on the information through NCIC.

   a. Receipt of a stolen or felony vehicle LPR alert may not rise to the level of reasonable suspicion and is certainly not sufficient probable cause to arrest without confirmation that the vehicle is still wanted.

   b. If the alert is for another type of want, the LPR Operator will read the description of the alarm and use the appropriate action or reporting method. Confirmation of the alert is essential prior to the stop of any person.

G. Ensure that all positive "hits" on the Terrorist Watch List are reported to the Terrorist Screening Center (TSC). All Terrorist Watch List hits will be handled by phone. There will be no radio traffic concerning Terrorist hits except in the case of emergencies. LPR Operators must be familiar with the (3) three levels of Terrorist.

Watch List hits:

1. Level (1) one stop hold and contact TSC
2. Level (2) two keep a visual and contact TSC for further instructions and do not alert subjects of your presence
3. Level (3) three document information, take no action, report information to TSC

H. Some LPR Operators will be power users and may assist with the training of Operators, troubleshooting problems with the LPR system, helping their co-workers understand the value of the LPR system, and improving the operations of the LPR system.

VI. SUPERVISORS

A. Supervisors will monitor the use of LPR systems and ensure they are being deployed regularly.

B. Supervisors will ensure LPR systems are deployed during the shift by trained LPR Operators.

C. The LPR systems should be deployed to maximize its ability to scan as many license plates as possible.

D. The supervisor shall investigate any damage to LPR's in accordance with established procedures. Damage and any reports or documentation will be forwarded to the LPR Manager.

VII. LPR MANAGER

A. The LPR Manager will determine how the LPR system will be integrated into CMPD patrol function and will also determine any restrictions for the use of the LPR system .

B. The LPR Manager will validate training for LPR Operators to ensure LPR Operators

are properly trained before accessing LPR data or participating in LPR field operations, to ensure training is timely and adequate, to ensure proper operations in accordance with this Standard Operating Procedure, and to ensure all training is documented.

C. The LPR Manager will recommend policy changes to the Field Operations Deputy Chief in his or her chain of command.

VIII. DATA RETENTION and USE

A. Data will be stored on CMPD database residing on a City of Charlotte server and will not be stored outside the control of the CMPD.

B. All LPR-generated data will be purged after an 18-month retention period unless a longer retention period has been identified for court or investigative purposes.

1. For retention beyond the 18-month retention period, officers must scan the "Exhibit Report" into KBCOPS.

2. LPR Operators will be responsible for advising their supervisor when LPR data they marked for extended retention is no longer needed.

3. The LPR system automatically erases stored data when the retention period has elapsed.

C. Access to LPR data is restricted to CMPD personnel, in furtherance of a criminal justice purpose, LPR data may be shared verbally by a member of CMPD with another criminal justice agency. Any other use of this data is strictly forbidden.

1. Users will be able to access the LPR data by providing the established user name and password. This access will allow for the user to query information as it pertains to vehicle tags read by the tag reader cameras.

2. The LPR manager will determine the personnel to have access to the database for investigative queries and reports. Any requests for database access will be handled on a case by case basis and those granted access will be provided the user name and password for access.

3. Information stored includes a photo of the registration plate showing the rear of the vehicle, a date and time stamp of when the registration plate was read by the LPR, and a GPS coordinate to identify the exact location the registration plate was read by the LPR.

IX. LPR MAINTENANCE

1. Neither the LPR equipment nor or software operating system shall be modified without direction from the LPR Manager.

2. Under no circumstances shall an LPR unit be connected to or removed from the vehicle while the LPR unit is powered up. Connection or disconnection of

the camera unit from the LPR system when powered will result in significant damage to the LPR system.

3. Any time the LPR unit is disconnected or removed from the vehicle, it shall be placed in a protective storage case or the LPR's original packaging and secured to prevent damage.

4. LPR camera lenses may be cleaned with glass cleaner or mild soap and water and a soft, non-abrasive cloth.

5. Damage to LPR equipment shall be immediately reported to a supervisor. The supervisor shall document (and investigate, if necessary) any damage in accordance with established procedures. Damage will also be reported to the supervisor's Captain and the LPR Manager.

6. The LPR Manager shall be notified immediately of any LPR equipment needing maintenance or repair and ensure that all maintenance and repair of LPR equipment is completed.

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lieutenant Governor

State of New Jersey
OFFICE OF THE ATTORNEY GENERAL
DEPARTMENT OF LAW AND PUBLIC SAFETY
PO BOX 080
TRENTON, NJ 08625-0080

PAULA T. DOW
Attorney General

DIRECTIVE NO. 2010-5

TO: Director, Office of Homeland Security and Preparedness
Director, Division of Criminal Justice
Superintendent, New Jersey State Police
All County Prosecutors
All County Sheriffs
All Police Chiefs
All Law Enforcement Chief Executives

FROM: Paula T. Dow, Attorney General

DATE: December 3, 2010

SUBJECT: **Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data**

In order to fulfill the mission of protecting the public, the New Jersey law enforcement community must take full advantage of new crime-fighting technologies as they become available. Automated license plate readers (ALPRs) are now being used by a number of law enforcement agencies around the nation, and a number of police agencies in New Jersey have recently acquired these devices or are planning to do so in the near future. License plate recognition technology can be used to support a wide range of law enforcement operations and activities, including homeland security, criminal and terrorist suspect interdiction, revoked/suspended driver interdiction, stolen property recovery, stay-away order enforcement and, of course, the apprehension of individuals who are subject to an outstanding arrest warrant.

These devices enable police officers to recognize and take immediate action against vehicles and persons who are subject to an investigative detention or arrest based on a "Be on the Lookout" bulletin. The data collected by ALPRs can also provide solid investigative leads if, for example, a device happened to be scanning license plates near a crime scene, allowing police to locate potential suspects, witnesses, or victims by identifying vehicles that were in the vicinity at the time of the

New Jersey Is An Equal Opportunity Employer · Printed on Recycled Paper and is Recyclable

offense. A careful analysis of stored ALPR data can also be used to detect suspicious activities that are consistent with the *modus operandi* of criminals. This new technology can in this way serve an especially important role in protecting our homeland from terrorist attack, as shown by the fact that many of the devices that are now or soon will be in operation in this State were purchased with homeland security grant monies.

While license plate recognition technology can help to protect public safety, the widespread deployment and use of ALPRs, and especially the collection and storage of data pertaining to individuals who are not reasonably believed to be involved in unlawful activity, raise legal and policy issues. Notably, the New Jersey Supreme Court has held that while police are permitted to "run the plates" of any vehicle they encounter while on patrol, and need not have a particularized reason before checking a vehicle's license plates against a government database, police in this State may not as a result of any such lookup be shown personal identifying information about a motorist unless there is a particularized basis for further police action. See State v. Donis, 157 N.J. 44 (1998). The Guidelines attached hereto are designed to protect the legitimate privacy interests of motorists by implementing the non-disclosure rule established in Donis and by adapting the Donis Court's rationale to the context and capabilities of ALPR technology.

Recognizing that our experience with this new and evolving technology is limited, and that we still have much to learn about how best to incorporate these devices into our arsenal of investigative techniques, it is appropriate for me as the State's chief law enforcement officer to issue uniform statewide guidelines to ensure that ALPRs are used only for *bona fide* law enforcement purposes, and that the data collected by these devices are used in accordance with substantive standards and procedural safeguards that appropriately balance the need for law enforcement agencies to prevent and respond to terrorism and other forms of crime against the legitimate privacy interests of persons operating motor vehicles on the roadways of this State.

THEREFORE, I, Paula Dow, Attorney General of the State of New Jersey, pursuant to the authority granted to me by the Constitution of the State of New Jersey and by the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 *et seq.*, and in consultation with the Director of the New Jersey Office of Homeland Security and Preparedness, hereby Direct the following:

1. Adoption of Guidelines

The "*Attorney General Guidelines for the Use of Automated License Plate Readers and Stored ALPR Data*" (dated December 3, 2010) attached to this Directive and incorporated by reference into this Directive are hereby adopted and shall be followed and enforced by all law enforcement agencies and officers operating under

the authority of the laws of the State of New Jersey.

2. Implementation

Every law enforcement agency operating under the authority of the laws of the State of New Jersey that possesses or uses one or more automated license plate readers shall, within 45 days of the issuance of this Directive, promulgate and enforce a rule, regulation, standard operating procedure, directive, or order, in a form as may be appropriate given the customs and practices of the agency, which shall comply with and implement the provisions of the attached Guidelines, and which shall provide that any sworn officer or civilian employee of the agency who knowingly violates the agency's rule, regulation, standard operating procedure, directive, or order shall be subject to discipline. A law enforcement agency operating under the authority of the laws of the State of New Jersey that purchases an automated license plate reader on or after the effective date of this Directive shall not operate the device without having promulgated a rule, regulation, standing operating procedure, directive, or order in accordance with this section.

3. Scope

The provisions of this Directive and of the attached Guidelines pertaining to stored ALPR data apply to all law enforcement agencies operating under the authority of the laws of the State of New Jersey that access or use stored ALPR data, even if the agency does not own or operate an ALPR.

4. Questions and Controversies

All questions concerning the interpretation, implementation, or enforcement of this Directive, or of the attached Guidelines, shall be addressed to the Attorney General or his or her designee.

5. Periodic Review

The Director of the Division of Criminal Justice, in consultation with the Superintendent of the New Jersey State Police, the Director of the Office of Homeland Security, the County Prosecutors, the County Sheriffs, and the New Jersey Association of Chiefs of Police, shall, within one year of the effective date of this

Directive, report to the Attorney General on the implementation of this Directive, and on any recommendations for revising the attached Guidelines.

6. Effective Date

This Directive shall take effect 45 days after it is issued in order to provide an opportunity for law enforcement agencies to comply with its requirements and to establish and enforce policies and procedures consistent with the attached Guidelines. Once effective, this Directive shall remain in force and effect unless and until a repealed, amended, or superseded by Order of the Attorney General.

