Attachment #3

Privacy Impact Assessment Report for the Utilization of License Plate Readers

Compiled by the International Association of Chiefs of Police

Privacy impact assessment report for the utilization of license plate readers

September 2009

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

IACP Leadership and Project Personnel

Executive Staff

Chief Russell Laine
President

James McMahon
Deputy Executive Director

Daniel Rosenblatt
Executive Director

Vincent Talucci
State and Provincial Police Director

Project Staff

Meghann Tracy
Project Manager, IACP Technology Center

Heather Ruzbasan Cotter
Senior Program Manager, IACP Technology Center
IACP LEIM Staff Liaison

William Nagel
Legal Consultant

Acknowledgements

The IACP would like to thank the law enforcement practitioners and subject matter experts who volunteered their time, expertise, and experience to create this document. Without their hard work and extraordinary collaboration on the *Privacy Impact Assessment for the Utilization of License Plate Readers* this document would not be possible. Thank you all for your continued commitment, time, energy, and patience. It is truly appreciated.

We would also like to thank the IACP Law Enforcement Information Management Section Board whose support has made this document possible.

IACP LEIM Section Board

CHAIR

Dean Hairston, Major
Danville (VA) Police Department

BOARD MEMBERS

Pamela Scanlon, Executive Director
Automated Regional Justice Information System (ARJIS)

Greg Browning, Chief of Police
Juneau (AK) Police Department

Ed Posey, Captain
Gainesville (FL) Police Department

Scott Edson, Captain
Los Angeles County (CA) Sheriff's Department

IMMEDIATE PAST CHAIR

Eddie Reyes, Deputy Chief
Alexandria (VA) Police Department

OVERSIGHT VICE PRESIDENT

Mark Marshall, Chief of Police
Smithfield (VA) Police Department
IACP 2nd Vice President

C

Contents

Executive Summary 1

Part 1. The Nature of License Plate Reader information 5

A. OVERVIEW: HOW LICENSE PLATE READERS FUNCTION 5

B. INFORMATION POTENTIALLY COLLECTED BY LPRs 6

C. POTENTIAL USES OF LPR DATA 7

D. LPR DATA IS NOT CONSIDERED PERSONALLY IDENTIFYING INFORMATION 7

Part 2. Types of privacy risks surrounding the use of LPRs 12

A. UNDERLYING PRIVACY CONCERNS 12

B. POTENTIAL CHILLING EFFECTS OF LPR SYSTEMS 13

C. IDENTIFICATION OF INDIVIDUALS VIA LICENSE PLATE NUMBERS 14

D. SECONDARY USE OF LPR DATA 15

E. AGGREGATION OF LPR DATA 16

F. POTENTIAL MISUSES OF LPR DATA 17

Part 3. Scope of the PIA Report 18

A. APPROACH OF THE ASSESSMENT 18

B. UNDERLYING PREMISES OF THIS REPORT 18

C. ISSUES NOT ADDRESSED IN THIS REPORT 19

Part 4. Collection of LPR data 21

A. LPR CAMERA DATA 21

B. LPR "HOT LISTS" 25

C. NOTICE OF DATA COLLECTION PRACTICES 27

Part 5. Access to and Dissemination of LPR data **30**

A. ACTIVE AND HISTORICAL LPR DATA 30

B. ACCESS TO LPR DATA 30

C. DISSEMINATION OF LPR DATA 31

D. UPDATING AND SHARING HOT LISTS 34

E. SECURITY SAFEGUARDS 34

Part 6. Retention of LPR data **36**

A. RETENTION OF CRIMINAL JUSTICE DATA, GENERALLY 36

B. CRITERIA TO CONSIDER WHEN ESTABLISHING RETENTION POLICIES 37

Part 7. Quality of LPR data **43**

A. INFORMATION QUALITY, CONCEPTUALLY 43

B. ACCURACY OF LPR COLLECTION OF LICENSE PLATE NUMBERS 44

C. ROUTINE DATA QUALITY AUDITS OF INFORMATION SYSTEMS 45

D. ACCURACY OF INFORMATION CONTAINED IN HOT LISTS 46

E. NO INDIVIDUAL RIGHT TO ACCESS OR CHALLENGE LPR DATA 46

Part 8. Accountability for LPR data **48**

A. AUDIT LOGS 48

B. SECONDARY DISSEMINATION LOGS 48

C. MONITORING AND CONDUCTING AUDITS OF SYSTEM USE 49

D. POLICY AWARENESS AND TRAINING 49

Appendix 1: 2007 Resolution on LPR Systems

Appendix 2: Issues Document

Appendix 3: List of Acronyms used in the PIA Report

Appendix 4: Footnote Reference List

ES

Executive Summary

This document addresses the privacy impact of the enhanced collection, analysis, and dissemination of license plate data made possible by the advent of license plate reader ("LPR") technologies.

Agencies interested in operating a LPR system do not have access to a uniform set of rules governing or even suggesting the appropriate uses and sharing of LPR data. This lack of regulation can cause the public to fear that the information collected by law enforcement agencies through their utilization of LPR systems might be mismanaged or misinterpreted with real-world consequences. Moreover, the potential misuse of LPR data may expose agencies operating such systems to civil liability and negative public perceptions.

The goal of this report is to set forth in a clear and concise manner the impact LPR systems can have on the public's privacy interests and to make recommendations for the development of information management policies intended to govern an agency's operation of a LPR system.

THE NATURE OF LICENSE PLATE READER ("LPR") DATA

License Plate Reader systems consist of high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates into computer-readable data. LPR systems typically utilize specialized cameras designed to capture images of license plates, whether from fixed positions or mobile patrol vehicles.

Images of vehicles and license plates are the primary form of information collected by a LPR system. Optical character recognition ("OCR") is performed on these images and the alphanumeric characters on each license plate are rendered into an electronically readable format. LPR systems can attach date, time, and location information to an image.

A license plate number does not identify a specific person; rather it simply identifies a specific vehicle. Although a license plate number may be linked or otherwise associated with an identifiable person, this potential is only 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 date, 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.

Nevertheless, this Report considers LPR data for official use only and discusses the appropriate protections a law enforcement agency should implement as part of a LPR system.

THE INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE 2007 RESOLUTION

In 2007, the International Association of Chiefs of Police ("IACP") passed a resolution in support of License Plate Reader (LPR) technology. That resolution strongly encouraged the U.S. Congress to fully fund license plate reader and related digital photographing systems, including interrelated information sharing networks, for the northern and southern borders of the United States. In support of this resolution, the IACP Law Enforcement Information Management ("LEIM") Section set out to develop this Privacy Impact Assessment ("PIA") Report.

TYPES OF PRIVACY RISKS SURROUNDING THE USE OF LPRs

LPR systems have the potential to reveal to the government individuals' driving habits. As LPR systems become more widespread, and as law enforcement agencies improve their information sharing capabilities, the potential to monitor where and when a particular vehicle has traveled is enhanced.

Recording driving habits could implicate First Amendment concerns. Specifically, LPR systems have the ability to record vehicles' attendance at locations or events that, although lawful and public, may be considered private. For example, mobile LPR units could read and collect the license plate numbers of vehicles parked at addiction counseling meetings, doctors' offices, health clinics, or even staging areas for political protests.

Several prominent privacy groups view information concerning individuals' locations as inherently prone to abuses, including expanding data uses beyond the original purposes of collection, sharing data with third parties beyond reasonable expectations, and heightening individuals' vulnerability to crime. Nevertheless, law enforcement agencies can develop policies that set forth the appropriate access and dissemination of LPR data; agencies can also prohibit and punish individuals who inappropriately disclose data from a LPR system. Moreover, agencies can conduct audits and monitor system operations to prevent and identify instances of misuse. As with other law enforcement data systems, security safeguards can also be implemented to limit unauthorized access to LPR data.

PURPOSES OF COLLECTING LPR DATA

Law enforcement agencies are charged with protecting the public as well as investigating crimes and criminal conduct. LPR systems serve four specific public safety goals. Specifically, LPR data can be used: (a) in various forms of crime analysis; (b) to alert law enforcement officials that a license plate number on a hot list is in proximity to a LPR camera; (c) to monitor the movements of vehicles operated by individuals subject to preexisting geographical limitations on their travel; and (d) to identify instances of criminal conduct that might have previously gone undetected without the aid of the LPR system.

Hot lists may be compiled by the local law enforcement agency utilizing the LPR system or by other state or federal government agencies. The purpose of these lists is to signal a law enforcement official that a vehicle displaying a license plate number that is included on a hot list is near a LPR camera.

ACTIVE AND HISTORICAL LPR DATA

Active LPR data is that information which is provided to an officer in real-time. It takes the form of alerts that a license plate number contained on a hot list is near a LPR unit, whether fixed or mobile. Historical LPR data is essentially a database containing the dates, times, and locations of individually identifiable motor vehicles; it is considered passive as it is essentially LPR data that is stored for future investigative or analytical use.

ACCESS AND DISSEMINATION OF LPR DATA

Appropriate access to active and historical LPR data is guided significantly by the purposes for which it is collected. Thus, LPR data may appropriately be accessed by law enforcement officials: (a) to support crime analysis efforts; (b) to alert law enforcement officials that a license plate included on a hot list is or has been near a LPR camera location; and (c) to help law enforcement officials detect instances of criminal conduct.

It may be appropriate to share LPR data with various agencies and individuals throughout the justice system. Any policy regulating the sharing of LPR data should clearly identify the receiving entity and the specific purpose for the dissemination. LPR data may be shared: (a) among law enforcement agencies; (b) with other, non-law enforcement government entities; and (c) in certain, limited circumstances with the public.

RETENTION OF LPR DATA

Agencies may be called upon to explain their reasons for retaining LPR data for as long as they do. Law enforcement agencies may consider several criteria as they develop a retention policy, including but not limited to statutes of limitation, the potential future usefulness of the LPR data, the relative sensitivity of the LPR data, and the LPR system's technologically implemented policy controls.

Although these criteria may be useful when deciding how long to retain LPR data, there is no formula for determining how long LPR data should be retained. There is considerable need to establish a set of guidelines, including standard criteria, to assist law enforcement agencies in their development of retention policies for LPR data.

QUALITY OF LPR DATA

Law enforcement agencies have no way to influence the accuracy of the OCR performed upon an image captured by a LPR camera. Nevertheless, law enforcement agencies will rely upon the accuracy of LPR data as they conduct their investigations. In addition to law enforcement

officers visually confirming the OCR read against the contextual image taken by the LPR camera, regular and systematic audits can help ensure that the quality of data contained in a LPR system remains high. Data quality audits are distinct from system usage audits and focus on the accuracy of the information. In the context of a LPR system, data quality audits concentrate on measuring the accuracy of the OCR output when compared with contextual images.

ACCOUNTABILITY FOR LPR DATA

Many privacy concerns surrounding LPR data can be mitigated by holding law enforcement agencies accountable for the information they collect and how they subsequently use that information. Several methods exist whereby agencies can ensure that their personnel are complying with applicable policies regarding the appropriate collection, use, and dissemination of LPR data. Creating tamper-proof audit trails as well as conducting real-time monitoring and analyzing LPR system usage can all function to protect the public's privacy interests. Training authorized users is also a critical accountability measure.

CONCLUSION

This Report discusses the privacy concerns surrounding a law enforcement agency's utilization of a LPR system and recommends certain measures that can address those concerns. This Report is also an exercise in good government. Transparency in government policy-making allows errors to be corrected through public criticism. Sometimes cogent and passionate arguments can persuade policy makers to see things in a truly new light; other times comments can come from a perspective that may be unavailable to those immersed in the administration of justice.

It is hoped that this Report provides a sound basis upon which law enforcement agencies can build meaningful LPR system policies that respects individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety.

1

Part 1. The Nature of License Plate Reader information

This Part discusses the types of information that can be collected by license plate readers ("LPRs"). Specifically, this Part provides a brief overview of how LPR systems work, the types of data they are capable of collecting, and how that information can subsequently be used. Whether license plate numbers and locations should be considered personally identifiable for purposes of drafting privacy policy recommendations is also discussed.

A. OVERVIEW: HOW LICENSE PLATE READERS FUNCTION

License Plate Reader systems consist of high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates into computer-readable data. Systems in existence as of the date of this report are routinely capable of capturing multiple license plate images per second on vehicles traveling at high speeds.[1]

Essential to any LPR system is the camera hardware that captures the image of the license plates. The quality of the captured image lays the foundation for the overall performance of the system. LPR systems typically utilize specialized cameras designed to capture images of license plates, either from fixed positions or mobile patrol vehicles. Factors which pose difficulty for license plate imaging cameras include the speed of the vehicles being recorded, the distance and angle of the vehicles from the camera; varying ambient lighting conditions, headlight glare, and harsh environmental conditions. In order to address these difficulties, many LPR systems employ infrared cameras operating in addition to visible light cameras.

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 include:

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 dimensions 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;

[1] Most LPR systems capture multiple images of the same vehicle and then use the best image; other systems are capable of capturing more than one vehicle per second.

5. Optical character recognition, which converts the image into actual characters; and
6. Syntactical/Geometrical analysis, which checks characters and positions against state-specific rules to identify the license plate's state of issuance.

Many LPR systems utilizing mobile LPRs are equipped with Global Positioning System ("GPS") Receivers. This allows mobile units to record the date, time, and location of license plate image capture. Data such as date and time stamps and GPS coordinates can be reviewed in relation to investigations and can help lead to critical breaks such as placing a suspect at a scene, witness identification, pattern recognition, or the tracking of previously identified suspects.

B. INFORMATION POTENTIALLY COLLECTED BY LPRs

LPR cameras take digital and infrared pictures of vehicles and license plates as they pass through the field of view of a LPR camera. These images, and the metadata associated with them, can be used in a variety of public safety contexts and the amount of information utilized from a LPR system can vary depending upon an agency's law enforcement mission. Thus, fixed LPR units in operation at national border crossings, which often operate in a setting consisting of slow-moving lanes of traffic, may collect different information than a mobile LPR camera operated by a local law enforcement agency. This Subpart describes the types of information that can potentially be collected by LPR systems as they function at the time of this Report. Agencies utilizing LPRs have the discretion to collect all or just a portion of the data elements described below.

Images of vehicles and license plates are the primary form of information collected by a LPR system. Optical character recognition is performed on these images and the alphanumeric characters on each license plate are rendered into an electronically readable format. LPR cameras can attach date, time, and location information to an image. The image collected by a LPR camera is maintained in the information system to provide a means of ensuring that the license plate number was properly converted into an electronically readable format. This digital image, sometimes referred to as a contextual photo, can include additional information that is not necessarily electronically recorded. Thus, LPR systems may contain information including, but not limited to, the following.

- Optical Character Recognition (OCR) of license plate numbers;
- Digital images of license plates as well as the vehicle's make and model;
- Digital image of the vehicle's driver and passengers;
- Images of distinguishing features (e.g., bumper stickers, damage);
- State of registration;
- Camera identification (mobile cameras may capture officer identification and vehicle/unit number);
- GPS coordinates or other location information; and
- Date and time of observation.

Together, these data elements are referred to as LPR data throughout this report.

C. POTENTIAL USES OF LPR DATA

Identifying the intended uses of LPR data is critical to assessing the privacy impact of law enforcement agencies' collection, analysis, and maintenance of license plate data collected via LPR systems. Moreover, how government agencies use the data they collect is of significant concern to the public. Thus, clearly articulating the purposes for collecting license plate numbers via a LPR system is one way to assist in the public oversight of governmental operations and serves a critical role in addressing privacy concerns surrounding the use of such a data system. Any sound privacy or information management policy intended to govern a LPR system should clearly identify the appropriate and intended uses of LPR data.

Law enforcement agencies are charged with protecting the public as well as investigating crimes and criminal conduct. LPR systems serve four specific public safety goals. Specifically, LPR data can be used: (a) in various forms of crime analyses; (b) to alert law enforcement officials that a license plate number on a hot list is nearby; (c) to monitor the movements of vehicles operated by individuals subject to geographical limitations on their travel; and (d) to identify instances of criminal conduct that might have previously gone undetected without the aid of the LPR system. Each anticipated use carries with it certain privacy concerns; these concerns are discussed later in this Report and should be addressed by any subsequently developed policy regulating the collection, maintenance, use, and retention of LPR data.

D. LPR DATA IS NOT CONSIDERED PERSONALLY IDENTIFYING INFORMATION

Technologies that pinpoint and record individuals' locations are improving in accuracy and growing in prevalence; in doing so, they are also provoking new conversations about what constitutes personal data. Privacy interests are only implicated by information that can be used to identify a unique individual. This section discusses whether a license plate number is considered a piece of personally identifying information for the purposes of this Report.

1. PERSONALLY IDENTIFIABLE INFORMATION DEFINED

Personally identifiable information is data that can be used to identify or locate a single person. The National Institute of Standards and Technology ("NIST") *Guide to Protecting the Confidentiality of Personally Identifiable Information* defines personally identifiable information ("PII") as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked

or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[2]

A single piece of data can be personally identifiable (e.g., social security number or fingerprints). Likewise, multiple pieces of data, when merged, can also be personally identifiable, even where each individual piece of data itself would not (e.g., date of birth plus name plus address). Moreover, law enforcement agencies have access to multiple databases; this is significant as data elements that can be linked together, although not sufficient to distinguish an individual when considered separately, could distinguish individuals when combined from multiple sources.

For example, suppose that two databases contain different PII elements and also share some common PII elements, such as license plate numbers. An individual with access to both databases may be able to link together information from the two databases and distinguish individuals. If the secondary information source is present on the same system or a closely-related system, then the data may be considered linked.

Data elements which might be considered personally identifiable include, but are not limited to:[3]

- A person's name, such as their full name, maiden name, mother's maiden name, or alias;
- A personal identification number, such as SSN, passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street or email address;
- Electronic identification numbers, such as Internet Protocol (IP) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;[4]
- Telephone numbers, including mobile, business, and personal numbers;
- Information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information;

---

[2] Erika McCallister *et al., Guide to Protecting the Confidentiality of Personally Identifiable Information (Draft)*, Special Publication No. 800-122, 2-1 (U.S. Dept of Commerce, National Institute of Standards and Technology, Jan. 2009) (adopting the definition of PII contained in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*).

[3] *See Id.* at 2-2.

[4] *But see In re Charter Commc'ns*, 393 F.3d 771, 774 (8th Cir. 2005) (holding an IP address does not identify a user's name or mailing address); *Klimas v. Comcast Cable Comm'cns, Inc.*, 465 F.3d 271, 276 n.2 (6th Cir. 2006) (noting "that IP addresses do not in and of themselves reveal 'a subscriber's name, address, [or] social security number.' That information can only be gleaned if a list of subscribers is matched up with a list of their individual IP addresses."); *Johnson et al. v. Microsoft*, C06-0900RAJ Or. Granting Def.'s Mot. S.J. 7 (W.D. Wash. June 23, 2009) (ruling that "In order for 'personally identifiable information' to be personally identifiable, it must identify a person. But an IP address identifies a computer, and can do that only after matching the IP address to a list of a particular Internet service provider's subscribers.").

- Personal characteristics, including handwriting, photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry); and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, or employment, medical, education, or financial information).

2. NON-PERSONALLY IDENTIFYING NATURE OF LPR DATA

(a.) License plates can be associated with individuals' PII

Although license plates don't directly include personally identifiable information, they are frequently associated, by means of computer inquiries, with the identity of an individual person. Thus, a license plate number, just as a name and date of birth, can serve as the gateway to personally identifiable information. Moreover, a license plate number is also a gateway to more traditional types of data relied upon by criminal justice practitioners. Although some intended uses of LPR data focus on the automobile itself (e.g., identifying stolen vehicles), other potential uses of LPR data involve the process of locating the individual(s) somehow connected to a particular license plate.

(b.) LPR data collection and privacy

The mere collection of information regarding individuals implicates privacy concerns. Fewer concerns are raised by the collection of information about individuals premised upon some reasonable suspicion that they are acting unlawfully. Greater concerns regarding the public's privacy interests are raised when the government collects information about individuals for investigatory purposes absent any suspicion of criminal wrongdoing.

Nevertheless, it is a strong argument that a person has a diminished expectation of privacy in public spaces. In the criminal justice context, the common good of public safety has been considered of greater importance than an individual's right to remain anonymous when passing through public spaces.[5]

Furthermore, in the context of license plate readers, the vast majority of states consider the operation of an automobile a privilege and not a right. Every state's laws require

[5] On at least two occasions the U. S. Supreme Court has been confronted with whether an individual can be required to identify himself to the police during a Terry stop, but decided those cases on other grounds. *See Brown v. Texas*, 433 U.S. 47 (1979) (holding the underlying seizure illegal thereby avoiding the constitutional question) and *Kolender v. Lawson*, 461 U.S. 352 (1983) (holding a statute requiring a suspect to identify himself to police officers during a Terry stop void for vagueness and refusing to decide the issues of the constitutionality of compulsory identification). It wasn't until 2004 in *Hiibel v Sixth Judicial District Court of Nevada*, 542 U.S. 177, that the Court concluded that requiring suspects to identify themselves did not violate the Fourth or Fifth Amendments.

the display of license plates when the vehicle is operated or parked on a public road and license plates are even required to be illuminated at night.

(c.) LPR data is not, itself, personally identifying

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.

The Driver's Privacy Protection Act ("DPPA"), 18 U.S.C.A. §§ 2721-25, also supports the premise that a license plate number alone is not PII. Enacted in 1994, the DPPA is a federal law that regulates how state motor vehicle departments release information contained in their records. The DPPA prohibits, with specific exceptions, state motor vehicle departments from disclosing personally identifying information connected to a motor vehicle record (e.g., a license plate number).[6]

While the DPPA requires states to disclose personal information for certain limited purposes, it permits the disclosure of personally identifiable information connected to a license plate for fourteen enumerated purposes. Three of those purposes relate to law enforcement use of the information and are relevant to the operation of a LPR system. Specifically, personally identifying information connected to a motor vehicle registration may be disclosed for use: (1) "by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions;"[7] (2) "in connection with matters of motor vehicle or driver safety and theft;"[8] and (3) "in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency."[9] The DPPA also regulates how an authorized recipient of motor vehicle records can share information with another subsequent user.

Thus, federal law acknowledges: (1) although license plate numbers are not, by themselves, personally identifying information, they can be linked to individuals and, (2)

[6] The Act defines "personal information" as an "individual's photograph, social security number, driver identification number, name, address...telephone number, and medical or disability information"; the term does not include information on vehicular accidents, driving violations, and driver's status. 18 U.S.C. § 2725(3). In 2000, the Act was amended to create a new class of "highly restricted personal information." This includes an "individual's photograph or image, social security number, and medical or disability information" collected or maintained by a DMV. 18 U.S.C. § 2725(4).

[7] 18 U.S.C. § 2721(b)(1).

[8] 18 U.S.C. § 2721(b)(2).

[9] 18 U.S.C. § 2721(b)(4).

the release of PII associated with a particular license plate number should be limited to official purposes.

Certain contextual photos may contain digital images of the vehicle's driver and/or passengers. As discussed above, the contextual photo is collected and maintained as a mechanism to ensure that the LPR software is accurately reading license plate numbers. Moreover, not every contextual photo contains an image of a vehicle's occupants.

A photograph of an individual's face certainly identifies that individual. Nevertheless, LPR systems currently being utilized by law enforcement agencies are not designed to capture images of occupants of vehicles. In the infrequent instances where images of a vehicle's occupants are captured by the LPR camera, LPR contextual photos may be used to confirm whether an individual already associated with a particular license plate was the person in the car when it passed the LPR camera.

This distinction between identification and confirmation is significant when determining whether to consider LPR data personally identifiable. Furthermore, the confirmation of the identity of the individuals occupying a vehicle only takes place as part of a subsequent investigation into an event surrounding the observation of the vehicle's license plate. Thus, even though some contextual photographs include an image of a vehicle's occupants, this Report considers LPR data as non-personally identifying information.

(d.) LPR data is for official use only

Even where an organization determines that a particular type of information is not personally identifying, the organization should still consider whether the information is sensitive or has organizational or individual risks associated with it, and determine the appropriate protections.

There may be risks surrounding the release of the dates, times, and locations of a certain license plate number where the requestor is in possession of the identity of that vehicle's owner. It is these risks, described in more detail later in this Report, that support the International Association of Chiefs of Police's recommendation that LPR Data be considered For Official Use Only (FOUO).[10]

[10] The term For Official Use Only is used within the U.S. Department of Homeland Security to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. LPR data may also fall into the federal information categorization of non-classified information being implemented pursuant to Executive Order 12958; under that system of categorization, LPR data may also be considered Controlled Unclassified Information (CUI) and may more specifically fall under the CUI category "Controlled, Special Dissemination." *See* Executive Order 12958 as amended by Executive Order 13292 at 68 Fed. Reg. 15315 (2004); *see also* White House *Memorandum for the Heads of Executive Departments and Agencies*: Designation and Sharing of Controlled Unclassified Information (CUI) (May 7, 2008) available on-line at: http://www.archives.gov/cui/documents/designation_cui.pdf.

2

Part 2. Types of privacy risks surrounding the use of LPRs

This Part summarizes the privacy risks created by the enhanced collection, recording, analysis, and retention of license plate numbers by means of LPR systems. The privacy concerns described below become the themes that run throughout the entire PIA Report; the discussions that follow briefly explain how these risks can be mitigated by policies intended to regulate the use of LPR systems from the initial collection of the data through its life cycle.

A. UNDERLYING PRIVACY CONCERNS

The enhanced sharing, even among law enforcement personnel, of substantial amounts of information about people not immediately suspected of criminal activity may lead the public to believe that its privacy interests are being ignored. Moreover, improper disclosures of potentially sensitive information not only damage the relationship between citizens and their governmental institutions, such disclosures also make people more vulnerable to physical, emotional, financial, and reputational harms.

System designers and justice practitioners sometimes overlook information processing risks that arise from the storage, analysis, and use of data that has already been collected by the justice system. One such risk implicated by the aggregation of data occurs where the compiled information used to judge an individual is incomplete or is distorted because it is being considered out of its original context. Another privacy concern involves the risk that a justice practitioner using an information system may target one individual because of acts committed by another due to a variety of data inaccuracies.

It has been law enforcement's position that the impact of LPR systems on the privacy of individuals is the same as the impact of any ordinary investigation. The premise of this position is that LPR systems simply automate the same exact process that has been available to police manually. Criminal justice agencies explain that LPR systems simply improve the accessibility of information that is already publicly visible and make it available for analysis and appropriate dissemination.