Paula T. Dow
Attorney General

Attest:
Carolyn Murray
Counsel to the Attorney General

Issued on: December 3, 2010
Effective on : January 18, 2011

ATTORNEY GENERAL GUIDELINES FOR THE USE OF AUTOMATED LICENSE PLATE READERS (ALPRs) AND STORED ALPR DATA

(Issued December 3, 2010; Effective January 18, 2011)

1. PURPOSE AND SCOPE

1.1 Reasons for Promulgating Uniform Statewide Guidelines

The purpose of these Guidelines is to provide direction to law enforcement agencies and officers on the appropriate us e of Automated License Plate Readers (ALPRs) and the data that are collected by these devices and stored for future law enforcement use. These Guidelines are not intended to serve as a comprehensive operational manual. Rather, they are meant to ensure that ALPRs and ALPR-generated data are used in an appropriate manner and only for *bona fide* public safety purposes.

The following Guidelines, which are promulgated pursuant to Attorney General Law Enforcement Directive 2010-5, should be interpreted and applied so as to achieve the following objectives:

- to ensure that "BOLO lists" (the compilation of targeted license plates that an ALPR is "on the lookout" for) that are programmed into the internal memory of an ALPR or that are compared against stored ALPR data are comprised only of license plates that are associated with specific vehicles or persons for which or whom there is a legitimate and documented law enforcement reason to identify and locate, or for which there is a legitimate and documented law enforcement reason to determine the subject vehicle's past location(s) through the analysis of stored ALPR data;

- to ensure that data that are captured by an ALPR can only be accessed by appropriate law enforcement personnel and can only be used for legitimate, specified, and documented law enforcement purposes;

- to permit a thorough analysis of stored ALPR data to detect crime and protect the homeland from terrorist attack while safeguarding the personal privacy rights of motorists by ensuring that the analysis of stored ALPR data is not used as a means to disclose personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst; and

- to ensure that stored ALPR data are purged after a reasonable period of time so as to

minimize the potential for misuse or accidental disclosure.

1.2 Applicability of Guidelines

These Guidelines apply to all law enforcement agencies that operate under the authority of the laws of the State of New Jersey that own or operate one or more ALPRs, that collect and maintain ALPR data, and/or that receive or are provided access to ALPR data collected by another agency.

1.3 Non-Enforceability of Rights by Third Parties

These Guidelines are issued pursuant to the Attorney General's authority under the Criminal Justice Act of 1970, N.J.S.A. 52:17B-97 *et seq.*, to ensure the uniform and efficient enforcement of the laws. These Guidelines impose limitations on the exercise of law enforcement discretion and the use of and access to ALPR-related data that may extend beyond the requirements of the United States and New Jersey Constitutions, and federal and state statutory law. Nothing in these Guidelines should be construed in any way to create any rights beyond those established under the Constitutions, statutes, and regulations of the United States and the State of New Jersey. The provisions of these Guidelines are intended to be implemented and enforced by law enforcement agencies that possess or use ALPRs, the New Jersey Office of Homeland Security and Preparedness, the County Prosecutors, and the Department of Law and Public Safety, and these provisions do not create any rights that may be enforced by any other persons or entities.

3. DEFINITIONS

As used in these Guidelines:

"Automated License Plate Reader" or "ALPR" means a system consisting of a camera, or cameras, and related equipment that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device, that automatically converts digital photographic images of scanned license plates into electronic text documents, that is capable of comparing scanned license plate text data with data files for vehicles on a BOLO (be on the lookout) list programmed into the device's electronic memory, and that notifies police, whether by an audible alert or by other means, when a scanned license plate matches the license plate on the programmed BOLO list. The term includes both devices that are placed at a stationary location (whether permanently mounted, or portable devices positioned at a stationary location) and mobile devices affixed to a police vehicle and capable of operating while the vehicle is in motion.

"BOLO (Be on the Lookout)" or "BOLO situation" refers to a determination by a law

enforcement agency that there is a legitimate and specific law enforcement reason to identify or locate a particular vehicle, or, in the case of a post-scan BOLO, there is a legitimate and specific reason to ascertain the past location(s) of a particular vehicle.

"BOLO list," sometimes referred to colloquially as a "hot list," is a compilation of one or more license plates, or partial license plates, of a vehicle or vehicles for which a BOLO situation exists that is programmed into an ALPR so that the device will alert if it captures the image of a license plate that matches a license plate included on the BOLO list. The term also includes a compilation of one or more license plates, or partial license plates, that is compared against stored license plate data that had previously been scanned and collected by an ALPR, including scanned license plate data that is stored in a separate data storage device or system.

"Initial BOLO list" refers to the BOLO list that was programmed into an ALPR at the time that the device was being used to scan license plates in the field.

"Post-Scan BOLO list" refers to a BOLO list that is compared against stored data collected by an ALPR, including scanned license plate data that has been transmitted to another device or data storage system.

"Stored data" refers to all information captured by an ALPR and stored in the device's memory or in a separate data storage device or system. The term includes the recorded image of a scanned license plate and optical character recognition data, a contextual photo (*i.e.*, a photo of the scanned vehicle and/or occupants), global positioning system("GPS") data (when the ALPR is equipped with a GPS receiver) or other location information, and the date and time of the scan. The term applies to both alert data and non-alert data that has been captured and stored by an ALPR or in a separate data storage device or system.

"Alert data" means information captured by an ALPR relating to a license plate that matches the license plate on an initial BOLO list or a post-scan BOLO list.

"Immediate alert" refers to an alert that occurs when a scanned license plate matches the license plate on an initial BOLO list and that is reported to the officer operating the ALPR, by means of an audible alarm or by any other means, at or about the time that the subject vehicle was encountered by the ALPR and its license plate was scanned by the ALPR.

"Non-encounter alert" refers to an immediate alert where the officer operating the ALPR is instructed to notify the agency that put out the BOLO without initiating an investigative detention of the subject vehicle or otherwise revealing to the occupant(s) of that vehicle that its location has been detected or that it is the subject of law enforcement attention (*e.g.*, a Violent Gang or Terrorist Organization File (VGTOF) alert).

"Personal identifying information" means information that identifies one or more specific individuals, including an individual's name, address, social security number, vehicle operator's

license number, or biometric records. The term includes personal identifying information that is included within the data comprising a BOLO list, as well as personal identifying information that is learned by checking a license plate scanned by an ALPR against the Motor Vehicle Commission database or any other data system that contains personal identifying information.

"Scan" refers to the process by which an ALPR automatically focuses on, photographs, and converts to digital text the license plate of a vehicle that comes within range of the ALPR.

"Authorized user"means a sworn or civilian employee of a law enforcement agency who has been authorized by the chief of the agency, or by the Attorney General or a county prosecutor or his or her designee, to operate an ALPR, or to access and use ALPR stored data, and who has successfully completed training provided by the agency on the agency's ALPR policy and on these Guidelines.

"Designated supervisor" means a superior officer assigned by the chief of a law enforcement agency to oversee and administer, or to assist in overseeing and administering, the agency's use of ALPRs and stored ALPR data. A law enforcement agency may have more than one designated supervisor.

"Chief" of a department or agency means the highest ranking sworn officer of a law enforcement agency.

"Post-Scan BOLO query" refers to the process of comparing a post-scan BOLO list against stored ALPR data.

"Crime scene query" refers to the process of accessing and reviewing stored ALPR data that had been originally scanned at or about the time and in the vicinity of a reported criminal event for the purpose of identifying vehicles or persons that might be associated with that specific criminal event as suspects, witnesses, or victims.

"Criminal event" means a specific incident, or series of related specific incidents, that would constitute an indictable crime under the laws of the State of New Jersey, whether or not the incident(s) have occurred or will occur within the State of New Jersey. The term includes an attempt or conspiracy to commit a crime, or actions taken in preparation for the commission of the crime, such as conducting a surveillance of the location to identify and evade or thwart security measures, or conducting a rehearsal of a planned crime. The term includes two or more separate criminal acts or episodes that are linked by common participants or that are reasonably believed to have been undertaken by a criminal organization or as part of an ongoing conspiracy.

"Crime trend analysis" refers to the analytical process by which stored ALPR data is used, whether alone or in conjunction with other sources of information, to detect crime patterns by studying and linking common elements of recurring crimes; to predict when and where future crimes may occur; and to link specific vehicles to potential criminal or terrorist activity. The term includes

an automated process in which a computer program analyzes stored data to identify potentially suspicious activity or other anomalies involving one or more scanned vehicles and where such automated analysis is done without disclosing personal identifying information about any individual to an authorized user or any other person except as may be authorized pursuant to Section 10.2.3 of these Guidelines.

4. DEPLOYMENT OF ALPRS

4.1 Restricted Uses

An ALPR and data generated by an ALPR shall only be used for official and legitimate law enforcement business.

4.2 ALPR Scanning Limited to Vehicles Exposed to Public View

An ALPR shall only be used to scan license plates of vehicles that are exposed to public view (*e.g.*, vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shopping mall or other business establishment).

4.3 Supervisory Approval of All ALPR Deployments

An ALPR shall not be deployed in the field unless the deployment has been authorized by the chief of the department or a designated supervisor, or by the Attorney General or designee or a county prosecutor or designee. Such authorization may be given for repeated or continuous deployment of an ALPR (*e.g.*, mounting the device on a particular police vehicle, or positioning the ALPR at a specific stationary location), in which event the deployment authorization shall remain in force and effect unless and until rescinded or modified by the chief or designated supervisor, or the Attorney General or county prosecutor or designee.

4.4 Trained Operators and Analysts

A sworn officer or civilian employee of the department may operate an ALPR or access or use ALPR stored data only if the person has been designated as an authorized user by the chief of the department, or by the Attorney General or designee or a county prosecutor or designee, and has received training from the department on the proper use and operation of ALPRs, the requirements of Attorney General Law Enforcement Directive 2010-5, and these Guidelines, and any policies and

procedures governing the use of ALPRs and ALPR data issued by the department pursuant to Attorney General Directive 2010-5and Section 14 of these Guidelines.

5. MAINTENANCE OF RECORDS

5.1 Records Documenting the Deployment of ALPRs

Each department that owns or operates an ALPR shall maintain a written or electronic record that documents the following information:

date and time when the ALPR was deployed;

whether the ALPR was mobile, or was stationed at a fixed specified location;

the identity of the operator;

whether ALPR data was transferred to any other database or data storage device or system.

5.2 Records Documenting the Use of Stored ALPR Data

Each department that stores ALPR data shall maintain a record of all access to stored ALPR data. The department's ALPR data record keeping system, which may be automated, shall document the following information:

the date and time of access, and, in the case of access to stored non-alert data, the type of access authorized by Section 10.2 of these Guidelines (*i.e.*, post-scan BOLO query, crime scene query, or crime trend analysis);

the authorized user who accessed the stored data;

whether an automated software program was used to analyze stored data;

the designated supervisor who reviewed and approved any disclosure of personal identifying information based upon crime trend analysis when such approval is required by Section 10.2.3 of these Guidelines;

the designated supervisor who approved any use of an automated crime trend analysis computer program that would automatically alert and disclose personal identifying

information in accordance with Section 10.2.3;

any other information required to be documented pursuant to Section 10.2 or any other provision of these Guidelines.

5.3 Maintenance of Records

All written or electronic records of ALPR activity and access to ALPR data shall be maintained by the department for a period of five years, and shall be kept in a manner that makes such records readily accessible to any person authorized by these Guidelines to audit the department's use of ALPRs and ALPR-generated data. When a department employs an automated system to record any information that is required to be documented pursuant to these Guidelines, it shall not be necessary for the department to maintain duplicate records of any events or transactions that are documented by the automated record-keeping system.

6. CONTENT AND APPROVAL OF BOLO LISTS

6.1 Criteria for and Examples of Legitimate BOLO Situations

A license plate number or partial license plate number shall not be included in an ALPR initial BOLO list unless there is a legitimate and specific law enforcement reason to identify or locate that particular vehicle, or any person or persons who are reasonably believed to be associated with that vehicle. A license plate or partial license plate number shall not be included in a Post-Scan BOLO list unless there is a legitimate and specific law enforcement reason to ascertain the past locations(s) of that particular vehicle, or of any person or persons who are reasonably believed to be associated with that vehicle.

Examples of legitimate and specific reasons include, but are not limited to: persons who are subject to an outstanding arrest warrant; missing persons; AMBER Alerts; stolen vehicles; vehicles that are reasonably believed to be involved in the commission of a crime or disorderly persons offense; vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list; vehicles with expired registrations or other Title 39 violations; persons who are subject to a restraining order or curfew issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements; persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity; and persons who are on any watch list issued by a State or federal agency responsible for homeland security.

6.2 Batch Downloading of BOLO List Data

BOLO list information may be downloaded in batch form from other databases, including but not limited to the National Crime Information Center (NCIC), National Insurance Crime Bureau, United States Department of Homeland Security, and Motor Vehicle Commission database.

6.3 Updates to BOLO Lists

An initial BOLO list may be revised at any time. In the event that an initial BOLO list is constructed, in whole or in part, with sets of data downloaded from another database, so as to account for any changes that may have been made in the data maintained in those other databases, updates to the initial BOLO list shall, in the case of a mobile unit attached to a police vehicle, be made at the start of each shift, and in the case of an ALPR positioned at a stationary location, be made as frequently as is practicable, and on not less than a daily basis. Information concerning any license plate that is referenced in an AMBER Alert activated by the New Jersey State Police shall be added to the initial BOLO list as expeditiously as possible, and shall remain in the initial BOLO list until the AMBER Alert expires or is withdrawn.

6.4 Special Instructions for Immediate Alert Response

When practicable, the reason for placing a vehicle on BOLO list shall be included with the BOLO and shall be disclosed to the officer who will react to an immediate alert. If for any reason an officer reacting to an immediate alert should not initiate an investigative detention (*e.g.*, where the license plate was included in the BOLO list because the department or any other agency wanted to be notified of the location of the subject vehicle without alerting the driver/occupants that they are the subject of law enforcement attention, such as in the case of Violent Gang or Terrorist Organization File (VGTOF) alert), to the extent feasible, the information attached to the license plate on the BOLO list shall be entered in such a way as to cause the ALPR to clearly designate an immediate alert as a "non-encounter" alert, and shall provide specific instructions to the officer as to who to notify of the alert. See Section 7, infra.

7. POLICE ACTIONS IN RESPONSE TO AN IMMEDIATE ALERT

When an officer operating a vehicle equipped with an ALPR receives an immediate alert, the officer shall take such action in response to the alert as is appropriate in the circumstances. An officer alerted to the fact that an observed motor vehicle's license plate is on the BOLO list may be required to make a reasonable effort to confirm that a wanted person is actually in the vehicle before

the officer would have a lawful basis to stop the vehicle. See State v. Parks, 288 N.J. Super. 407 (App. Div. 1996) (police do not have reasonable suspicion to justify a stop based on a computer check that shows that the operator's license of the registered owner of the vehicle is suspended unless the driver generally matches the owner's physical description (*e.g.*, age and gender)).

An officer reacting to an immediate alert shall consult the database to determine the reason why the vehicle had been placed on the BOLO list and whether the alert has been designated as a non-encounter alert. In the event of a non-encounter alert, the officer shall follow any instructions included in the alert for notifying the law enforcement or homeland security agency that had put out the BOLO. See Section 6.4, supra.

8. SECURITY OF STORED ALPR DATA

8.1 Physical Security and Limited Access

All ALPR stored data shall be kept in a secure data storage system with access restricted to authorized persons. Access to this stored data shall be limited to the purposes described in Section 10 of these Guidelines.

8.2 Differentiation of Stored Positive Alert Data From Non-Alert Data

Stored ALPR data shall be maintained electronically in such a manner as to distinguish alert data from non-alert data so as to ensure that access to and use of non-alert data and any disclosure of personal identifying information resulting from the analysis of non-alert data occurs only as may be authorized pursuant to section 10.2 of these Guidelines. Positive alert data may, as appropriate, be transferred to the appropriate active investigation file, see also Section 10.1, infra, and may as appropriate be placed into evidence in accordance with the department's evidence or records management procedures.

9. RETENTION PERIOD AND PURGING OF STORED DATA

Each law enforcement agency shall, pursuant to the provisions of Section 14 of these Guidelines, establish and enforce procedures for the retention and purging of stored ALPR data in accordance with this Section. ALPR stored data shall be retained for a period of five years, after which, the data shall be purged from the agency's data storage device or system. A law enforcement agency may purge ALPR data before the expiration of the five-year retention period only if the data has been transferred to the State Police Regional Operations Intelligence Center (R.O.I.C.)or any other system that aggregates and stores data collected by two or more law enforcement agencies in accordance with the provisions of these Guidelines. Any ALPR data transferred to another agency

shall indicate the date on which the data had been collected by the ALPR so that the receiving agency may comply with the five-year retention and purging schedule established in this Section. See also Section 11.1 and 11.2, infra.

10. LIMITATIONS ON ACCESS TO AND USE OF STORED ALPR DATA

10.1 Access to Positive Alert Data

An authorized user may access and use stored ALPR alert data as part of an active investigation or for any other legitimate law enforcement purpose, including but not limited to a post-scan BOLO query, a crime scene query, or crime trend analysis. A record shall be made of the access to the data, which may be an automated record, that documents the date of access, and the identity of the authorized user. An authorized user need not obtain approval from the chief or designated supervisor, or Attorney General or county prosecutor or designee, for each occasion on which he or she accesses and uses stored ALPR data. Once positive alert data has been accessed and transferred to an investigation file, it shall not be necessary thereafter to document further access or use of that data pursuant to these Guidelines.

10.2 Access to Non-Alert Data

Access to and use of stored non-alert ALPR data is limited to the following three purposes: a post-scan BOLO query, a crime-scene query, and crime trend analysis. An authorized user does not need to obtain approval from the chief or a designated supervisor, or Attorney General or county prosecutor or designee, for each occasion on which he or she accesses and uses stored non-alert data pursuant to this Section.

10.2.1 Post-Scan BOLO Query

A law enforcement agency is authorized to compare a post-scan BOLO list against stored ALPR data where the results of the query might reasonably lead to the discovery of evidence or information relevant to any active investigation or ongoing law enforcement operation, or where the subject vehicle might be placed on an active initial BOLO list. (For example, a law enforcement agency may review stored non-alert data to determine whether a specific vehicle was present at the time and place where the ALPR data was initially scanned for the purpose of confirming or dispelling an alibi defense, or to develop lead information for the purpose of locating a specified vehicle or person. A law enforcement agency may also check stored data to determine whether a vehicle that was only recently added to an initial BOLO list had been previously observed in the jurisdiction before it had been placed on an initial BOLO list.)

10.2.2 Crime Scene Query

a. A law enforcement agency is authorized to access and use stored non-alert data where such access might reasonably lead to the discovery of evidence or information relevant to the investigation of a specific criminal event as defined in these Guidelines. Note that if the law enforcement agency has reason to believe that a specific person or vehicle was at or near the location of the specific crime at the time of its commission, non-alert stored data might also be examined under the authority of Section 10.2.1 as part of post-scan BOLO query.

b. A crime scene query may not be conducted to review stored non-alert data based on general crime patterns (*i.e., e.g.*, to identify persons traveling in or around a "high crime area"), but rather is limited to situations involving specific criminal events as that term is defined in these Guidelines.

c. The crime scene query of non-alert stored data shall be limited in scope to stored non-alert data that is reasonably related to the specified criminal event, considering the date, time, location, and nature of the specified criminal event. For example, a crime that reasonably involves extensive planning and possible "rehearsals," such as a terrorist attack, would justify examining stored non-alert data that had been scanned and collected days or even weeks or months before the criminal event, and that may have been scanned at a substantial distance from the site of the crime or intended crime (*e.g.*, at any point along a highway leading to the intended crime site). A spontaneous crime, in contrast, might reasonably justify examination of stored non-alert data that was scanned and collected on or about the time of and in closer physical proximity to the criminal event.

d. The law enforcement agency shall document the specific crime or related crimes constituting the criminal event and the date(s) and location(s) of the specific crime(s).