These positions are woven throughout the discussions and recommendations contained in this Report. Ultimately, the goal of this Report is to inform a law enforcement agency's efforts to develop an information management policy that attempts to ensure

the rights of individuals to be treated with fairness and respect while providing law enforcement with the LPR data it needs to protect the public safety in an efficient and productive manner.

B. POTENTIAL CHILLING EFFECTS OF LPR SYSTEMS

Individuals are already compelled to disclose a great deal of information to their government. One privacy issue associated with the enhanced collection and compilation of LPR data from multiple sources is a chilling effect on social and political activities. Specifically, the risk is that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance.

Surveillance is the watching, listening to, or recording of an individual's activities.[11] The potential privacy harm of surveillance is its potential use as a tool of social control: the mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition.[12]

The degree of any system's chilling effect depends a great deal upon the types of information it collects and how the data will subsequently be utilized. LPR systems, unlike other forms of public surveillance, have the potential to reveal to the government individuals' driving habits. As LPR systems become more widespread, and as law enforcement agencies improve their information sharing capabilities, the potential to monitor where and when a particular vehicle travels is enhanced.

Recording driving habits could implicate First Amendment concerns.[13] Specifically, LPR systems have the ability to record vehicles' attendance at locations or events that, although lawful and public, may be considered private. For example, mobile LPR units could read and collect the license plate numbers of vehicles parked at addiction counseling meetings, doctors' offices, or even the staging areas for political protests. Furthermore, fixed LPR units located at traffic choke points may identify travel patterns of particular vehicles as they commute to and from their homes.

Although there may be some chilling effects surrounding the utilization of a LPR system, the development and implementation of policies regulating the collection, uses, sharing, and retention of LPR data can operate to reduce these effects. Deployment of LPR cameras based upon crime analysis that takes into account crime patterns and the types

[11] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490 (Jan. 2006).
[12] *Id.* at 493.
[13] One resident of a municipality considering the installation of LPRs who "[didn't] see too much harm in [LPRs]" admitted that a LPR system "still has the taint of Big Brother." Demian Bulwa, *Tiburon may install license plate cameras*, A-1 San Francisco Chronicle (July 10, 2009) http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/07/10/MNT6189U0U.DTL.

of crime targeted by LPR systems can also reduce the perception that LPRs are simply a tool for public surveillance.[14] Developing retention periods are another way to address the potential chilling effects of LPR systems.

C. IDENTIFICATION OF INDIVIDUALS VIA LICENSE PLATE NUMBERS

Identification is the act of connecting data to particular individuals.[15] Identification enables surveillance by facilitating the monitoring of persons.[16] The potential harm of identification is that it increases the government's power to control individuals through the chilling effects discussed above. It can further inhibit one's ability to be anonymous, which is important in so far as it protects people from bias based on their identities and enables people to vote, speak, and associate more freely by protecting them from the danger of reprisal.[17]

Few rights guaranteed by the First Amendment can be enjoyed without moving about. The rights to "enter into certain intimate human relationships" and "to associate for the purpose of engaging in those activities protected by the First Amendment – speech, assembly, petition for the redress of grievances"[18] are predicated upon freedom of movement. In order to associate with others in political activities or pursue religious beliefs, one must be able to go to the place where their associations meet. To assemble and participate in a rally on behalf of a political candidate, or alternatively to demonstrate against a government policy, traveling is a prerequisite.

The benefits of anonymity in the exercise of First Amendment rights have been recognized by the U.S. Supreme Court. In one case, referencing the "important role in the progress of mankind" that anonymous literature has played, the Court upheld the right to not identify one's self in the exercise of the free press on the grounds that it "provides a way for a writer who may be personally unpopular to ensure that readers will not prejudice her message simply because they do not like its proponent."[19] The right to not identify one's self has also been upheld in other First Amendment contexts. "It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute...restraint on freedom of association."[20]

---

[14] As discussed in Part 4, LPR cameras can be fixed or mobile and can be deployed in an overt or covert manner.
[15] Solove, *supra* note 11 at 511.
[16] *Id.* at 514.
[17] *Id.* at 515.
[18] *Roberts v. United States Jaycees*, 468 U.S. 609, 617-618 (1984).
[19] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-343 (1995) (citing *Talley v. California*, 362 U.S. 60, 62 (1960) (internal quotations and footnotes omitted)).
[20] *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958). *See also Brown v. Socialist Workers' 74 Campaign Comm.*, 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations").

LPR systems have the potential to record the license plate numbers of vehicles that embark on travels related to the occupants' exercise of their First Amendment rights. Law enforcement agencies are not implementing LPR systems with the goal of collecting this type of information; rather, LPR camera's potential to impact First Amendment freedoms is a byproduct of the day-to-day operation of the system. Such chilling effects can be reduced by enforcing policies designed to limit access to LPR data for certain, express law enforcement or investigatory purposes. Moreover, the development of policies concerning the collection of license plate numbers by mobile LPR units should include provisions concerning the appropriate use of mobile LPR cameras in areas known to reflect an individual's political, religious or social views, associations, or activities (e.g., churches, abortion clinics, etc.) and limit such collection to instances directly related to criminal conduct or activity.

D. SECONDARY USE OF LPR DATA

Secondary use is the utilization of data for purposes unrelated to the reasons for which the data was initially collected.[21] Secondary use essentially creates the potential for dignitary harm in that it thwarts people's reasonable expectations about how data collected and maintained by LPR systems will ultimately be used.[22] The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability among those whose information is collected.[23] Secondary use of information also creates interpretation problems in its analysis; specifically, data may be misunderstood when it is removed from its original context.[24]

Law enforcement agencies' primary concern with regard to their operation of LPR systems is the investigation of crimes and ensuring the public's safety. Privacy concerns regarding secondary uses of LPR data can be addressed in part by: (1) clearly articulating the agency's original purposes for collecting license plate numbers; (2) anticipating and disclosing how LPR data will likely be used; and (3) limiting subsequent uses of LPR data to those original purposes.[25]

Agencies could also address secondary uses of LPR data by clearly articulating permissible secondary uses of the information in advance of the data's collection. Any secondary analyses or uses of LPR data should take into account its limitations in terms of identifying anything other than the vehicle.

---

[21] Solove, *supra* note 1111 at 521.
[22] *Id.*
[23] *Id.* at 522.
[24] *Id.*
[25] The DPPA implements these three suggestions and specifically makes it "unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted [by the Act]." 18 U.S.C. § 2722(a); *see also* text accompanying *supra* notes 6-9.

E. AGGREGATION OF LPR DATA

Aggregation is the gathering together of various pieces of information about a person.[26] Although less direct than surveillance, aggregating data from multiple sources is another way to acquire information about an individual.[27] The U.S. Supreme Court has even ruled that there is a significant difference between information that, although public, might be difficult to obtain from multiple locations, and a computerized summary located in a single clearinghouse of information.[28]

The potential privacy harms surrounding aggregation are similar to those of Secondary Use, described in Subpart D above. A piece of information here or there about an individual is not very telling; but when combined, these bits and pieces of data begin to form a portrait of a person.[29] In other words, personally identifiable information brought together from various source systems has the potential to reveal an individual's beliefs or ideas concerning public or social policy, as well as political, educational, cultural, economic, philosophical, or religious matters.

Aggregation can cause dignitary harms because of its ability to unsettle an individual's expectations regarding how much information they actually reveal to others.[30] Aggregation can also create interpretation problems where the data compilation used to judge the individual is incomplete or results in a distorted portrait of the person because the information is disconnected from the original context in which it was gathered.[31]

LPR Systems use optical character recognition to translate the alpha-numerical text of a license plate into electronic data. The license plate number, combined with the date, time, and location of observation is then stored electronically and can readily be combined with other data sources. An authorized user can use LPR data to gather the name and contact information of a vehicle's registered owner from a department of motor vehicles data system. Care should be exercised when combining LPR data with other personally identifying data; this is because the LPR data relates only to the vehicle, not necessarily the registered owner.[32] Thus, to address concerns related to the aggregation of data, law enforcement agencies should keep in mind that LPR data relates only to vehicles and it may be misleading to combine LPR data of vehicles with other data linked to the personally identifying information of registered owners or other occupants.

---

[26] Solove, *supra* note 11 at 507.
[27] *Id.* at 508.
[28] *See U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 764 (1989).
[29] *Id.* at 507.
[30] *Id.* at 508.
[31] *Id.* at 508-511.
[32] Moreover, there are no assurances that an inquiry into the license plate number will lead to the registered car, as in the case of stole license plates.

F. POTENTIAL MISUSES OF LPR DATA

Several prominent privacy groups view information concerning individuals' locations as inherently prone to abuses, including expanding data uses beyond the original purposes of collection, sharing data with third parties beyond reasonable expectations, and heightening individuals' vulnerability to crime.

Misuses of LPR data can take several forms. A common misuse of any data system involves the improper disclosure of its information by authorized users. When data is improperly disclosed by those authorized to access it, the promise the agency made to keep the information confidential is broken. The harm caused by such breaches is not simply that the information has been disclosed, but that the promise made to the subject of the data has been broken.[33] Protections against breaching the confidentiality of the data help promote certain relationships that depend upon trust, such as the relationship between citizens and their government.[34]

Privacy concerns also surround the disclosure of certain true information about a person that, when revealed, impacts the way others judge her character; the potential harm of disclosure involves the damage to an individual's reputation caused by the dissemination.[35] Disclosure can also be a form of social control and carries with it the potential chilling effects associated with surveillance described above in Subpart B. Moreover, knowledge of a person's location could, for example, heighten that person's vulnerability to property theft or physical harm. Disclosure harms occur regardless of whether the dissemination is the result of an inappropriate release of data by an authorized user or is the result of an unauthorized person obtaining access to the data (e.g., by hacking into the system) and releasing the information.

Simply because a type of information may be subject to misuse is not necessarily determinative as to whether to collect and use it; there are several things law enforcement agencies can do to prevent misuse of LPR data. Specifically, law enforcement agencies can develop policies that set forth the appropriate access and dissemination of LPR data; agencies can also prohibit and punish individuals authorized to access LPR data but who inappropriately disclose the information. Furthermore, conducting audits and monitoring system operations can prevent and identify instances of misuse. Security safeguards are common in other law enforcement data systems and can be useful in limiting unauthorized access to LPR data.

[33] *Id* at 527.
[34] *Id.*
[35] *Id.* at 531.

3

Part 3. Scope of the PIA Report

Part 3 explains the approach this Report takes to analyze the privacy concerns surrounding a law enforcement agency's use of a LPR system. It explains the steps taken to prepare this document and decisions related to narrowing the scope of this Privacy Impact Assessment.

A. APPROACH OF THE ASSESSMENT

In 2007, the International Association of Chiefs of Police ("IACP") passed a resolution in support of License Plate Reader (LPR) technology.[36] That resolution strongly encouraged the U.S. Congress to fully fund license plate reader and related digital photographing systems, including interrelated information sharing networks, for the northern and southern borders of the United States. In support of this resolution, the IACP LEIM Section set out to develop this Privacy Impact Assessment ("PIA") Report.

The goal of the PIA Report was to identify and address the primary privacy issues implicated by the electronic collection, analysis, dissemination and storage of license plate information by law enforcement agencies across the country. The first step taken in the development of this Report was the preparation of a comprehensive listing of privacy issues raised by the use of LPR systems. This document, entitled *Issue identification: Privacy issues concerning the utilization of automated license plate readers* ("the Issues document"), is included in this Report as Appendix 2. The Issues document reflects the LEIM Section's efforts to document in a comprehensive manner the privacy concerns that should be addressed by any law enforcement agency utilizing or seeking to implement a LPR system.

B. UNDERLYING PREMISES OF THIS REPORT

(1) Focus on law enforcement uses – The privacy impact analysis and discussions contained in this Report focus on law enforcement agencies' utilization of LPR systems and the LPR data they collect to investigate crimes and enforce the criminal laws. If LPR data will be used for additional purposes, additional analysis will be necessary.

[36] Intl. Assn. of Chiefs of Police, *2007 Resolutions*, 51-52 (Oct. 16, 2007) available on-line at: http://www.iacp.org/resolution/2007Resolutions.pdf.

(2) **Absence of regulation of LPR data** – There is an absence of uniform regulation concerning the appropriate collection, use, analysis, and retention of LPR data. This Report is intended to help law enforcement agencies develop policies meant to fill this gap in regulation in such a manner that ensures public safety needs are met while protecting individuals' privacy interests.

(3) **Adult status is presumed** – Part 1 explained that LPR Data is not considered personally identifying information for purposes of this Report. Nevertheless, contextual images that include vehicle occupants may contain images of minors; this is because states routinely issue drivers' licenses to individuals under the age of majority and because minors are frequently passengers in cars. Thus, LPR systems may potentially contain the location information of minors whose personally identifying information is associated with a certain vehicle. The discussions contained in this Report do not distinguish between LPR data attributed to adults or minors.

(4) **Existing information sharing practices remain in effect** – The discussions contained in this Report are not intended to supersede existing data sharing practices concerning license plate data. Rather, this Report is focused on the access, use, and dissemination of license plate data collected by LPR cameras and stored in LPR systems.

(5) **LPR data is not considered criminal intelligence information**[37] – The data collected by LPR cameras and upon which OCR is performed is only fact-based information; it is not intelligence data. Nevertheless, once that fact-based LPR data is analyzed, it may become intelligence data in the future and be subject to the U.S. Department of Justice's regulations contained at 28 C.F.R. Part 23.

(6) **Internal access to LPR data is determined at the agency level** – The terms "law enforcement officials" and "law enforcement officers" are used interchangeably throughout this Report. It is up to local agency heads to determine who within the organization may access LPR data.

C. ISSUES NOT ADDRESSED IN THIS REPORT

There are numerous privacy and other public accountability issues surrounding a law enforcement agency's utilization of a LPR system. Some of these issues surround the administration of the system and others concern the utilization of LPR data compiled by

[37] Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria. 28 C.F.R. §23.3(b)(3).

other agencies. The scope of this Report was narrowed to exclude consideration and discussion of the following issues.

(1) **An agency's decision to utilize a LPR system** – This Report focuses on the privacy concerns surrounding the operation and administration of a LPR System; it does not, however, discuss a law enforcement agency's initial decision to procure and begin utilizing LPR cameras.

(2) **Privacy policy development** – Although it is beneficial to utilize a formal development process when creating policies regarding LPR data, this Report does not recommend to law enforcement agencies any particular method of creating privacy or information management policies that implement the recommendations that follow.

(3) **Use of another entity's LPR data** – This Report contemplates the privacy concerns surrounding a law enforcement agency's collection of LPR data through the use of its own LPR cameras and computer systems. Where LPR data collected by another entity is going to be used by a law enforcement agency, it should determine that the LPR data is reliable and of sound quality.

(4) **Sharing LPR data with private companies** – Although Part 5 discusses the dissemination of LPR data with various members of the general public, it does not address the sharing of LPR data outside the context of an investigation or public safety purpose. Law enforcement agencies seeking to share LPR data with private companies should fully examine the privacy and public confidence issues of doing so.

(5) **Freedom of information and sunshine acts** – Since freedom of information acts vary from state to state, this Report does not address the release of LPR data to the public pursuant to such a statute. Nevertheless, such laws are important and their impact on the operation and administration of a LPR system should be reviewed as part of any policy development process.

4

Part 4. Collection of LPR data

This Part explains that LPR system data consists of: (A) the images and data collected by LPR cameras; and (B) the Hot Lists that alert a user to the presence of a particular license plate. The discussions that follow concern how LPR data is collected and for what purposes.

A. LPR CAMERA DATA

1. LPR CAMERA DEPLOYMENT

LPR systems can observe and record over 1,000 license plates an hour in various lighting and weather conditions. LPR cameras can be fixed, mobile, or portable. A fixed LPR unit is permanently mounted, usually to a bridge or a pole, and frequently in a jurisdiction's most heavily traveled points of ingress and egress. Mobile LPR units are mounted to law enforcement agency vehicles and can capture data from any area of an agency's jurisdiction. Portable LPR cameras can be moved from vehicle to vehicle or deployed in covert configurations.

Some privacy issues will vary depending upon the type of camera deployment utilized. For instance, mobile LPR cameras are much less likely than fixed LPR units to collect information concerning the routine commuting of particular vehicles. This is because mobile LPR units are attached to cars and are therefore unlikely to observe license plate numbers in the same location at the same time on a consistent basis. Mobile units, however, do have the potential to patrol parking lots of certain establishments; thus, mobile LPR cameras may collect the license plate numbers of vehicles parked at locations that, even though public, might be considered sensitive, such as doctor's offices, clinics, churches, and addiction counseling meetings, among others.

2. LPR DATA ELEMENTS

As discussed in Part 1 above, LPR systems take images of vehicles and license plates within range of a LPR camera. Thus, depending upon the placement and resolution of its cameras, a LPR system has the potential to gather a wide spectrum of data.

Typically, the contextual image collected by a LPR camera is maintained in the information system to provide a means of ensuring that the license plate number was

properly converted into an electronically readable format by the optical character recognition (OCR) software. The contextual photo provides a more inclusive view of the vehicle and its surroundings. Depending on the focal length of the camera and the distance of capture, the photo may provide a view of part or all of the vehicle, its surroundings, and possibly the occupants of a vehicle. This information may be helpful in *inter alia*: (a) identifying the vehicle by providing color or unique attributes such as damage or bumper stickers; (b) confirming the location of the LPR camera that took the photograph; or (c) confirming the identity of a vehicle's occupant.

Although a contextual photo contained in a LPR system may contain a great deal of raw information, only certain pieces of information contained in any LPR photograph will be subjected to OCR and rendered into an electronically readable format. Thus, images of vehicle occupants, vehicle make and model, and any distinguishing features of a vehicle contained in a contextual photo are not electronically readable or compiled by existing LPR systems.[38]

In addition to collecting the OCR of license plate numbers, LPR systems do ascribe date, time, and location information to an image. Some systems also attach to the image a camera identifier; in the case of mobile LPR units, the patrol car and officer identification number may also be collected.

3. PURPOSE SPECIFICATION

Law enforcement agencies are charged with protecting the public as well as investigating crimes and criminal conduct. LPR systems serve four specific public safety goals. Specifically, LPR data can be used: (a) in various forms of crime analysis; (b) to alert law enforcement officials that a license plate number on a hot list is nearby; (c) to monitor the movements of vehicles operated by individuals subject to geographical limitations on their travel; and (d) to identify instances of criminal conduct that might have previously gone undetected without the aid of the LPR system.

(a.) LPR data is collected to support various forms of crime analysis.

Law enforcement agencies utilize crime analysis to prevent and suppress crime, apprehend offenders, and recover stolen property.[39] Crime analysis is usually conducted on offenses with discernable patterns and trends that can be prevented or reduced through the implementation of directed action plans.[40] A review of existing crime analysis operations reveals that burglary, robbery, auto theft, larceny, fraud, sex crimes, aggravated assaults, and murder are the crimes most appropriate for crime analysis.[41]

[38] Technology is continually advancing. If LPR systems evolve to a level where they can read and compile data other than license plate numbers, the policy discussions contained in this Report will need to be supplemented.
[39] Steven Gottlieb, *et al.*, *Crime Analysis: From First Report to Final Arrest* 14-16 (Alpha 1994).
[40] *Id.*
[41] *Id.* at 133.

There are three types of crime analysis: (1) tactical; (2) strategic; and (3) administrative. Tactical analysis is the first priority of law enforcement agencies.[42] Specifically, tactical crime analysis (a) detects crime patterns and series by studying and linking common elements of crimes;[43] (b) predicts when and where future events will occur; and (c) provides information to officers regarding specific crime problems and is intended to result in the arrest of a suspect.[44]

Strategic crime analysis concentrates on long-term crime trends and can be used to project where police presence should be increased or decreased. Administrative analysis, unlike tactical and strategic crime analysis, interprets crime statistics categorized by economic, geographic, or social conditions and provides information for grant applications, feasibility studies, and city council reports.[45] Thus, administrative analysis provides information useful in running a law enforcement agency while tactical and strategic crime analysis is intended to help the law enforcement agencies protect the public and enforce the criminal laws.

When law enforcement agencies talk about using LPR data to check crime series information to determine if the same vehicles are in the area of different crime scenes, they are referring to tactical crime analysis. Tactical crime analysis is used to determine who is doing what to whom and focuses on crimes against persons and property. LPR data can also be useful to other agencies whose missions are broader in scope, like counter terrorism taskforces interested in utilizing strategic crime analyses. The following categories of data are widely considered most useful for crime analysis purposes.[46]

- Geographic factors[47]
- Victim descriptors
- Physical evidence descriptors
- Suspect descriptors
- Time factors
- Property loss descriptors
- Specific modus operandi factors
- Suspect vehicle descriptors

[42] *Id.* at 15.

[43] A crime pattern is merely a set of similar offences happening in a specific geographical area while a crime series is a crime pattern that appears to be done by either the same person or group of persons. Shawn A. Hutton & Mark Myrent, *Incident-Based Crime Analysis Manual* 34 (Ill. Crim. J. Info. Auth. 1999).

[44] Shawn A. Hutton & Mark Myrent, *Incident-Based Crime Analysis Manual* 7 (Ill. Crim. J. Info. Auth. 1999).

[45] Gottlieb, *supra* note 39 at 15 (stating that administrative analysis essentially includes the "nice to know stuff.").

[46] *Id.* at 128. Experienced analysts have found that the importance of each factor differs depending upon the type of crime being investigated. For example, suspect vehicle descriptors are more useful in determining whether a pattern of thefts from vehicles exists than a pattern of strong armed robberies. See *Id.* at 318-320.

[47] Spot maps can be of great assistance to the analyst. Nevertheless, spot maps will only depict crime patterns; additional information is necessary to determine if a crime pattern is also a crime series.

(b.) LPR systems collect information to alert law enforcement of the proximity of a vehicle displaying a license plate number that is included on a hot list.

License plate numbers of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts are routinely added to "hot lists" circulated among law enforcement agencies. These lists serve an officer safety function as well as an investigatory purpose.

Hot lists are typically transferred daily and can be updated by an operator/officer in the field. Hot list information can come from a variety of sources, including but not limited to, stolen vehicle information from the National Insurance Crime Bureau and 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 to the LPR system.

LPR systems function in such a way as to notify an officer when a license plate on the hot list is observed in real time; this can be the case for both fixed and mobile LPR units. Historical LPR data can also be searched to determine the date and time a license plate number contained on a hot list passed a certain camera.

(c.) LPR data is collected to assist in the monitoring of certain identified individuals' compliance with travel restrictions.

In some circumstances, a court can limit the movements of certain individuals for public safety purposes. For instance, sex offenders, probationers and parolees, and people subject to orders of protection may be subject to court-imposed restrictions on their geographic movements. LPR systems can be useful in assisting with the enforcement of geographic limitations on the movements of these types of individuals. Specifically, LPR cameras can record the license plate numbers of vehicles observed near certain locations such as schools and day care facilities, or residences and work addresses of people protected by court orders. These locations and license plate numbers associated with such individuals can be added to LPR systems to bring any potential violations to an officer's attention in real-time or the plate numbers can be queried against historical LPR data. In these instances, the LPR data is merely evidence of a possible violation and further verification is needed to identify the operator of a vehicle.

In instances of mass evacuations, LPR systems could be useful in determining the number of vehicles that have left an area and can also serve as a means of identifying those vehicles. This latter capability may be beneficial to law enforcement agencies' ability to respond to calls asking about the welfare or evacuation status of a relative.

(d.)LPR data is collected to help law enforcement agencies identify previously-undetected crimes

LPR systems have the potential to identify and observe criminal conduct that, prior to the implementation of the technology, would have been extremely difficult to detect in the absence of an offender's chance encounter with authorities.

For example, the failure to obtain and provide proof of mandatory car insurance is grounds for several states to suspend license plates and driver's licenses. Unless these vehicles are operated in such a manner as to raise the suspicions of a police officer, these uninsured vehicles would remain undetected. In a jurisdiction utilizing a LPR system, a department of motor vehicles can create a list of license plate numbers attached to invalid driver's license numbers. That list can be uploaded into a LPR system and officers can be notified when that license plate number passes a LPR camera.

LPR systems can also be used to help implement programs intended to more efficiently bring certain crimes to law enforcement officers' attention. Several states have programs to combat auto thefts that permit vehicle owners to provide written consent for their vehicles to be stopped without cause during late evening hours. LPR systems provide an efficient means of implementing such programs and increase the odds of recovering stolen vehicles because these systems can cross check license plate numbers against lists of stolen plates and vehicles many times faster than if done manually.

LPR systems, like other forms of surveillance cameras, are excellent tools for figuring out what has already happened. Moreover, overt LPR systems may have some deterrent impact.[48]

B. LPR "HOT LISTS"

Many of the potential uses of LPR data involve the comparison of license plate numbers collected by a LPR system to numbers contained on a previously compiled list. These hot lists may be compiled by the local law enforcement agency utilizing the LPR system or by other state or federal government agencies. The purpose of these lists is to signal a law enforcement official that a vehicle displaying a license plate number that is included on a hot list is near a LPR camera. This can be done in real-time or through the use of historical LPR data.

The use of hot lists is essential to LPR systems intended to serve public safety purposes, and the actions taken by law enforcement officers informed of a "hit" will vary depending upon the list that contains the vehicle's license plate number. Limiting the number of hot lists uploaded to a LPR system is recommended to guard against the

[48] *See* Jerry Ratcliffe, *Video Surveillance of Public Places*, 8-11 (U.S. Dept of Justice, Office of Community Oriented Policing Services Feb. 2006) (referring to closed-circuit television surveillance of public spaces).

system "crying wolf." If law enforcement officers are bombarded by an alert at every third license plate that passes the LPR camera due to the inclusion of too many hot lists, a danger exists that officers may turn off the system or otherwise ignore alerts during their shifts. Only including hot lists that further the law enforcement agency's goals is one way to guard against this danger. Local agencies are ultimately responsible for selecting which hot lists to upload onto their LPR systems.

1. COMPILATION & MANAGEMENT OF LPR HOT LISTS

Managing hot lists is a key element to the success of a LPR system. The content of hot lists should be monitored to protect people whose vehicles license plates numbers are contained on such lists from continued and unnecessary annoyance.

While some hot lists focus on identifying a particular vehicle regardless of who is operating it (e.g., stolen cars, AMBER alerts), other lists include license plate numbers known to be associated with specific individuals (e.g., sex offenders, wanted persons). These hot lists, whether they relate to stolen cars or potential occupants of vehicles, enhance law enforcement agencies' ability to detect crime and provide critical officer safety information.