10.2.3 Crime Trend Analysis

a. A law enforcement agency may access and use stored non-alert data for purposes of conducting crime trend analysis, as that term is defined in these Guidelines, when such access and analysis is approved by a designated supervisor and where such analysis is undertaken to produce analytical products that are intended to assist the agency in the performance of its duties. A designated supervisor may authorize one or more authorized users to conduct a method or methods of crime trend analysis on a repeated or continuous basis, in which event such authorization shall remain in force and effect unless and until modified or rescinded by the supervisor. A designated supervisor may also approve the use of an automated software program to analyze stored data to look for potentially suspicious activity or other anomalies that might be consistent with criminal or terrorist activity.

b. Crime trend analysis of stored non-alert data, whether automated or done manually, shall not result in the disclosure of personal identifying information to an authorized user or any other person unless:

1) the agency can point to specific and articulable facts that warrant further investigation of possible criminal or terrorist activity by the driver or occupants of a specific vehicle *(i.e.*, unusual behavior consistent with the *modus operandi* of terrorists or other criminals), and access to the personal identifying information based on those specific and articulable facts has been approved by a designated supervisor. Such approval may be given by a designated supervisor in advance when the crime trend analysis reveals the existence of specified suspicious circumstances that would warrant further investigation and that would justify disclosure of personal identifying information to the authorized user conducting the analysis under the "specific and articulable facts that warrant further investigation" standard of proof established in this Section. The supervisor shall document any and all specified suspicious circumstances for which disclosure of personal identifying information is pre-approved if those suspicious circumstances are revealed by authorized crime trend analysis. When an automated crime trend analysis computer program is used, specified suspicious circumstances that would warrant further investigation and that would justify disclosure of personal identifying information to an authorized user under this Section may also be pre-approved by a designated supervisor and built into the computer program so that if the program identifies the existence of the pre-determined suspicious circumstances, it will automatically alert the authorized user of the suspicious activity and provide to him or her the relevant personal identifying information in accordance with the "specific and articulable facts that warrant further investigation"standard of proof established in this Section; or

2) Disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.

c. Nothing in this Section shall be construed to prohibit a computer program from accessing and comparing personal identifying information of one or more individuals who are associated with a scanned vehicle as part of the process of analyzing stored non-alert data, provided that such personal identifying information is not disclosed to a person unless the "specific and articulable facts that warrant further investigation" standard is satisfied. The "specific and articulable facts that warrant further investigation" standard set forth in this Section applies only to the crime trend analysis of non-alert data, and nothing in this Section shall be construed to limit disclosure of personal identifying information of a person who is the registered owner of a vehicle that is on an initial or post-scan BOLO list (*i.e.*, alert data).

d. For the purposes of this Section, the "specific and articulable facts that warrant further investigation" standard required for the disclosure of personal identifying based upon crime trend

analysis of stored non-alert data is intended to be comparable to the "specific and articulable facts that warrant heightened caution" standard developed by the New Jersey Supreme Court in State v. Smith, 134 N.J. 599, 616-19 (1994) (establishing the level of individualized suspicion required before an officer may order a passenger to exit a motor vehicle stopped for a traffic violation).

e. The law enforcement agency accessing stored non-alert ALPR data for purposes of conducting crime trend analysis shall document: the nature and purpose of the crime trend analysis; the persons who accessed stored non-alert ALPR data for use in conducting that analysis; and the designated supervisor who approved access to ALPR non-alert data. In any instance where personal identifying information is disclosed based upon crime trend analysis of stored non-alert data, the agency shall document the specific and articulable facts that warrant further investigation and the designated supervisor who reviewed those facts and approved the disclosure of personal identifying information, or who pre-approved disclosure of personal identifying information based upon specified circumstances identified by an automated crime trend analysis computer program, or, where applicable, the fact that access to personal identifying information was authorized by a grand jury subpoena.

11. SHARED LAW ENFORCEMENT ACCESS TO STORED ALPR DATA

11.1 Authorization to Share and Aggregate Data

Any ALPR data that may in conformance with these Guidelines be accessed and used by the law enforcement agency that collected the data may be shared with and provided to any other law enforcement agency. Stored ALPR data may be combined with ALPR data collected by two or more law enforcement agencies (*e.g.*, collection of stored data by the State Police Regional Operations Intelligence Center), provided that such aggregated data shall only be retained, accessed, and used in accordance with the provisions of these Guidelines.

11.2 Record of Shared Access and Responsibilities of the Receiving Agency

When ALPR data is made accessible to or otherwise shared with or transferred to another law enforcement agency, the agency that collected the ALPR data shall document the identity of the other agency and the specific officer(s) or civilian employee(s) of that agency who were provided the information. When the transfer of stored ALPR data is done periodically as part of a system for aggregating data collected by two or more law enforcement agencies (*e.g.*, the scheduled and routine transmittal of data to the State Police Regional Operations Intelligence Center), each agency contributing data to the combined database shall maintain a record of the data transfer, which may be an automated record, and shall have and keep on file a memorandum of understanding or agreement or other memorialization of the arrangement for maintaining and populating a database comprised of stored ALPR data collected by multiple law enforcement agencies. Any agency

provided with access to or use of the ALPR data collected by another agency shall comply with all applicable provisions of these Guidelines concerning stored ALPR data and disclosure of personal identifying information.

13. RELEASE OF ALPR DATA TO NON-LAW ENFORCEMENT PERSONS OR AGENCIES

Stored ALPR data shall be treated as "criminal investigatory records" within the meaning of N.J.S.A. 47:1A-1 *et seq.*, and shall not be shared with or provided to any person, entity, or government agency, other than a law enforcement agency, unless such disclosure is authorized by a subpoena or court order, or unless such disclosure is required by the Rules of Court governing discovery in criminal matters. Any agency receiving a subpoena or court order for the disclosure of ALPR data shall, before complying with the subpoena or court order, provide notice to the County Prosecutor, or to the Division of Criminal Justice in the case of any state-level law enforcement agency.

14. PROMULGATION AND ENFORCEMENT OF DEPARTMENTAL POLICIES

14.1 Required Contents of Departmental Policies

Pursuant to the requirements of Attorney General Law Enforcement Directive 2010-5, every law enforcement agency that possesses or uses an ALPR must promulgate and enforce a rule, regulation, standing operating procedure, directive, or order that establishes a comprehensive policy governing the operation of ALPRs, and governing access to, use, and retention of all stored ALPR data. The ALPR policy promulgated by the department must be consistent with the standards and procedural safeguards established in these Guidelines, and each ALPR policy must include the following provisions:

a. The ALPR policy shall provide that the chief of the department will designate one or more superior officers to oversee and administer the agency's ALPR program. These designated supervisors will be authorized to: provide or oversee the training of all officers and civilian employees who are authorized to operate an ALPR or to access or use ALPR stored data; review and approve requests to access and use stored ALPR data to conduct crime trend analysis and/or to access personal identifying information based upon crime trend analysis; and generally to ensure compliance with the department's ALPR policy and these Guidelines.

b. The ALPR policy shall provide that the chief of the department shall designate all

authorized users, and that no officer or civilian employee will be authorized to operate an ALPR, or to access or use ALPR stored data, unless the officer or civilian employee has received training by the department on the proper operation of these devices, and on the provisions of the department's ALPR policy and these Guidelines.

c. The ALPR policy shall implement and enforce the five-years retention period for ALPR stored data established in Section 9 of these Guidelines, and must provide for the purging of all ALPR stored data at the expiration of the five-year term.

d. The ALPR policy shall provide for the documentation of all ALPR-related activities and decisions that are required to be documented by Section 5 or any other provision of these Guidelines, which may be done by an automated record-keeping system, and shall provide that such records documenting the use of ALPRs and ALPR stored data shall be maintained for 5 years and shall be kept in a place and in a manner as to facilitate a review and audit of the department's ALPR program by the County Prosecutor or by the Attorney General or his or her designee.

e. The ALPR policy shall provide that any sworn officer or civilian employee of the agency who knowingly violates the agency's policy, or these Guidelines, shall be subject to discipline.

f. The ALPR policy shall provide that all significant violations of the agency's policy, or of these Guidelines, including but not limited to all instances involving the unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor, or to the Director of the Division of Criminal Justice in cases involving a state-level agency, upon discovery of the violation. Unless the County Prosecutor or Director elects to conduct or oversee the investigation of the violation, such notification of the violation shall be followed up with a report, approved by the chief of the department, explaining to the County Prosecutor, or to the Director, the circumstances of the violation, and the steps that are being taken to prevent future similar violations.

14.2 Notice of ALPR Policies and Revisions Provided to County Prosecutors or the Division of Criminal Justice

The chief of the department shall provide a copy of the agency's written ALPR policy to the County Prosecutor, or to the Division of Criminal Justice in the case of a state-level agency, at or before the time of promulgation, and shall provide to the County Prosecutor, or to the Division, copies of any amendments or revisions to the agency's ALPR policy at or before the time that such amendments take effect.

15. ALPR PROGRAM ACCOUNTABILITY

15.1 ALPR Program Audits

All ALPR records documenting the use of an ALPR, or access to or use of ALPR stored data, whether kept manually or by means of an automated record-keeping system, shall be subject to review and audit by the County Prosecutor, or by the Attorney General or his or her designee.

15.2 Handling of Complaints

Any complaints about a department's ALPR program made by any citizen or entity shall be forwarded to the appropriate County Prosecutor, or to the Director of the Division of Criminal Justice in the case of a State-level agency, for appropriate review and handling. The County Prosecutor, or Director, may conduct an investigation, or may direct the agency that is the subject of the complaint to conduct an investigation and to report back to the County Prosecutor or Director.

16. SANCTIONS FOR NON-COMPLIANCE

If the Attorney General or his or her designee has reason to believe that a law enforcement agency or officer or civilian employee is not complying with or adequately enforcing the provisions of these Guidelines, the Attorney General may temporarily or permanently suspend or revoke the authority of the department, or any officer or civilian employee, to operate an ALPR, or to gain access to or use ALPR stored data. The Attorney General or her designee may initiate disciplinary proceedings, and may take such other actions as the Attorney General in his or her sole discretion deems appropriate to ensure compliance with these Guidelines.

17. AUTHORITY OF ATTORNEY GENERAL TO GRANT EXEMPTIONS OR SPECIAL USE AUTHORIZATIONS

ALPRs, and all ALPR stored data, shall only be used and accessed for the purposes and in the manner authorized by these Guidelines. In recognition of the need to be able to address issues or circumstances that are not contemplated by these Guidelines, the Attorney General or his or her designee may grant an exemption from any provision of these Guidelines, and may authorize the specific use of an ALPR, or the data collected by or derived from an ALPR, that is not expressly authorized by these Guidelines. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by these Guidelines shall be made to the Attorney

General or his or her designee through the Director of the Division of Criminal Justice or his or her designee, who shall make recommendations on whether to grant the agency's specific request for an exemption or special authorization. Such requests shall be made in writing unless the circumstances are exigent, in which event the request by the agency and approval or denial by the Attorney General or his or her designee may be given orally, in which event the circumstances of the request and the approval or denial shall be memorialized in writing as soon thereafter as is practicable.

New York State

Suggested Guidelines:

Operation of License Plate Reader Technology

2011

STATE OF NEW YORK
Andrew M. Cuomo, Governor

Sean Byrne
Acting Commissioner
Division of Criminal Justice Services

Office of Program Development and Funding

Anne Marie Strano
Deputy Commissioner

New York State Division of Criminal Justice Services
4 Tower Place
Albany, NY 12203
http://criminaljustice.state.ny.us

16042

Table of Contents

Advisory Panel……..……3

Introduction……..……4

Part I. License Plate Reader Technology…….……..……4

Background and description

LPR Technology and Investigations

Part II. Legal Considerations…….9

License Plate Readers (Bianchi)

License Plate Readers and the Law (Zelenka)

Part III. Suggested policy/procedures…….…..……13

LICENSE PLATE READER ADVISORY PANEL

The New York State License Plate Reader (LPR) Advisory Panel is comprised of professionals with experience in various aspects of law enforcement and license plate reader technology. Original guidelines were developed in 2008; however, as LPR technology and court decisions have evolved since that time, it became necessary to review the guidelines.

During 2010, the Advisory Panel met to review the previous guidelines and to discuss changes in technology, applications and developments in various aspects of license plate readers (LPR). This document includes a history of the LPR project in New York State, general operations of LPR technology, practical guidelines for the deployment of LPRs and for the management of data derived from this technology.

William Zelenka, Assistant District Attorney, Bronx County, NY
Patrick Ryder, Detective Sergeant, Nassau County Police Dept., NY
John Ventre, Detective, Nassau County Police Dept., NY
Tom Lohmann, Director, National Insurance Crime Bureau
Kevin Gallagher, Special Agent, National Insurance Crime Bureau
Terence Hurson, Deputy Inspector, New York Police Dept., NY
Rich Belluci, Investigator, New York County District Attorney
Larry Wyman, Senior Investigator, NYS Dept. of Motor Vehicles
Eileen Langer-Smith, NYS Division of Criminal Justice Services
Michele Mulloy, NYS Division of Criminal Justice Services
Ken Buniak, NYS Division of Criminal Justice Services
Robert Fernandez, Lieutenant, New York State Police
Randy Morehouse, Sergeant, New York State Police
Kevin Chevier, NYS Division of Homeland Security and Emergency Services
James Burke, Inspector, Suffolk County Police Dept., NY
Steven Vandervelden, Assistant District Attorney, Westchester Co. District Attorney
Mark A. Spawn, Director of Research/Training, NYS Association of Chiefs of Police
Ken Middleton, First Deputy Director, New York / New Jersey HIDTA
Robert J. Poisson, Lieutenant, New York State Police
Matthew E. B. Brotmann, Special Advisor, NY Attorney General's Office

Part I

LICENSE PLATE READER TECHNOLOGY

16045

INTRODUCTION

This report has been prepared to offer guidelines and best practices for agencies using LPR technology (LPR systems can be an important asset to agencies in carrying out their law enforcement function). A carefully developed policy that addresses issues such as authorized uses, training, data retention, audit trails, dissemination and sharing of data will help to ensure that LPR technology remains an important tool for use by the law enforcement community.

The goal of these guidelines is to provide a basis upon which law enforcement agencies can build policies that provide authorized users with the information necessary to ensure public safety while protecting individual privacy rights. The LPR Advisory Panel urges agencies to use these guidelines in the development of their own agency protocols.

NOTE: The procedures outlined herein have been developed as a general framework for the development of a comprehensive policy for the deployment, use, and management of license plate readers and data. This document has been developed so that policymakers can modify certain procedures to best fit the needs, operations and resources of their individual agency. LPR technology has evolved rapidly and that progress will likely continue. As a result, administrators are encouraged to regularly monitor their policy as technological advances may require that procedures be updated to be consistent with such changes.

BACKGROUND AND DESCRIPTION: TECHNOLOGY

The concept of using cameras as a method to record a vehicle passing through a specific location and then identifying the owner/operator has been in development since the 1970s. Early technology could capture a picture of a license plate and vehicle with the date and time. Upon retrieving the plate number after searching hours of captured images, the plate number could then be manually searched against a database. This technology was time consuming, expensive and limited by lighting and weather conditions.[1]

License plate reader technology developed along with the use of videotape and camcorders. The analog videotape had to be converted from analog images to digital images and stored on a computer hard disk. The resulting digital images were further processed to locate and extract the license plate and time-stamp information through specialized software using character recognition techniques. This technology, while better than earlier methods, still had many drawbacks, including high costs that limited its general use by state and local governments. [2]

---

[1] Transportation Research Board, 2002. "Effects of Ambient Light, Camcorders, and Automated License Plate Reader Settings on Plate Transcription Rates".

[2] Transportation Research Board, 2002. "Reduction of Video License Plate Data".

The latest license plate reader technology has incorporated digital photography which eliminates the conversion steps and reduces the amount of computer file storage needed to support an effective system. Digital photography has also decreased the size of the camera hardware required and utilizes infrared lighting to address lighting and weather conditions. This has also reduced the overall costs for an effective system, making the technology obtainable at the local, county and state levels of government.

Today's LPR systems use specialized digital cameras and computers to quickly capture large numbers of photographs of license plates, convert them to text and compare them quickly to a large number of plates of interest. LPR systems can identify a target plate instantly, allowing law enforcement to identify target vehicles that might otherwise be overlooked. The technology is available in mobile systems mounted on police cars, and fixed/portable systems that can be mounted on poles or on the roadside.

A range of camera systems are available, most capable of reading license plates during the day or night and in a variety of weather conditions. The systems operate fast enough to capture all of the license plates they come into contact with so that the number of license plates that can be read is limited only by the number of vehicles passing the cameras. LPR systems typically include infrared strobe and camera systems that can take high speed, high contrast images that allow plates to be read at closing rate speeds of 150 miles per hour.

Mobile license plate reading systems are designed to allow officers to patrol at normal speeds while the system reads license plates and alerts the officer if there is a match to a "hot list." "Hot lists" contain a large list of target plates stored within the vehicle's LPR computer. This is essential due to the volume of plates scanned by the LPR and the necessity for an immediate alert if a target plate is scanned. Currently, "hot lists" are transferred daily by state and federal authorities and can be updated by the LPR operator through a hard-link or wireless upload. "Hot lists" may contain a variety of plate data, including terrorist watch lists, stolen cars and parking scofflaws.

When a target plate is scanned, the officer is notified with a message. The alert can be specific to the plate, and some alerts can be customized by the user/agency. Once a "hot list" has been uploaded into the LPR computer, it can be updated automatically or manually. For example, once a daily upload has been made, any recent car thefts, for example, will not be posted until the next (daily) upload. Most LPR systems allow the user to add plates to, and delete plates from, the "hot list". This is particularly useful for crimes that recently occurred, AMBER Alerts, Be-on-the-LookOut (BOLOs), for cases in which stolen vehicles have been recovered, or other situations in which the alert can be cancelled. Some LPR systems can also alert the driver if a manually entered "hot list" entry was recently scanned. Integrated GPS technology allows the operator to locate the last contact with the vehicle.

The use of LPR technology in law enforcement has included a variety of applications: homeland security, electronic surveillance, suspect interdiction, stolen property recovery, facility management and more. The identification of stolen vehicles, stolen license plates, and wanted and missing persons was the primary focus of most early implementations.

LPR systems record every license plate scanned. Some systems record the location, date and time of each scan. This intelligence resource is available as a law enforcement tool, allowing the officer to identify the last known contact with a vehicle and also to report the list of vehicles located in a specific area within a given time range.

Most LPR systems include a set of cameras, most of them infrared-illuminated. Some include "progressive" cameras that capture images at a variety of computer-controlled lighting conditions by actively managing infrared strobes integrated into the cameras. These cameras are typically mounted outside of the vehicle as auto glass can interfere with their operation. Most cameras are mounted either permanently on the rooftop or trunk, magnetically in a transportable configuration, integrated into the light bar, or within a covert housing.

Some implementations of LPR use a dedicated computer for the high-intensity camera and image management while others use the in-car computer. In either case, the cameras connect to a computer and display that can be the same mobile data terminal or in-car computer. Typically, LPR systems only require the operator to have one computer display in the vehicle. The processor in an LPR system can include a specialized computer that manages the cameras and allows the system to run at very high speeds regardless of the speed or power of the existing in-car PC.