LPR hot lists are compiled to serve agency-specific needs. Hot lists may include, for example, license plate numbers of vehicles known to be operated by: (a) violent probationers and parolees; (b) violent gang members; (c) individuals with outstanding warrants; and (d) individuals identified as witnesses. In some instances, individuals provide the license plate numbers of vehicles they may operate; in others, departments of motor vehicles may provide license plate numbers of vehicles registered to individuals. In still other circumstances, license plate numbers may be linked to certain individuals by direct observation and documentation of law enforcement officers.

When developing their own hot lists, law enforcement agencies should develop a process that sets forth criteria for including certain license plate numbers on a hot list. For instance, in order to activate an America's Missing: Broadcast Emergency Response (AMBER) Alert certain criteria must be met. Specifically, a juvenile: (a) must have been confirmed as abducted; (b) is under the age of 16 or has a proven mental or physical disability; and (c) is in danger of serious bodily injury; finally, there also needs to be enough descriptive information to believe that a broadcast alert will help.[49]

Additionally, agencies may consider providing a process whereby a license plate number's inclusion on a hot list can be verified. Providing for verification is one way of monitoring the accuracy of data contained on a hot list. It also helps ensure that law enforcement officials act only upon complete, correct, and timely information.

[49] U.S. Dept. of Justice, *Recommended AMBER Alert Criteria*, (LT000498, Apr. 2005) available on-line at: http://www.ncjrs.gov/html/ojjdp/amberalert/PocketCard.pdf.

Agencies should also develop procedures for removing license plate numbers that do not belong on a particular hot list.

C. NOTICE OF DATA COLLECTION PRACTICES

1. FAIR INFORMATION PRACTICES

In 1973, the U.S. Department of Health, Education, and Welfare ("HEW") published a groundbreaking report responding to concerns that harmful consequences may result from the storing of information related to individuals in computer systems. That report, entitled *"Records, Computers and the Rights of Citizens,"* articulated several principles HEW deemed essential to the fair collection, use, storage, and dissemination of personal information by electronic information systems.[50]

The five basic principles contained in the HEW Report held that: (1) there must be no personal data record keeping systems whose very existence is secret; (2) there must be a way for an individual to find out what information about him is in a record and how it is used; (3) there must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent; (4) there must be a way for an individual to correct or amend a record of identifiable information about him; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[51]

Several years later, in 1980, the Organization for Economic Cooperation and Development ("OECD") would publish its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* The OECD Guidelines articulated eight Fair Information Practices that incorporated the HEW Report's principles and are still today universally recognized as a solid foundation upon which to build privacy legislation and policies.[52]

The fair information practices provide rules governing the processing of data subjects' personal data. "Processing," "data subjects," and "personal data" are broadly defined

[50] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, Records, Computers and the Rights of Citizens: Report of The Secretary's Advisory Committee on Automated Personal Data Systems xx-xxi (1973) (hereafter "HEW Report"), available at http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[51] *Id.*

[52] NAT'L CRIM. JUST. ASS'N, Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems 22 (NCJA 2002) (hereafter "NCJA Guideline"), available at http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf

terms.[53] One of the fundamental principles is providing to data subjects notice of data collection and data management practices.

2. NOTIFYING THE PUBLIC ABOUT THE USE OF LPR SYSTEMS

The most fundamental Fair Information Practice is notice.[54] Without notice, an individual cannot make an informed decision as to whether and to what extent to disclose information to the data collector. Moreover, other fair information practices are only meaningful when a person has notice of an agency's data collection and management practices.

The decision to provide the public with notice of a law enforcement agency's use of a LPR system involves the consideration of several competing interests. First, there is a growing recognition that promoting public confidence in the administration of justice is one of the primary goals of good government. One way to promote public confidence is to increase the transparency surrounding how LPR data will be managed by the law enforcement agency, even if the LPR data itself should not be released to the public. Doing so serves two purposes: first, it invites constructive comments regarding the operation of the LPR system, and second, it is a mechanism to hold the justice system accountable for adhering to the rules and procedures it develops.

There may also be benefits to being proactive about informing the public of the use of a LPR system. Since the public is very likely to discover an agency's utilization of LPR technology, it could be best to be forthcoming with a positive news story. Moreover, such publicity could also result in some deterrence effect as prospective offenders would be made aware that their license plate numbers could be collected.

Nevertheless, there may be drawbacks to providing the public with notice that LPR cameras are in use in the jurisdiction. Not providing notice can help minimize offenders' implementation of countermeasures. Additionally, knowledge of the locations of fixed LPR units may give offenders information they need to avoid, sometimes with the assistance of GPS devices, passing a LPR camera. Providing the location of fixed LPR cameras could also result in increased costs due to intentionally inflicted damage.

After weighing the costs and benefits, some agencies may still be interested in providing notice. There are several ways to provide public notice of a LPR system. One way is to post a notice on the law enforcement agency's website. To be effective, website notice should be clear and understandable as well as conspicuous and posted in a prominent

[53] Barbara Crutchfield George, *et al., U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 752 (2001).

[54] This is sometimes referred to as the *Openness Principle*, under which there should be a general policy of openness about developments, practices, and policies with respect to personal data. Under this principle, means should be readily available of establishing the existence and nature of personal data, and the main purposes of its use, as well as the identity and usual residence of the data controller. *See* NCJA Guideline *supra* note 52 at 31.

location. Agencies may also consider publishing their privacy impact assessments or portions of their LPR system information management policies for a public comment period. Although more costly, signage can also be used to inform the public that a LPR system is being utilized in the jurisdiction.

If a law enforcement agency opts to provide notice, it is recommended that the agency limit the publication of details regarding the locations of fixed and mobile LPR units.

5

Part 5. Access to and Dissemination of LPR data

Part 5 addresses the closely related concepts of access and dissemination of the data collected by LPR cameras. This Report explains the distinction between historical and active LPR data and the privacy concerns surrounding each. The access to and dissemination of LPR Hot Lists are also discussed.

A. ACTIVE AND HISTORICAL LPR DATA

Active LPR data is that information which is provided to an officer in real-time. It takes the form of alerts that a license plate number contained on a hot list is near a LPR unit, whether fixed or mobile. The LPR data recorded during an officer's shift and accessible from within the squad car can also be considered active data as it has not been downloaded into a historic database of LPR data.

Historical LPR data is essentially a database containing the dates, times, and locations of individually identifiable motor vehicles; it is considered passive as it is essentially LPR data that is stored for future use. The amount of historical LPR data available for inquiries depends, in part, upon an agency's number of LPR cameras and its retention policies.

This Report distinguishes between active and historical LPR data as a method of addressing privacy concerns regarding the observation and recording of the date, time, and location of individuals' automobiles. It is submitted that the real-time utilization of LPRs implicates less privacy concerns than historical LPR data. Historical LPR data raises more concerns because of the potential to link a license plate number with an identifiable person.

B. ACCESS TO LPR DATA

Police officials have a duty to investigate crimes and criminal conduct. To fulfill this responsibility, police officials collect various types of information in order to identify potential suspects. Active LPR data helps bring a law enforcement officer's attention to certain violations as they occur, such as the operation of a stolen car or a vehicle displaying license plates associated with a violent felony or child abduction. Historical LPR data can play an important role in the investigation of crimes and can be utilized to

help create investigative leads and ultimately prosecute offenders. Historical LPR data is also utilized in traditional forms of crime analysis.

Appropriate access to active and historical LPR data is guided significantly by the purposes for which it collected. Thus, LPR data may appropriately be accessed by law enforcement officials: (a) to support crime analysis efforts; (b) to alert law enforcement officials that a license plate included on a hot list is or has been near a LPR camera location; and (c) to help law enforcement officials detect instances of criminal conduct.[55]

LPR data is most likely to be utilized by law enforcement officers; nevertheless, there may be additional, foreseeable users of LPR data. Each type of authorized user's access permissions should be clearly articulated.

Moreover, although it is axiomatic that active LPR data is available to any law enforcement officer, agencies might consider establishing more specific criteria for granting access to historical LPR data. Reducing the level of access law enforcement officials have to historical LPR data can protect against misuse of the information and provide additional privacy protections.

C. DISSEMINATION OF LPR DATA

It may be appropriate to share LPR data with various agencies and individuals throughout the justice system. Any policy regulating the sharing of LPR data should clearly identify the receiving entity and the specific purpose for the dissemination. Secondary uses, defined as uses other than the original purposes underlying the collection of the license plate numbers as discussed earlier in this Report, should be described in detail.

1. SHARING LPR DATA AMONG LAW ENFORCEMENT AGENCIES

Law enforcement officials have a duty to investigate crimes and criminal conduct. To fulfill this responsibility, officers collect, analyze, disseminate, and retain a variety of information, including active and historical LPR data. Many of the proposed purposes for collecting license plate data through the use of LPR systems implicitly require the sharing of LPR data across jurisdictions.

It has long been a basic tool of criminal investigators to start with known subjects and vehicles, and, with proper authorization, look for information about them and the people with whom they interact. Historical LPR data could provide police officials with information concerning the location of specific vehicles and, as a result, identify individuals for investigation because of their link to a vehicle observed by a LPR camera.

[55] *See* Part 4 of this Report; subsection (c) is intended to include law enforcement monitoring of certain identified individuals' compliance with travel restrictions and identification of previously-undetected crimes.

Although some of the connections revealed by an analysis of historical LPR data may be tenuous, it is the role and responsibility of law enforcement officials to exhaust investigative leads, something they routinely do in the course of any criminal investigation.

Combining LPR data from agencies in the same region can aid in the investigation of cold cases and in the identification of larger or more expansive crime trends.[56] Where one jurisdiction has already identified a vehicle of interest, it may be enough for a law enforcement agency of another jurisdiction to share the LPR data concerning that particular license plate number. Alternatively, conducting analyses of crime trends and series across jurisdictions may require submitting significant amounts of historical LPR data to another agency or regional data repository.

2. SHARING LPR DATA WITH OTHER GOVERNMENT ENTITIES

Several types of governmental agencies are likely to request LPR data from law enforcement entities. These agencies include, but are not limited to, parking enforcement bureaus,[57] departments of transportation, airport authorities, port authorities, and state departments of motor vehicles. While such requests may be for statistical information, other requests, like those from agencies like parole and departments of corrections officers,[58] might seek LPR data related to specific license plate numbers.

With the development of Fusion Centers, existing guidelines and memoranda of understanding regarding the inter-agency sharing of law enforcement data likely address the sharing of LPR data.

3. SHARING LPR DATA WITH THE PUBLIC

LPR data should only be shared for legitimate law enforcement purposes as it is considered for official use only. There may be instances where law enforcement purposes are furthered by sharing LPR data with the public. Whether LPR data may be shared with the public depends upon the type of entity receiving the LPR data, the nature of the information disseminated, and the circumstances surrounding the disclosure.

[56] Although not always the case, fixed LPRs frequently capture "transient vehicles" driving through a jurisdiction whereas mobile LPRs collect license plate data from local vehicles. Thus, fixed LPRs may further regional law enforcement goals whereas mobile LPRs may be of more value to local law enforcement agencies.

[57] Parking enforcement bureaus are not considered law enforcement in many jurisdictions.

[58] In many jurisdictions, parole and probation officers are peace officers with specific powers of arrest; in those instances, the sharing of information with such officers should be considered the sharing of LPR data among law enforcement agencies.

(a.) LPR data may be shared with private security personnel

Approximately 85 percent of the nation's critical infrastructure[59] is owned by the private sector and vulnerable to crime, such as terrorism and fraud.[60] Fusion Center Guidelines provide for the sharing of certain types of law enforcement data with privacy security personnel even where such access is not available to the public at large.[61] Thus, historical LPR data may be shared with private security personnel in accordance with memoranda of understanding and non-disclosure agreements entered into with the law enforcement agency.

(b.) LPR data may be shared with certain non-governmental organizations

Certain non-government organizations, such as the National Insurance Crime Bureau or the National Center for Missing and Exploited Children may seek access to LPR data. Certain statistical and license plate specific LPR data[62] may be shared with such entities to further the purposes underlying the collection of the license plate numbers by the LPR system. Law enforcement agencies should enter into memoranda of understanding or non-disclosure agreements with the non-government organization receiving the data.

(c.) LPR data may be shared with the general public in certain instances

Although there should be a general prohibition on the dissemination of LPR information to the general public, LPR data[63] could be useful in line-ups and in identifying vehicles involved in the commission of crimes or hit-and-run accidents. Such information may also be useful in seeking missing persons. In these and similar circumstances, law enforcement entities may want to affirmatively disseminate LPR information to the public.

In addition to case-by-case disseminations that take place during the course of an investigation, there may be instances where a vehicle or its known occupants pose a threat of substantial harm to the public. In these instances, the head of a law enforcement agency may release to the general public or news media LPR data that could reasonably protect the public from harm.

[59] Critical infrastructure is defined as those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. U.S. Dept. of Justice, *The National Criminal Intelligence Sharing Plan*, 13 (October 2003) (hereafter "NCISP") available on-line at http://www.it.ojp.gov/documents/NCISP_Plan.pdf.

[60] U.S. Dept. of Justice, *Fusion Center Guidelines—Developing and Sharing Information in a New Era*, 17 (August 2006) (hereafter "Fusion Center Guidelines") available on-line at http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

[61] *Id.* at 29.

[62] Although statistical summary information is unlikely to create privacy concerns, the sharing of LPR data related to a license plate number may raise privacy issues.

[63] LPR data may include images of vehicle occupants.