LPR software typically has three components – the character translation component (Optical Character Recognition), the hot list management component and the user interface. Other additional software components manage GPS information, plate read, alarm history, and reporting features.

The Optical Character Recognition (OCR) of images taken by LPR cameras is performed through the use of sophisticated algorithms. Six primary algorithms that LPR system software requires to identify a license plate are:

1. Plate localization, which finds and isolates the plate contained in the picture;
2. Plate orientation and sizing, which compensates for the skew of the plate and adjusts the dimension to the appropriate size and shape;
3. Normalization, which adjusts the brightness and contrast of the image;
4. Character segmentation, which finds the individual characters on the plates;
5. Optical character recognition, which converts the image into actual characters, and
6. Syntactical / Geometrical analysis, which checks characters and positions against specific rules to identify the license plate state of issuance. [3]

The "hot list" management component enables the LPR to obtain daily updates to the "hot list", maintain "hot list" files and retain all relevant files per time frame established by the law enforcement agency. The agency then may choose to upload the data retained in the LPR to a designated server for retention. The user interface manages LPR activity and allows the user to quickly identify an alarm and the target vehicle. In most cases, most of the screen

[3] International Association of Chiefs of Police, 2009, Privacy impact assessment report for the utilization of license plate readers, pp 5-6 (September, 2009).

space on the user interface is reserved for the target vehicle/plate photo as that is the primary means for alarm vehicle identification. The interface also allows the user to enter additional target plates, check information in the "hot list", and deal with the visual and audible alarm queues. The Global Positioning Software (GPS) enables the LPR to record date, time and location of license plate scans.

LPR TECHNOLOGY AND INVESTIGATIONS

LPRs are an excellent resource to aid in criminal investigations. For the purpose of this document, investigative applications are discussed as active and passive. The active search describes situations in which license plate data is uploaded to an LPR computer, generally with an alarm that will indicate the nature of the entry. For example, LPRs used by patrol officers and detectives might contain lists of wanted subjects. The passive search focuses on the investigative or crime analysis level of enforcement in researching data already collected.

Part II

LEGAL CONSIDERATIONS

16050

MEMORANDUM

TO: Local Law Enforcement Agencies

FROM: Gina L. Bianchi
Deputy Commissioner and Counsel

DATE: October 26, 2006

SUBJECT: License Plate Readers

There does not appear to be any legal impediment to the use of a license plate reader by law enforcement. It does not appear that such use would constitute a Fourth Amendment search. An observation made by a police officer without a physical intrusion into a constitutionally protected area does not implicate the Fourth Amendment or require a search warrant (see, Hester v. United States, 265 U.S. 57 [1924]). A police officer who is lawfully present in an area may look into the windows of a parked car (see, United States v. Martin, 806 F.2d 204[1986]).Given the foregoing, it seems clear that a police officer's observation of a license plate on a car located in an area viewable from a public street would not constitute a search. The use of a license plate reader to enhance the officer's observation would likely not cause the observation to become a search for purposes of the Fourth Amendment. For example, the use of artificial illumination to aid an officer's observations does not constitute a search (see, United States v. Lee, 274 U.S. 559 [1927]; People v. Hughes, 211 A.D.2d 576, 622 N.Y.S.2d 12 [1995]; People v. Vasquez, 229 A.D.2d 997, 645 N.Y.S.2d 672 [1996]). Similarly, the use of binoculars to magnify an object does not constitute a search (see, United States v. Lee, supra). A license plate reader merely accomplishes, more efficiently, the same task that a police officer may accomplish by reading a license plate and manually entering the number into a data-base. Therefore, it is reasonable to assume that a court would not hold that the use of a license plate reader would constitute a search. However, at this time there is no decisional case law from any court concerning the use of a license plate reader.

The foregoing information concerning the use of license plate readers is advisory only and is meant to provide guidance and highlight points to consider in developing a policy to govern the use of license plate readers. It is recommended that each law enforcement agency consult with its own legal advisor prior to adopting a policy regarding the use of license plate readers.

LICENSE PLATE READERS AND THE LAW (NEW YORK)
ADA WILLIAM ZELENKA, BRONX COUNTY DISTRICT ATTORNEY'S OFFICE

The law surrounding the use of License Plate Readers is in its infancy. As technology involving the ability to track individuals has advanced over the last few years, the law is playing catch-up. In New York, a case from the Court of Appeals in March 2009 regarding GPS tracking devices appears to indicate the current direction of the clash between law enforcement's use of technological advancements and the privacy concerns of citizens. This issue is unfolding across the country.

The License Plate Reader (LPR) is a device which represents the marriage of a series of cameras connected to a computer which downloads a hotlist of license plates of interest. Depending on the state, the hotlist usually originates from the Department of Motor Vehicles or State Police. The system can capture over 3,000 plate images per minute. It can be stationary or mobile, including being mounted on helicopters. Mobile devices can capture plates travelling well beyond the legal speed limit or plates parked bumper to bumper with another vehicle. These alphanumeric reads are then compared with the hot list. In New York, the hotlist is downloaded through the State Police, having been obtained from the Department of Motor Vehicles (DMV). Plate numbers may also be manually entered by the vehicle operator. Examples would be in response to an AMBER Alert or while conducting an ongoing investigation. Multiple vendors currently have LPRs on the market, with differences in quality and performance.

In their initial release years ago in New York, LPRs could only be updated by driving the LPR vehicle to a limited number of sites where the hotlist could be updated. Updates were only available once per day. The Division of Criminal Justice Services (DCJS) had established protocols for the use of LPRs by law enforcement, and the NYPD had issued guidelines for the "use, maintenance and accountability" of each LPR (NYPD Operations Order No. 33). One of the first cases in New York that dealt with the protocol originated in Bronx County. In People v. Davila, 27 Misc. 3d 921, 901 N.Y.S. 2d 787 (2010), the officer who was conducting an LPR-based car stop, which resulted in the recovery of a gun, had not updated the system nor confirmed the hit prior to the stop, both of which were protocol recommendations. After conducting an extensive hearing on the issue, the Court ruled that the NYPD guidelines were recommendations, not law. Having found the officer's conduct otherwise proper, suppression of the weapon was denied.

Another New York State case which utilized an LPR to help convict two defendants charged with arson and homicide of a family of five in 2007 was People v. Mark Serrano and Charles Gilleo, (Indictment no. 16/2007). In this case, a New York State trooper car in Dutchess County was on patrol with its LPR capturing plates. Prior to a radio run of a house on fire, the LPR captured a plate which was later determined to belong to one of the defendants, placing his car in the vicinity of the crime minutes after the fire was started. The photo of the plate also possessed unique identifying features on the front of the vehicle confirming that it was the defendant's car.

(ADA William Zelenka; rev. Sept. 2010)

LICENSE PLATE READERS AND THE LAW (NEW YORK)
ADA WILLIAM ZELENKA, BRONX COUNTY DISTRICT ATTORNEY'S OFFICE

The License Plate Reader (LPR) constitutes one of the latest computer based investigatory tools to be used by officers in the field. The system requires an ongoing download of target license plates emanating from the Department of Motor Vehicles and the State Police. The hardware required is either attached to a vehicle or mounted as a standalone. The scanner reads all license plates which are within view and compares them with the wanted database. The computer also stores the location of every read via GPS. When the computer matches a plate with the database, it notifies the operator (a police officer in most cases) of the reason for the match, and shows a color photo of the image capture. A record of every plate read and its result is kept. The officer confirms the hit and a car stop occurs. If an arrest is made and the officer testifies at a hearing or trial, is the information contained in the computer Rosario?

Rosario material is part of the discovery process found in Sections 240.44 and 240.45 of the Criminal Procedure Law (CPL). It is "Any written or recorded statement…made by such witness…which relates to the subject matter of the witness's testimony." The statement must be in the possession or control of the People.[1] It must relate to the subject matter of the witness's direct testimony.[2] But the People are not required to create Rosario material.[3] If the material is deemed to be Rosario, the People are obligated to turn it over if it is under their control.

There is no question that the information stored in the computer is under the control of the operator. The remaining issue is whether the hit (data) the operator relies on to proceed to the confirmation step is a statement. Although the data is a written instrument under the Penal Law[4], it should be argued that it is **not** a statement by the operator/officer. Statements are either recorded or written notations of the witness. In the case of LPRs, the data generated has no connection to any statement made by the operator/officer. However, any notes made during the confirmation process by the operator/officer to verify the information would be Rosario because they would constitute notes which the operator/officer would be expected to testify about.

LPRs have the ability to store any information which the operator/officer requests. It is recommended that any scans which lead to arrests be stored in the computer until such time that a court in your jurisdiction definitely rules that the scan alone is not Rosario.

[1]People v. Rosario, 9 N.Y.2d 286 (1961)
[2]People v. Roebuck, 279 A.D.2d 350 (1st Dept. 2001)
[3]Peoplel v. Steinberg, 170 A.D.2d 50 (1st Dept. 1991)
[4]Penal Law §170.00

(ADA William Zelenka)

Part III

SUGGESTED POLICY/PROCEDURES

16054

SUGGESTED POLICY/PROCEDURES: LICENSE PLATE READERS
DATE:
REVIEW DATE:
SECTION:

Editorial note: *Policymakers are encouraged to customize this document for their own agency, giving consideration to personnel/assignments, resources, and infrastructure, among other things. Blank lines and italicized language has been inserted as a guide for the development of your customized protocols. Be sure to delete any blanks or italicized language before saving your final document.*

I. PURPOSE: The purpose of this policy is to provide members and staff with guidance on the application and use of license plate readers (LPR), management of LPR data, and maintenance of LPR equipment.

II. POLICY: License plate readers have enhanced law enforcement's ability to detect violations of law, recover stolen property, apprehend fugitives, assist in investigations and more. Members and staff will use LPRs in accordance with the procedures and guidelines set forth. Further, data captured from LPRs will be used properly and responsibly as defined herein.