D. UPDATING AND SHARING HOT LISTS

Hot lists are typically uploaded onto a LPR system daily and can be updated by the authoring agency or an officer in the field. Hot list information can come from a variety of sources, including but not limited to, stolen vehicle information from the National Insurance Crime Bureau and 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 police departments can also interface their own hot lists to the LPR system. Hot lists can be uploaded onto a LPR system either as separate lists or merged into a single list.

Law enforcement officials have access to the license plate numbers contained on any LPR hot lists. Some hot lists will contain numerous license plate numbers and officials may not be able or desire to review their entire contents. Thus, for purposes of sharing hot lists across jurisdictions, it may be beneficial for law enforcement agencies that create hot lists to maintain supporting documentation regarding why a particular license plate number is on the specific hot list and make that information available, upon request, to the agency utilizing that hot list as part of its LPR system.

The heads of law enforcement agencies are ultimately responsible for determining which hot lists are uploaded onto the agency's LPR system and what actions officers take in response to a LPR hit. Agencies may want to establish some criteria for determining which hot lists will be uploaded onto the LPR system.

Since hot lists are created to enhance law enforcement officers' abilities to conduct investigations and provide for officer safety, the contents of hot lists should not be disseminated to the public.

E. SECURITY SAFEGUARDS

The focus of this Report is to set forth the impact LPR systems may have on the public's privacy interests; nevertheless, security safeguards may impact the degree to which the public's privacy may be impacted by a law enforcement agencies' operation of a LPR system. LPR data is sensitive enough to be categorized for official use only. As such, LPR systems should be protected by reasonable security safeguards to prevent loss or unauthorized access, destruction, use, modification or disclosure of LPR data. Ensuring that LPR data remains secure is one way for law enforcement agencies to build public confidence.

Law enforcement agencies may consider taking several steps to help secure LPR data. LPR systems and the computers that access them should utilize anti-virus software and firewalls. Additionally, authorized users should be required to utilize alphanumeric passwords consisting of a combination of upper and lower case letters, numbers and symbols; users should also be required to frequently change their passwords and keep

them safe. Law enforcement agencies should also utilize encryption technologies to protect LPR data in storage and in transit over networks.

6

Part 6. Retention of LPR data

Although retention periods were once necessitated by physical storage constraints, electronic storage of records has made the destruction of criminal justice and law enforcement information largely unnecessary. Thus, whether to retain a piece of information indefinitely is now a matter of policy. Part 6 addresses the retention of LPR data; it highlights several criteria a law enforcement agency may want to consider when developing a retention policy. This Part ultimately concludes that a comprehensive study of LPR data practices may be necessary to identify standards for retention periods.

A. RETENTION OF CRIMINAL JUSTICE DATA, GENERALLY

Criminal justice agencies are continuously collecting information about individuals. While some information is collected pursuant to an incident or an arrest, other information is gathered as a result of a tip and follow-up investigation. The information law enforcement agencies collect may be personally identifiable and other information may simply relate to the facts or circumstances of an event. This continuous collection, when combined with indefinite retention of that information, creates some privacy concerns.

The indefinite retention of law enforcement information makes a vast amount of data available for potential misuse or accidental disclosure. Additionally, retaining certain types of information indefinitely can be a form of undesirable social control that can prevent people from engaging in activities that further their own self-development, and inhibit individuals from associating with others, which is sometimes critical for the promotion of free expression. Although there are several reasons to retain certain types of law enforcement data for a substantial period of time,[64] those reasons may not apply to LPR data. Moreover, the indefinite retention of LPR data may enhance certain information dissemination risks.

[64] Official criminal history record information is collected and maintained to compile crime statistics, assist a court in imposing an appropriate sentence, and to help corrections officials make prisoner placement decisions. Criminal history records are also maintained to implement sentence enhancement provisions for recidivists and are also used to ensure that civil disability and offender registration statutes are properly applied. *See* U.S. Dept. of Justice, *Use and Management of Criminal History Record Information: A Comprehensive Report*, 101-127 (NCJ 187670, Dec. 2001) available on-line at http://www.ojp.usdoj.gov/bjs/abstract/umchri01.htm.

Nevertheless, justice practitioners and policy-makers are justifiably hesitant to destroy records. The government's reluctance may be rooted in investigators' experience that seemingly irrelevant or untimely information may acquire new significance as an investigation brings new details to light.[65] Deleting or destroying information, justice practitioners argue, would impede investigations and potentially result in fewer cases being solved.

Unfortunately, state and local records acts don't resolve the issue of data retention. The requirements contained in records retention laws vary from state to state.[66] Most statutes allow, but do not require, the destruction of particular criminal justice records after an established period of time. In many instances, governmental and law enforcement agencies must apply for permission to destroy records prior to doing so. Even though an agency may not be required to dispose of its electronic records, it may choose to remove LPR data from its information systems as a means to address the public's privacy concerns or simply to reduce the costs of storing the numerous back-up tapes necessary to ensure a computer system can recover from an unforeseen disaster.

B. CRITERIA TO CONSIDER WHEN ESTABLISHING RETENTION POLICIES

There is no formula for determining how long LPR data should be retained; nor have standards or guidelines been established that agencies can refer to as they set out to develop LPR data retention policies. In fact, there is surprisingly little literature discussing what criteria should be considered in developing retention periods for electronic criminal justice information in general or for LPR data in particular. Nevertheless, agencies may still need to explain their reasons for retaining LPR data for as long as they do.

1. STANDARD CRITERIA SHOULD BE ESTABLISHED TO ASSIST AGENCIES' DEVELOPMENT OF LPR DATA RETENTION POLICIES

A law enforcement agency seeking to develop a retention period for the data collected by and contained in its LPR systems faces many challenges. Chief among these challenges is the lack of thoroughly researched and well-articulated guidelines regarding how long LPR data should appropriately be retained.

LPR data is multi-faceted and subject to many potential uses. Historical LPR data may lose some of its value over time due to the sale and transfer of automobiles. The public's privacy interests regarding the stored LPR data may diminish as time passes. It's

[65] *See* 68 Fed. Reg. 14140 (2003).

[66] A threshold issue exists as to whether a contextual image taken by a LPR camera and the data associated with that image (including but not limited to the OCR text of the license plate and the date, time and location of observation) are considered records under the law of the jurisdiction.

uncertain if each query-response from a LPR system should be considered a record separate from the underlying LPR data that resides in the system.[67]

Although there are certain criteria that are intuitively useful when deciding how long to retain LPR data, it is unclear how those criteria relate to each other or which criteria would be considered more important in the case of a conflict. There may also be several criteria that are not intuitive but provide sound rationales for the retention or destruction of LPR data.

Thus, there is considerable need to establish a set of guidelines, including standard criteria, to assist law enforcement agencies in their development of retention policies for LPR data. Establishing such guidelines will likely require a thorough study of existing LPR data practices and rationales in use across the country and perhaps internationally. The IACP recommends that such a study be conducted and the results utilized to establish a set of standard criteria as well as guidelines for how those criteria may be used by law enforcement agencies in their development of a retention policy for LPR data.

2. INTERIM CRITERIA EXIST THAT AGENCIES MAY CONSIDER AS THEY DEVELOP RETENTION POLICIES

Regardless of whether a law enforcement agency deletes LPR data after 30 days or retains LPR data indefinitely, it may be called upon to explain how it came to that determination. Even though there is no set of standard criteria or guidelines for the appropriate retention of LPR data, there are still certain criteria specific to LPR data that a law enforcement agency may use to explain its decision to retain LPR data as long as it does.

Although not an exhaustive list, the criteria that follow are interrelated and can be applied comprehensively when setting a retention period for LPR data collected, used, and maintained by a law enforcement agency. Each criterion is described in greater detail below. It is important to note that these criteria are not beyond criticism. The application of the criteria is susceptible to multiple interpretations. Thus, two agencies can review the same facts about their respective sets of LPR data and come to different conclusions about how long the information should appropriately be retained. This is the result of the many judgments that must take place during the development of a retention policy and further counsels the need for uniform guidance in this area.

(a.) Statutes of limitation

Statutes of limitation exist to encourage prompt investigations and prevent stale prosecutions. Where LPR data is associated with crimes not subject to a statute of limitations, law enforcement agencies are justified in setting a long retention period.

[67] If so, those records may have different retention periods; specifically, the query-response record would likely be maintained for purposes of monitoring system use as opposed to supporting criminal investigations.

Conversely, where LPR data is associated with a crime that is subject to a shorter statute of limitation, law enforcement agencies may tend toward setting a shorter retention period.

It is important to note that certain characteristics of a criminal offense that might otherwise have a shorter statute of limitations may operate to extend or toll statutes of limitation.[68] Where those characteristics are present, the LPR data may be retained longer. Similarly, this criterion favors a longer retention period where the LPR data at issue concerns a crime that may be one of a series of acts performed at different times.[69]

Unfortunately, there are several difficulties with implementing statute of limitations criteria. Specifically, these criteria are premised upon the prompt reporting of crimes and that all steps of a crime take place in the same proximity to the location of the occurrence. Some crimes, especially those against property, may go undetected for some time; this may be the case where the property owner is away on vacation. Other crimes are the result of several steps made by one or a group of offenders that may not be readily detectible within days, weeks, or even months of an incident.

Furthermore, a large majority of LPR data will not be directly associated with a crime. Where this is the case, other criteria may need to be relied upon.

(b.) Potential future usefulness of the LPR data

Information collected by LPR systems may have usefulness beyond an individual investigation. Not only could information be part of a continuing series of acts as discussed in the statute of limitations criteria above, but information may be useful to generate leads for the investigation of subsequent crimes. Moreover, the retention period of LPR data may differ depending upon its foreseeable uses.

Law enforcement agencies may consider whether the characteristics of the LPR data (e.g., the geographic location or the date and time of the LPR camera observations) warrant keeping the information for a period longer than the statute of limitations alone advises.

The characteristics of the jurisdiction might also weigh in favor of retaining LPR data longer. For instance, jurisdictions containing likely targets for terrorism may justify retaining LPR data longer. Additionally, differences between LPR data collected by fixed and mobile LPR units may influence retention periods. LPR data collected by fixed units mounted near bridges and other critical infrastructure within a jurisdiction may have

[68] Characteristics of crimes that may extend or toll a statute of limitations vary from state to state. Generally, statutes of limitations are extended in cases involving *inter alia* certain thefts involving a breach of fiduciary duty, identity theft offenses, and certain sex offenses; statutes of limitations are typically tolled *inter alia* when the defendant is not residing in the prosecuting jurisdiction or when a material witness is on active military duty.

[69] Such crimes typically include conspiracy and thefts by deception that continue over a period of time.

greater long-term usefulness than mobile LPR data. Moreover, law enforcement agencies may also base their decision to maintain LPR data for a longer period of time on the premise that the information is useful in counterterrorism measures.[70]

Additionally, law enforcement agencies might also consider whether the LPR data is appropriate for the forms of crime analysis likely to be performed. Vehicle descriptions, including full and partial license plate numbers, are a type of information commonly utilized to analyze similarities of different crimes to connect them to a common offender. The more useful the LPR data is for crime analysis purposes, the more likely a law enforcement agency can justify a longer retention period for the information.

LPR data may also serve important officer safety needs. For example, it can be useful for officers to know that a vehicle was near a domestic violence call or was previously involved in a suspect's use of violence toward police officials. Where the LPR data is likely to improve officer safety, law enforcement agencies may establish a longer retention period for the information.

Some criteria, however, may reduce the potential future usefulness of information and counsel a shorter retention period for LPR data. Retaining vast amounts of data for long periods may undermine the usefulness of an information system over time. Depending upon its capabilities, the overall performance of an information system may decrease as the amount of data stored increases. Not only might it take longer for the system to search its vast repository of data, but the system might also return too much information for a user to sort through effectively.

Thus, processing, analysis, and user limitations of a LPR system caution against overly broad interpretations and expectations of the potential future usefulness of LPR data. These criteria also counsel a shorter retention period for LPR data that is not likely to generate a useful investigative lead, inform a crime analysis technique, or enhance officer safety.

Another consideration that might reduce the potential usefulness of information is lack of public support of the LPR system and its information practices. A law enforcement agency may wish to consider the public's reasonable expectations of how LPR data may be used in the future when developing a retention period for LPR data. In most instances, the public's expectations likely are parallel to the justice system's practices; this is true especially in regard to generating future leads, informing crime analyses, and helping to ensure officer safety. Upsetting reasonable expectations can subject an information system to intense public scrutiny and lead to formal resistance to not only a LPR program but future information systems as well. When taking the public's expectations into account, it is useful to consider the availability of a substitute source

[70] The 9/11 Commission Report found that it took between two and four years to plan and carry out the attacks against the World Trade Center.

of information that would meet the same need but not contain the same risks of alienating the public's trust and confidence in the justice system, such as electronically compiled traffic warnings and citations.

(c.) Relative sensitivity of the LPR data

Part 1 of this Report has already discussed the limits of LPR data to identify individuals and concluded that LPR data is not alone personally identifying. Part 2 cautioned against combining LPR data with other personally identifying data because the LPR data relates only to the vehicle's whereabouts and not necessarily the registered owner or occupant.

Nevertheless, LPR data may be considered sensitive for the purposes of setting a retention period because: (1) it can serve as a gateway to other, more personally identifying information; and (2) the locations from which the LPR data was collected may be considered potentially sensitive. Locations which may be considered sensitive may include, but are not limited to, churches, doctor's offices, clinics, and protest staging areas.