III. DEFINITIONS

Department: the _____ Police/Sheriff's Department/Office.

Fixed camera: permanently affixed to a structure such as a pole, overhead, or bridge.

GPS: global positioning system.

LPR: license plate reader.

LPR Data Query Logs: a record of a search or query of LPR data from (the server).

Hot List: data is provided through the New York State Integrated Justice Portal and includes license plate numbers of stolen vehicles, stolen license plates, wanted person with a license plate associated with the record, and suspended or revoked registrations. Also includes national data (i.e. NCIC, NICB) for similar categories, and for license plates associated with AMBER Alerts, terrorist watch lists and the like; also includes manually entered license plate information for crimes just occurred in a local jurisdiction, gang members, wanted persons, and other investigative targets.

Members: sworn police officers of this department.

Mobile camera: affixed to a vehicle permanently or magnet-mount.

MOU: memorandum of understanding.

OCR: optical character recognition.

Portable camera: stationary but are capable of being moved as needed, such as a traffic barrel or speed radar sign.

SOP: standard operating procedure.

Staff: non-sworn employees of the Department.

IV. GENERAL ADMINISTRATION

a. LPRs will be used only by members who have been properly trained in the use of same. *(designation of personnel authorized to use LPR_____)*

b. LPR data may be accessed by members for a legitimate law enforcement purpose. (*designation of personnel authorized to access LPR data_____)*

c. LPR data may be accessed by staff who have been authorized by *(specify position, i.e. Chief/Sheriff/Detective Captain/etc._____)* for a legitimate law enforcement purpose.

d. The *(specify person/position_____)* is responsible for receiving reports of LPR defects, damage or other matters requiring maintenance of the Department's LPR systems.

e. The *(specify person/position_____)* is responsible for the maintenance of data including backing up of LPR data, requests for searches or LPR data, and for maintenance of internal hot lists.

f. The *(specify person/position_____)* is responsible for the inventory of LPRs within the Department and for ensuring that the Department has included all LPR equipment valued at more than *(indicate threshold, i.e. $2,000, $5,000, $10,000, etc._____.)* is included for coverage on the municipality's insurance plan.

g. The *(specify person/position_____)* is responsible for the annual review of the policy and procedures contained herein and for making recommendations to the *(Chief/Sheriff_____)* for any necessary amendments thereto.

h. LPR hot lists and data gathered by Departmental LPRs will be maintained securely. Requests for searches may be made by members of this Department or by other law enforcement agencies subject to the provisions of this policy *(or state other permissible uses, sharing or restrictions_____).* Also see ____ (i.e.: Section VI(b), below)

i. Prior to the use of mobile LPR equipment, members must receive training administered by *(specify_____).* The *(specify_____)* will ensure that any changes in hardware, software or law are the subject of continued in-service training or bulletins.

V. OPERATIONS

a. Prior to a tour of duty, members using an LPR will ensure that an upload of hot list data from the Integrated Justice Portal has been performed for that day.

b. Data from field LPRs, whether mobile or portable, will be uploaded to *(specify, i.e. the Department's server_____)* via *(specify method of transmission, position responsible, and how often, i.e. via flash drive by the LPR Data Custodian_____).*

c. When enforcement action, an investigation or prosecution results from an LPR hit, the hit will be preserved via *(specify method in which you will document the hit_____).*

d. LPRs may be used in special operations or details such as high crime area patrols, STOP DWI initiatives, enforcement details, directed criminal investigations, etc. subject to the authorization of *(position_____).*

e. When violent crimes occur, this Department may solicit assistance from other agency's with LPR-equipped cars for assistance in identifying a vehicle or to gather license plate data in a particular area. Similarly, other departments may request assistance from this Department in the event of the same. Any mutual aid requests will be directed through the *(specify position, i.e. Duty Sergeant, Desk Officer, Duty CID Detective, etc. _____).* Consideration should be given to deploying LPRs strategically such as at a perimeter, choke points, major highways, other avenues of escape, etc.

VI. LPR DATA

a. Members may request of *(specify position_____)* that certain license plate numbers *(complete or partial_____)* be entered into the Department's Hot List. Examples of entries include:

    1. Gang members/associates
    2. Sex offenders
    3. Crime suspects
    4. Fugitives
    5. Search warrant targets

b. Access to LPR data shall be limited to *(specify positions/personnel, designees_____).*

c. Members making inquiries must make a log entry onto the LPR Query Log.

d. If the LPR Query Log contains a hit with an arrest associated with it, the LPR Query Log must be retained as part of the case file.

e. LPR Data Query Logs shall be maintained and secured for future audits.

f. Access to LPR data must be for a legitimate law enforcement purpose.

g. Members or staff conducting a query on behalf of an authorized requestor should make a log entry.

h. Requests to review stored LPR data and search results will be recorded and maintained in appropriate case files.

i. LPR data will be transferred/uploaded on a *(specify timeframe, i.e. daily/weekly/monthly_____)* basis by *(specify position responsible_____)* to the *(specify destination of data, i.e. central server, crime analysis center, etc._____.)*

j. LPR data from all mobile, portable and fixed LPRs will be managed by *(specify person/position_____).*

k. LPR data will be stored in the Department's *(specify, central server/other_____)* for a period of no less than *(specify_____),* except in the following circumstances:

    1. LPR records will be maintained for *(time_____)* and/or until a final disposition has been reached in the particular case.
    2. LPR hits associated with an arrest will be maintained in the criminal case file and retained for the maximum period of time associated with such record.
    3. LPR hits associated with felony investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.
    4. Whenever otherwise directed by the *(specify command position_____)*

l. Sharing and dissemination *(describe your agency's authorized LPR data sharing procedures, i.e. In addition to the procedures in Section VIII below, access to LPR data shall be limited to designated personnel who have been provided account access or who have been specifically authorized to access or search LPR data; data will be uploaded to the Crime Analysis Center, etc. or to other law enforcement entities upon the direction of the Chief of Police/Sheriff/Commissioner, etc.; note whether certain sharing is done routinely, and/or upon specific request of a law enforcement agency, etc.)*

m. Backing up of LPR data system *(designation of position responsible for preserving LPR data, frequency, redundancy and method of backup)*

VII. FIELD PROTOCOLS

a. PATROL – LPRs are useful in general patrol assignments when the patrol vehicle is in a position to monitor vehicular traffic. LPRs may only be used for a legitimate law enforcement purpose.

b. Members may not use a mobile LPR unless properly trained in its use and operational protocols.

c. LPR-equipped vehicles should be used as often as possible. When not in use, LPR-equipped vehicles should be secured.

d. Members will ensure that a daily upload of hot list data has been performed to the LPR system so as to prevent stops using outdated data.

e. When the LPR indicates a hit, prior to making the stop, the member must

    1. Verify that the captured plate image matches the plate number of the vehicle
    2. Confirm that the hit is accurate through dispatch, etc.

f. The proactive entry of data or access to LPR records must be for a legitimate law enforcement purpose by authorized personnel. This applies to data uploaded prior to the deployment of the LPR as well as data which may be uploaded by a member during a tour of duty. Proactive/manual entry of LPR hot list in the field is <u>permitted</u> for:

    1. Dispatch reports of crimes, BOLOs, alerts in which a license plate number is part of the broadcast
    2. When directed or authorized by *(specify: dispatch, Sergeant, CID, etc. _____)* and which must be for a legitimate law enforcement purpose.
    3. members should query their LPR to ascertain if there is a prior read of the license plate which is the subject of the particular alert, bulletin or alarm.

g. Proactive/manual entry of LPR hot list in the field is <u>required</u> for AMBER Alert or Missing Child or College Student Alert bulletins. Additionally, members must query their LPR to ascertain if there is a prior read of the license plate which is the subject of the alert.

h. Members will make an entry in the LPR Daily User Log whenever the LPR is used.

    1. Upon completion *(or when the log is filled_____)*, the LPR Daily User Log will be forwarded to the *(specify person/position_____).*
    2. The *(specify person/position)* will ensure that entries are complete.
    3. If the LPR Daily User Log has an arrest or associated hit, it will be retained in the case folder.
    4. The LPR Daily User Log will be retained until all arrests have reached a final disposition.

VIII. INVESTIGATIVE PROTOCOLS

a. Access to stored LPR data shall be limited to *(specify positions authorized_____).*

b. Members conducting LPR data inquiries must have been granted access by *(specify person/position_____).*

c. Requests to review stored LPR data shall be recorded and maintained in the same manner as criminal history logs.

d. All inquiries of LPR data will be recorded by the member making the inquiry in the LPR Data Query Log.

e. LPR Data Query Logs will be retained until all matters have reached a final disposition.

IX. LPR MAINTENANCE

a. At the beginning of each tour of duty, members should verify the aim of the LPR camera(s) to ensure they are reading the correct lanes of traffic.

b. Camera lenses may be cleaned with glass cleaner sprayed on a soft cloth.

c. Any damage shall be reported immediately to the *(specify LPR Administrator_____).*

d. Technical questions concerning the LPR shall be directed to the *(specify LPR Administrator_____)*

Authorized by: _____ Chief/Sheriff

Date:_____

Appendix B: IACP ALPR Survey Instrument

16062

International Association of Chiefs of Police
2009 Survey of Law Enforcement Agencies
Policy and Operational Guidance for Law Enforcement License Plate Readers

Grant No. 2007-MU-MU-K004

CONTACT INFORMATION OF SURVEY RESPONDANT

Name:

Title:

Agency:

Address:

Suite/Bld:

City:

State:

Zip Code:

Telephone: Ext:

E-mail:

IMPORTANT: Please read the instructions below prior to completing this questionnaire.