The public's perception that the law enforcement agency will protect the LPR data from improper disclosure is a significant criterion when establishing a retention period. The higher the public's confidence in the law enforcement agency, the more receptive the public may be to a longer retention period. Conversely, if public confidence in the agency's ability to maintain the confidentiality and security of the LPR data is low,[71] a shorter retention period may be advised.

(d.) Quality of LPR data

Although it seems intuitive that reliable LPR data that is accurately attributed to the right vehicles may be retained longer than LPR data that is of lesser quality or from a less reliable source, data quality is not a very useful criteria in the development of a retention period. Law enforcement agencies do not have any control over the quality of LPR photographs or OCR reads of those images. Moreover, even inaccurate OCR reads can yield positive results because the contextual photo may still contain valuable data. Thus, arguments that LPR data should be retained for a shorter period of time due to the uncertain quality of the information are unlikely to be persuasive.

(e.) Technologically implemented policy controls

Information technologies can be utilized to address potential risks of harm associated with accidental and abusive disclosure of the information. Policy controls that can be technologically implemented as part of a law enforcement data system include, but are not limited to, rule-based processing functions, selective revelation of data, encryption, and audit trails. Implementing policy controls promote the public's confidence in a law

[71] Public confidence in a law enforcement agency's ability to maintain the confidentiality of LPR data could be reduced due to the scope of that jurisdiction's freedom of information act.

enforcement agency's abilities to keep LPR data confidential and to limit misuse of the data by authorized and unauthorized users.

Where law enforcement agencies have reduced the risks of improper disclosure of LPR data through training and technologically imposed access restrictions on the data, a longer retention period may be appropriate. Where only minimal training or access restrictions are present a shorter retention period may be advised to reduce the amount of data in the LPR system available for inadvertent disclosure or purposeful misuse.

7

Part 7. Quality of LPR data

Data quality concerns implicated by the operation of a LPR program surround the quality of the license plate data collected by LPR cameras as well as the quality of the information contained on the hot lists that are uploaded to the system. This Part introduces the concept of information quality, describes the data quality issues surrounding OCR reads taken from contextual photos, and briefly discusses the accuracy of information contained in hot lists uploaded onto a LPR system.

A. INFORMATION QUALITY, CONCEPTUALLY

Information quality is a multidimensional concept encompassing critical relationships among multiple attributes.[72] For instance, the quality of a particular set of information can be expressed, among other ways, as the extent to which the data is: (a) available or easily and quickly retrievable; (b) appropriate for the task at hand; (c) regarded as true and credible; (d) easy to interpret and apply to different tasks; (e) correct and reliable; or (f) unbiased, unprejudiced, and impartial.[73] Together, these attributes contribute to the validity of the information as it is used to make informed decisions. Good information quality is the cornerstone for sound decisions by law enforcement officers and inspires trust in the criminal justice system and in the agencies that use information.

Data quality takes on significant importance in the development of information sharing policies. Law enforcement agencies may be more reluctant to share data that is of poor or uncertain quality, preferring instead to share data that can be verified as accurate. Restricting the dissemination of potentially inaccurate data helps to limit the possibility that subsequent users will act or rely upon erroneous information.

Incorporating data quality principles into a privacy or information management policy requires a careful consideration of the accuracy of data contained in the information system and the documentation of the protocols that will be used to locate and correct erroneous information.

---

[72] U.S. Dept. of Justice, *Information Quality: The Foundation for Justice Decision Making*, 1 (Feb. 2008) available on-line at http://www.it.ojp.gov/documents/IQ_Fact_Sheet_Final.pdf.
[73] *Id.* at 2.

B. ACCURACY OF LPR COLLECTION OF LICENSE PLATE NUMBERS

LPR cameras capture images of vehicles and license plates; optical character recognition (OCR) software utilizing sophisticated algorithms translate the alphanumeric characters on each license plate into an electronically readable format. The image collected by a LPR camera is maintained in the information system to provide a means of ensuring that the license plate number was properly converted into an electronically readable format.[74] A LPR system's ability to accurately identify the characters on a license plate lies at the heart of the data quality issue.

1. OCR ACCURACY

Many variables affect OCR accuracy. Each state has multiple license plate designs and plates vary significantly from state to state. For maximum effectiveness, LPR systems must be properly configured to recognize the design and layout of plates most likely to be encountered in the area of operation. The shape of the characters, amount of contrast between a particular state's background and the color of the license plate's characters, and whether the characters are raised or flat can all impact the accuracy of the OCR read.

Poor image resolution, and thus poor character recognition, can be the result of several factors. License plates can be too far away for the capabilities of the LPR 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. 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 LPR circumvention device.

Increasing the height of the LPR camera may correct some of these problems; however, changing the position of the LPR camera with respect to the license plate it is supposed to read may require the system to adjust for the new orientation and increased skew of the license plate.

From time to time, states may make significant changes in their license plate formats and designs that can substantially impact OCR accuracy. For instance, a state might add a character or issue a new license plate design. LPR systems must adapt to these changes quickly in order to remain effective.

Sometimes the letter D is mistaken for a Q or an O. Other times, the characters on the license plate are sometimes cut off from the frame of the image; when this occurs, the OCR software may incorrectly read an E as an F or a Z as a 7. Some colors, especially reddish tones, may be difficult for LPR system OCR software to read. Learning the type

[74] Law enforcement agencies should not strip the image from the OCR information in order to save storage space; the OCR information cannot be verified without the contextual photo.

of mistakes LPR system's OCR software makes can help investigators run queries on potentially-misread license plate numbers.

2. COMPARISON OF OCR INFORMATION WITH HOT LIST DATA

Another data quality challenge involves the comparison of the OCR data with the license plate numbers on a hot list. States develop license plate number formats robust enough to provide unique serials for all the motor vehicles the jurisdiction expects to register. Less-populous states may use six-character formats whereas more populous states may choose to utilize a seven-character format.[75] Complicating this factor is the fact that multiple states may utilize the same alphanumerical formats; for example, neighboring states may use three letters followed by four numbers. Thus, two cars from different jurisdictions could have the same number, but different license plate designs.[76] This means that each time a law enforcement officer is alerted to the proximity of a vehicle displaying a license plane number contained on a hot list, the user should make certain that the plate that caused the alert matches the hot list data.

C. ROUTINE DATA QUALITY AUDITS OF INFORMATION SYSTEMS

Although law enforcement officers are able to visually confirm an OCR read against the contextual image, regular and systematic audits can also ensure that the quality of data contained in the LPR system remains high. There is also considerable precedent for subjecting law enforcement computer systems to data quality audits.[77] Data quality audits are distinct from system usage audits and focus on the accuracy of the information. In the context of a LPR system data quality audits would concentrate on measuring the accuracy of the OCR output when compared with contextual images.

As discussed above in Part 6, law enforcement agencies have no way to influence the accuracy of the OCR performed upon an image captured by a LPR camera. Nevertheless, law enforcement agencies will rely upon the accuracy of LPR data as they conduct their investigations. Conducting data quality audits is another method of ensuring that law enforcement officers rely upon accurate and complete LPR data. Data quality audits also have the ability to identify routine errors made by OCR software thereby identifying concrete areas for future improvement.

[75] Delaware and Rhode Island are able to use formats of 123456 and 123-456, respectively, while several populous states use seven-character formats, including 1ABC234 in California, AB1-C234 in Texas, A12-3456 in Illinois, and ABC-1234 in New York, Pennsylvania, Ohio, Georgia, North Carolina, Virginia, and Arizona.

[76] This is also common in the area of vanity license plates.

[77] Mandatory audits are routinely conducted of official criminal history record information (CHRI) repositories to measure the accuracy, completeness, and timeliness of their data. *See* 28 C.F.R. § 20.21(e). These audits are one of the reasons the justice system and society have deemed official CHRI records reliable enough on which to base important decisions affecting individuals' liberty interests.

Law enforcement agencies should develop procedures for identifying and correcting inaccurate OCR reads. Data corrections may be performed on an *ad hoc* basis by investigators as they utilize the LPR system in the course of their investigations or by auditors conducting a formal data quality audit.

D. ACCURACY OF INFORMATION CONTAINED IN HOT LISTS

It is axiomatic that law enforcement officers would have access to the license plate numbers contained on any LPR hot lists. Nevertheless, many hot lists are compiled or administered by entities other than the law enforcement agency utilizing the LPR system. This means that law enforcement agencies frequently do not have supporting documentation regarding why a particular license plate number is on a particular hot list.

Because law enforcement officers will act upon a LPR system hit, it is important that information contained in hot lists is accurate. NCIC requires that records entered into the vehicles hot list be double checked by a second party to verify that the data entered matches that contained in an investigative file.[78]

Law enforcement agencies utilizing a LPR system may develop procedures to verify with the hot list's author that a license plate number is properly on the list prior to taking certain arrest-type actions. Thus agencies compiling hot lists for later use in an LRP system should maintain records sufficient to verify the accuracy of the hot list data.

The heads of law enforcement agencies are ultimately responsible for determining which hot lists will be uploaded onto the agency's LPR system and what actions officers take in response to a LPR hit. Agencies may want to establish some criteria for determining which hot lists will be uploaded onto the LPR system. Those criteria may include indicia of the hot list's accuracy and the ease with which law enforcement officials can verify, from the field, that a particular license plate number properly belongs on the hot list. Moreover, law enforcement agencies utilizing a LPR hot list should take steps to confirm which agency (i.e., the law enforcement agency utilizing the LPR system or the agency that authored the hot list) is ultimately responsible for the quality of the data contained on the hot list.

E. NO INDIVIDUAL RIGHT TO ACCESS OR CHALLENGE LPR DATA

As LPR data alone is not personally identifiable, there is no need to extend to individuals a right to access or challenge LPR data concerning the vehicles registered in their name.

---

[78] U.S. Dept. of Justice, Federal Bureau of Investigation, *National Crime Information Center Mandatory Minimum Standards Curriculum for Full Access Terminal Operations*, LPF-17; LPR-22 (1992) available on-line at: http://www.eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=ED354315&ERICExtSearch_SearchType_0=no&accno=ED354315.

Moreover, LPR systems simply collect and compile images of vehicles (and in some instances vehicle occupants) that pass within range of a LPR camera. That contextual picture depicts the scene captured by the LPR camera; there is no basis under which an individual could reasonably challenge the contents of the photograph. Furthermore, there is less of a need to provide individuals with an opportunity to access LPR data because the information is not released to the public.

Nor is it appropriate or necessary to grant individuals access to review or challenge hot list information since doing so would likely interfere with pending or future investigations. Although federal statutes grant individuals a right to access and challenge to certain criminal justice related information concerning them,[79] there is no comparable right to investigative information.[80] Additionally, hot lists enhance law enforcement agencies' ability to detect crime and provide critical officer safety information. Thus, LPR hot lists, which consist only of license plate numbers, are not the type of personally identifying information that would ordinarily be subject to an individual's right to access and challenge.

[79] *See* 28 C.F.R. § 20.21(g)(1).

[80] *See* 28 C.F.R. § 20.3(d) (excluding investigative information from the definition of criminal history record information).

8

Part 8. Accountability for LPR data

Many privacy concerns can be mitigated by holding law enforcement agencies accountable for the information they collect and how they subsequently use that information. This Part describes several methods by which agencies can ensure that they are complying with applicable policies regarding the appropriate collection and use of LPR data. Utilizing tamper-proof audit trails combined with oversight in the form of real-time monitoring and subsequent analysis of LPR system usage can provide a check on the privacy concerns described earlier in this Report.[81] Training authorized users is also a critical accountability measure.

A. AUDIT LOGS

The primary goal of maintaining audit logs is to deter and discover users' abuse and misuse of a LPR system. Programmatic audit trails should be built into LPR systems and such logs should be checked for inconsistencies that raise a suspicion of abuse. Law enforcement officers may be discouraged from requesting LPR data if they know that their access to that data is being monitored and recorded; nevertheless, such audit capabilities can be an effective means to discourage unnecessary or inappropriate use of LPR data and trace any improper uses to the offending party.

In order to facilitate the periodic and random audits necessary to monitor user compliance with relevant laws and policies, audit logs should include certain information. Specifically, queries to a LPR system should be logged and include: (1) the identity of the user initiating the query; (2) the license plate number or other data elements used to query the LPR system; (3) the date and time of the inquiry; and (4) the response to the user's query.

B. SECONDARY DISSEMINATION LOGS

Since LPR data is for official use only, and because LPR data is collected for specified purposes, instances where LPR data is disseminated outside the originating agency should be documented in a secondary dissemination log. Such logs, like programmatic audit trails, help law enforcement agencies monitor the use of LPR data. When information from a LPR system is disseminated outside the law enforcement agency, a

[81] See K. A. Taipale, *Technology, Security And Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123, 151 (2005).

log should be maintained that contains: (1) a description of the LPR data disseminated; (2) the date and time the information was released; (3) the identity of the individual to whom the information was released, including their agency and contact information; and (4) the purpose for which the LPR data will subsequently be used.[82]

C. MONITORING AND CONDUCTING AUDITS OF SYSTEM USE

Audits of LPR systems help to ensure that law enforcement agencies are operating in accordance with the policies developed to regulate the collection, use, and dissemination of LPR data. An audit of a LPR system involves an evaluation of the law enforcement agency's operations as recorded in its audit logs to determine if the agency is administering its LPR system in accordance with its information management policies. LPR system audits should focus on ensuring that LPR data is only disclosed to authorized users and that the information is utilized for official purposes only. To do this, auditors should be familiar with common misuses of LPR data.