- Do not leave any questions blank.
- For the purpose of this survey, license plate reader (LPR)system types are defined as follows:
  - Mobile = Camera(s) affixed to a vehicle
  - Fixed = Camera(s) permanently affixed to a structure such as a pole, bridge, or overhead sign
  - Portable = Camera(s) that are stationary but capable of being moved as needed, such as a unit in large traffic barrel, trailer, etc

If you have any questions about these instructions or this survey, please contact Meghann Tracy at (703) 836-6767 ext. 387 or tracy@theiacp.org

LICENSE PLATE READER (LPR) SYSTEMS POLICY & OPERATIONAL QUESTIONS

GENERAL QUESTIONS

1. Does your agency have a strategic operational plan for license plate readers (LPR)?

   ○ Yes ○ No ○ I don't know

   1.1 If yes, may we obtain a copy?

   ○ Yes ○ No ○ I don't know

2. Do you have a specific policy regarding LPR?

   ○ Yes ○ No ○ I don't know

   IF YES

   2.1 May we obtain a copy?

   ○ Yes ○ No ○ I don't know

   2.2 What elements are included in your policy? (Check all that apply)

   ☐ Data Access
   ☐ Data Sharing
   ☐ Data Quality
   ☐ Data Retention
   ☐ Public requests for information
   ☐ Other (please explain) _____
   ☐ I don't know

3. What was your primary purpose for acquiring a LPR systems?

4. Has that focus expanded?

   ○ Yes ○ No ○ I don't know

   If yes, please describe:

5. In which of the following areas are you using LPR data? (Check all that apply)

- ☐ Traffic initiatives of enforcement
- ☐ Crime Analysis
- ☐ General investigations efforts
- ☐ Narcotics
- ☐ Smuggling
- ☐ Gang enforcement
- ☐ Auto theft
- ☐ Other (please explain) _____
- ☐ I don't know

6. What have been the benefits of LPR technology use in your agency? (Check all that apply)

- ☐ Increase in stolen vehicle recoveries
- ☐ Increase in arrests
- ☐ Increase in productivity by officers
- ☐ Increase in crimes solved by using the LPR data
- ☐ Other (please explain) _____
- ☐ I don't know

7. On a scale of 1 to 5, with 1 being minimally beneficial and 5 being very beneficial, how beneficial have LPRs been to your agency?

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

8. Have you noticed any countermeasures being taken to thwart LPRs?

○ Yes ○ No ○ I don't know

If yes, what where those countermeasures and how have you responded?

9. Do you have plans to expand your current LPR capability?

○ Yes ○ No ○ I don't know

If yes, please explain.

10. Who owns the LPR data your agency collects? (Check all that apply)

- ☐ Our agency
- ☐ Regional agency (please explain)_____
- ☐ Vendor
- ☐ Other (please explain) _____
- ☐ I don't know

11. Are you part of a regional LPR effort or initiative?

○ Yes ○ No ○ I don't know

If yes, please explain.

DATA ACCESS AND RETENTION SUBSECTION

1. Does your agency have a written policy regarding retention of your LPR data?

○ Yes ○ No ○ I don't know

IF YES

1.1 May we have a copy of your agency's policy?

○ Yes ○ No ○ I don't know

2. Does your agency have an electronic media evidence data retention policy?

○ Yes ○ No ○ I don't know

IF YES

2.1 May we have a copy of your agency's policy?

○ Yes ○ No ○ I don't know

3. What is the period of time that you currently retain your LPR data? _____
4. What were the key factors in determining length of retention?

5. If you use more than one type of LPR (mobile, fixed, portable), is there a difference in retention time between the different types?

○ Yes ○ No ○ Not applicable ○ I don't know

IF YES

5.1 Please explain.

6. Does your agency retain both the photos and the plate information for the full retention period established by your agency?

○ Yes ○ No ○ I don't know

IF NO

6.1 Please explain your process

7. Is your agency aware of any LPR pertinent legislation passed by a governing body that affects or restricts your agency?

○ Yes ○ No ○ I don't know

IF YES

7.1 Please explain.

8. Are there restrictions in your agency as to who can query LPR data (e.g. conduct a check to see if a plate is in the system and where it was captured)?

○ Yes ○ No ○ I don't know

IF YES

8.1 Please explain.

9. Does your agency's LPR system have audit capability? (i.e. The ability to determine who as conducted a query and what was queried?

○ Yes ○ No ○ I don't know

LICENSE PLATE READER (LPR) SYSTEMS TECHNICAL QUESTIONS

GENERAL QUESTIONS

1. Does your current system support LPR data without negatively impacting your network?

   ○ Yes ○ No ○ I don't know

   IF NO

   1.1 Please explain.

2. Have you experienced LPR data loss based on inadequate bandwidth?

   ○ Yes ○ No ○ I don't know

3. Which best describes the where your LPR data is stored?

   ☐ On the hard drive of the laptop computer that is in the mobile LPR unit

   ☐ On a dedicated hard drive that is maintained at our agency

   ☐ On a server that supports multiple LPR feeds (fixed, mobile, portable)

   ☐ Ona regional server that holds data from more than just our agency

   ☐ Other (please explain) _____

   ☐ I don't know

4. What is the file size of an individual LPR capture? _____

FIXED LICENSE PLATE READER (LPR) SUBSECTION

The questions in this section refer exclusively to fixed LPR systems which are defined as those that are permanently affixed to a structure such as a pole, bridge, or overhead sign.

1. Does your agency use fixed LPR systems?

   ○ Yes ○ No ○ I don't know

   IF NO

   Please skip the remainder of this section and go on to the Portable License Plate Readers (LPR) Subsection

2. When did you first *deploy* your fixed LPRs? (Please use month/year XX/XXXX) _____
3. How many fixed LPR units does your agency have? _____
4. How many locations have fixed LPR cameras? _____
5. Do your fixed LPR locations have dedicated cameras for each lane of traffic?

   ○ Yes ○ No ○ Some do and some do not ○ I don't know

6. What information is captured by your agency's LPRs? (Check all that apply)

- ☐ Time and Date
- ☐ GPS coordinates
- ☐ Conceptual photo (e.g. car make and model, vehicle passengers)
- ☐ Image of plate
- ☐ Other (please explain) _____
- ☐ I don't know

7. How does your agency transfer data to/from LPR units? (Check all that apply)

- ☐ USB stick
- ☐ Wi-fi or hot spot
- ☐ Cellular
- ☐ Radio modem (e.g. 700 MHz, 800 MHz, VHF, UHF, etc.)
- ☐ Mesh
- ☐ Other (please explain) _____
- ☐ I don't know

8. How often are the captured plates (plates read by the LPR) transferred to your database?

- ☐ Once a day
- ☐ Each shift
- ☐ Multiple times per shift
- ☐ Real time or near real time
- ☐ They stay on the computer in the vehicle
- ☐ Other (please explain) _____
- ☐ I don't know

9. Which of the following are included in your alert/hot list for fixed LPR? (Check all that apply)

- ☐ Stolen vehicles
- ☐ Stolen plates
- ☐ Wanted persons
- ☐ Probationers and/or paroles
- ☐ AMBER alerts
- ☐ Registered sex Offenders
- ☐ Documented gang members
- ☐ Suspended/revoked drivers
- ☐ No insurance
- ☐ Parking scofflaws
- ☐ Other (please explain) _____
- ☐ I don't know

10. How often is the alert list (hot list) updated?

- ☐ Once a day
- ☐ Each shift
- ☐ Multiple times per shift
- ☐ Real time or near real time
- ☐ Other (please explain) _____
- ☐ I don't know

11. On a scale of 1 to 5, with 1 being Very Poor and 5 being Very Good, please rate the ability of your agency's LPR system to perform under each of the following conditions:

Daylight

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Night

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Rain

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Fog

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Dust Storm

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Snow

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Low speed (i.e. Urban/suburban streets

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

High speed (i.e. Highways

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Installation Questions

12. Which of the following factors did you consider during planning for your fixed LPR deployments? (Check all that apply)

- ☐ Infrastructure (e.g. existing poles, signage or structure that could be used)
- ☐ Connectivity (ability to connect with the internet/intranet
- ☐ Permitting requirements
- ☐ Access to power
- ☐ Key ingress/egress point
- ☐ Mission oriented enforcement
- ☐ Ability to intercept or predict course of travel of vehicle after alert
- ☐ Other (please explain) _____
- ☐ I don't know

13. Who performed the installation of your fixed LPR (check all that apply)

- ☐ Agency personnel
- ☐ LPR Vendor
- ☐ Contractor
- ☐ Other (please explain) _____
- ☐ I don't know

14. How are your fixed LPR systems mounted (check all that apply)

- ☐ Dedicated (solely for LPR use) pole mounts
- ☐ Bridge mounts
- ☐ Light poles
- ☐ Existing signage structure
- ☐ Other (please explain) _____
- ☐ I don't know

15. How are your fixed LPR systems powered? (Check all that apply)

- ☐ AC
- ☐ Battery
- ☐ Solar
- ☐ Wind
- ☐ Other (please explain) _____
- ☐ I don't know

16. Was a permit process required for installation? (Check all that apply)

○ Yes ○ No ○ I don't know

IF YES

16.1 Who handled the process? (Check all that apply)

- ☐ Agency
- ☐ LPR vendor
- ☐ Contractor
- ☐ City/County/State
- ☐ Other (please explain) _____
- ☐ I don't know

16.2 Approximately how long did the permit process take? _____

Hardware/Software

17. Which of the following does your LPR system use? Check all that apply)

- ☐ Black & white camera for conceptual photo
- ☐ Color camera for conceptual photo
- ☐ Infrared camera for plate
- ☐ Other (please explain) _____
- ☐ I don't know

18. Has your agency experienced any hardware failures with your fixed LPR system?

○ Yes ○ No ○ I don't know

19. Has your agency experienced any software failures with your fixed LPR system?

○ Yes ○ No ○ I don't know

20. Have there been any software conflicts as a result of your fixed LPR system?

○ Yes ○ No ○ I don't know

International Association of Chiefs of Police
515 North Washington Street
Alexandria, Virginia 22314