Existing law enforcement data systems already have policies that include prohibitions against misuse of criminal justice data; those policies also frequently impose penalties for such misuse. These existing policies may inform information management policies against misuse of data contained in a LPR system.

D. POLICY AWARENESS AND TRAINING

Personnel employed by law enforcement agencies should be informed about why policies limiting access, use, and dissemination of LPR data are important and how those policies protect the agency and the public. Moreover policy education and awareness surrounding LPR systems is a continual process that must be regularly updated as laws and regulations governing LPR data or law enforcement's access to information change over time.

Each law enforcement agency will have the responsibility of ensuring that its employees have completed training about the appropriate use and sharing of LPR data. LPR system policies should be easily accessible by law enforcement agency employees and, depending upon the level of detail, available to the public as well.[83] Users should be educated and informed about how LPR policies will be enforced, including any penalties for committing violations of the policy provisions.

Law enforcement agencies may consider having each individual with access to the LPR data acknowledge their access to and thorough understanding of LPR system policies.

---

[82] The DPPA contains a similar requirement; see 18 U.S.C. § 2721(c).

[83] Where LPR system policies are considered too detailed, law enforcement agencies may consider developing a guidance document to inform the public, in general terms, of practices and procedures developed to address privacy concerns surrounding LPR data.

Law enforcement agencies should monitor relevant legislative and regulatory activity and update LPR system policies accordingly. When policies are updated, those individuals having access to LPR data should be informed of the changes and when those new terms take effect.

A:1

Appendix 1: 2007 Resolution on LPR Systems

In 2007, the International Association of Chiefs of Police ("IACP") passed the attached resolution in support of License Plate Reader (LPR) technology. The resolutions adopted by the IACP at the114th Annual Conference in New Orleans, Louisiana on October 16, 2007 are available on-line at http://www.iacp.org/resolution/2007Resolutions.pdf.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

RESOLUTION

Adopted at the 114th Annual Conference
New Orleans, Louisiana
October 16, 2007

SUPPORT FOR LICENSE PLATE READER SYSTEMS

Submitted by the Narcotics & Dangerous Drugs Committee
NDD.020.a07

WHEREAS, effective anticrime programs are effective antiterrorism programs; and evidence indicates that terrorist organizations which are funded in part by the sale of illegal drugs adds a new dimension to the need for continued investigation of narcotics related crime; and

WHEREAS, license plate reader and related digital photographing systems at border checkpoints incorporate the use of technology that provides a searchable database, including associated photographic images; license plate information; and statistical data such as date, time, and entry lane; and

WHEREAS, license plate reader systems and related digital photographing systems, working in combination with existing law enforcement databases, have the potential capability of identifying conveyances used for illegal activity, including the transportation of drugs and bulk cash; and

WHEREAS, law enforcement intelligence information may be shared more efficiently through greater use of technology and information sharing programs such as license plate reader systems to help ensure that investigative links are made to organized drug trafficking and related crime to the maximum extent possible; and

WHEREAS, all countries are encouraged to use technology such as license plate reader and related digital photographing systems, where practical, to share appropriate law enforcement information; and

WHEREAS, license plate reader and related digital photographing systems provide law enforcement with important tools necessary to combat all types of crime and is particularly useful in combating narcotics trafficking; and

WHEREAS, a significant commitment of resources will be required by federal, state, and local law entities to fully take advantage of this emerging technology; now, therefore, be it

RESOLVED that the International Association of Chiefs of Police duly assembled at its 114th Annual Conference in New Orleans, Louisiana, strongly encourages the U.S. Congress to fully fund license plate reader and related digital photographing systems, including interrelated

information sharing networks, for the northern and southern borders of the United States; and, be it

FURTHER RESOLVED that all countries are encouraged to use like technology, to the extent possible, to share appropriate law enforcement information; and be it

FURTHER RESOLVED that the IACP supports the development of a comprehensive License Plate Reader guide for law enforcement executives that addresses current technologies; best practices; privacy issues, legal implications, and open source data systems.

A:2

Appendix 2: Issues Document

Issue identification: Privacy issues concerning the utilization of automated license plate readers is attached to provide additional context and areas of privacy concern that may not have been directly addressed in the PIA Report.

Issue identification:

Privacy issues concerning the utilization of automated license plate readers

March 24, 2009

INTRODUCTION

Law enforcement agencies across the country are utilizing or seeking to utilize automated license plate readers. There is currently no uniform guidance concerning the appropriate collection, use, dissemination, and retention of information collected by automated license plate readers. This is problematic because collecting license plate data, which is frequently associated with or connected to personally identifiable information concerning individual drivers, could be considered a form of surveillance. Assessing the privacy risks associated with the broad use of automated license plate readers and developing policies to address those risks will help ensure that license plate data is managed in such a way as to meet public safety needs while protecting individuals' privacy interests.

This document represents the Automated License Plate Reader Policy Working Group's efforts to document the privacy concerns that should be addressed by any criminal justice agency utilizing automated license plate readers or data collected by another agency's use of these devices.

This document is intended to continually evolve as additional uses for license plate reader information come to light. It will lay the foundation for the development of a guidance document intended to: (1) assess the impact of automated license plate readers on the public's privacy interests; and (2) propose procedures and policies intended to protect the public's privacy interests while meeting the goals of law enforcement.

Table of contents

1. General privacy considerations 1
   A. LICENSE PLATE NUMBERS AS PERSONALLY IDENTIFIABLE INFORMATION 1
   B. PUBLIC'S PERCEPTIONS OF AUTOMATED COLLECTION OF LICENSE PLATE DATA 1
   C. ADDRESSING THE CONCEPT OF PRACTICAL OBSCURITY 2
   D. TYPES OF PRIVACY HARMS SURROUNDING THE USE OF LPRs 3
   E. FAIR INFORMATION PRACTICES 4
2. Potential Uses of LPR data 6
   A. CRIME ANALYSIS 6
   B. ALERTS AND HOT LISTS 8
   C. TRACKING INDIVIDUALS 9
   D. IDENTIFY PREVIOUSLY-UNDETECTED CRIMES 10
   E. REVENUE COLLECTION 11
3. Collection 12
   A. LICENSE PLATES PROVIDE ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION. 12
   B. LPR DEPLOYMENT 13
   C. NOTICE OF DATA COLLECTION 13
   D. "OWNERSHIP" OF LPR SYSTEM DATA 14
   E. LAW ENFORCEMENT COLLECTION OF LPR DATA COMPILED BY OTHER ENTITIES ... 14
   F. COMPILATION AND SUBMISSION OF "HOT LISTS" 15
4. Access to and Dissemination of LPR Data 16
   A. SHARING LPR DATA AMONG LAW ENFORCEMENT AGENCIES 16
   B. SHARING LPR DATA WITH OTHER GOVERNMENT ENTITIES 17
   C. PUBLIC ACCESS TO LPR DATA 18
   D. ACCESS AND DISSEMINATION OF "HOT LIST" DATA 19
5. Retention 19
6. Accountability issues 21
   A. DECIDING TO USE LPRS 21
   B. ACCOUNTABILITY DURING POLICY DEVELOPMENT 21
   C. ACCOUNTABILITY PROVISIONS CONTAINED IN A PRIVACY POLICY 22
7. Data quality 23
   A. ACCURACY OF LPR COLLECTION OF LICENSE PLATE NUMBERS 23
   B. ACCURACY OF INFORMATION CONTAINED IN HOT LISTS 24
   C. PARTIAL LICENSE PLATES 24
   D. RIGHTS TO ACCESS AND CHALLENGE LPR DATA 24
8. Intelligence issues 25
9. Security 26

1. General privacy considerations

A. LICENSE PLATE NUMBERS AS PERSONALLY IDENTIFIABLE INFORMATION

Although license plates function primarily to uniquely identify automobiles, there is no doubt that many of the anticipated uses of license plate data involve acquiring the identity of the registered owner of the automobile. It is important to note that, because most law enforcement data systems have been designed with traffic stops in mind, it is very easy for a police officer to obtain information about vehicle owners and drivers from license plate information.

(1.) Because the license plate number operates in such a manner as to link the vehicle to its registered owner, should license plate numbers be discussed or treated in a manner similar to personally identifiable information?
(2.) Does it matter that law enforcement agencies and DMVs and their authorized employees are the only individuals able to access personally identifiable information from license plate data?
(3.) What anticipated uses of recorded license plate numbers involve accessing personally identifiable information about the vehicle's register owner?
(4.) What anticipated uses of recorded license plate numbers involve the mere monitoring or otherwise identifying a vehicle?

B. PUBLIC'S PERCEPTIONS OF AUTOMATED COLLECTION OF LICENSE PLATE DATA

There is no controlling legal precedent directly addressing the privacy implications surrounding law enforcement agencies' use of automated license plate readers ("LPRs"). Even though analogous cases suggest that the use of LPRs does not violate constitutional privacy protections, this does not mean that the public's perceptions of the use of this technology are addressed; nor should the fact that license plate numbers are publicly displayed end the inquiry.

It is likely that the public would consider the use of LPRs as a form of surveillance. Surveillance is the watching, listening to, or recording of an individual's activities. The potential harm of surveillance comes from its use as a tool of social control. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition. Too much social control can adversely impact freedom, creativity, and self-development.

(1.) It may be desirable to educate the public as to what information is collected by LPRs, how that information will be used, what information is available to criminal justice agencies and what information is available to the public. Are there any risks of informing the public about an agency's utilization of LPRs and how the information will be used?

(2.) One of the most important notions underlying the Fair Information Practices[1] is the concept of notice; specifically, people should be informed when information about them is being collected in order to make an informed decision as to whether and to what extent to disclose information about them. In the context of LPRs, this would involve posting signs explaining to motorists that their license plates are being electronically read and recorded, thus affording them an opportunity to take a different route if they desired. Should motorists be informed of the presence of fixed and mobile LPRs?

(3.) Driving is considered by state governments as a privilege and not a right. How does treating driving as a privilege affect the nature of the data collection and the public's perceptions of the surveillance?

C. ADDRESSING THE CONCEPT OF PRACTICAL OBSCURITY

Privacy issues will always be generated by the collection and storage of information about the behavior of people not suspected of criminal activity regardless of whether that information is recorded by hand or compiled electronically. License plates function to uniquely identify automobiles. Frequently, license plate numbers are associated with the vehicle owner's driver's license number, which functions to uniquely identify the individual. Thus, automated license plate scanners have the potential to track the movement of individuals who have not committed and are not suspected of committing criminal acts.

Viewed in isolation, each piece of information created by one's day-to-day activities is not telling; however, viewed in combination, that information begins to paint a portrait of that individual's personality. It arises from the fact that data systems enable information from disparate sources to be easily collected and analyzed. In the context of LPRs, information such as a license plate number, while not in and of itself informative, provides access to a host of additional information such as the registered owner's identity and criminal history information.

The U.S. Supreme Court, in *U.S. Dept of Justice et al. v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 764 (1989), has recognized a difference, for purposes of evaluating privacy interests, 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 single clearinghouse of information. Ultimately, 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 information in such a way as to restrict the disclosure of the computerized summary of that information.

[1] The Fair Information Practices are addressed below in Section 1(E) of this document.

Manually recording license plate numbers of vehicles traveling near a particular location is an arduous and, depending upon the traffic conditions, impossible task without the use of camera technology. LPRs, however, can create summaries of all license plate numbers traveling past that camera. Just like in the *Reporters Committee* case, the use of advanced technology (i.e., LPRs) to compile otherwise difficult to obtain information (i.e., license plate numbers of every vehicle traveling past a particular location), even where that information is publicly and openly available, changes the public nature of that information and raises the privacy interests surrounding that information.

(1.) It is not enough that police are authorized to watch for and write down license plate numbers. The ability to collect vast quantities of license plate numbers and store them in a manner that facilitates analysis and tracking of vehicles carries with it privacy concerns. How does increasing the scale of the collection of data by means of LPRs remove practical obscurity as a source of privacy protection?
(2.) If license plate data is publicly available and is not cause for privacy concern, doesn't it stand to reason that law enforcement agencies would have no reason to deny any member of the public access to LPR data?
(3.) License plate data stored electronically may be combined with other data sources to create a more complete picture of individuals associated with certain vehicles. What other data sources may be combined with license plate data collected by LPRs?
(4.) Under what circumstances would the types of data identified in Issue 3 above be combined?

D. TYPES OF PRIVACY HARMS SURROUNDING THE USE OF LPRs

Poor data management can make people more vulnerable to harm (i.e., injuries to the individual's dignity, person, or financial well-being). Moreover, data collection activities, including but not limited to the use of LPRs, can upset the balance of social or institutional power in undesirable ways; the classic example of this issue is the potential chilling effect of being able to easily track individuals' vehicles and readily identify people based upon the vehicle they are driving. Privacy harms generally fall into four categories: information collection, information processing, information dissemination, and invasions.

(1.) Surveillance is the watching, listening to, or recording of an individual's activities. The potential privacy harm of surveillance is its potential use as a tool of social control: the mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition. What is the potential surveillance impact of LPRs?

(2.) Identification is the act of connecting data to particular individuals. Identification enables surveillance by facilitating the monitoring of a person. The potential harm of identification is that it increases the government's power to control individuals. It can inhibit one's ability to be anonymous, which is important in so far as it protects people from bias based on their identities and enables people to vote, speak, and associate more freely by protecting them from the danger of reprisal. How can LPRs impact motorists' ability to associate and move freely?

(3.) Secondary use is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent. The potential privacy harm of secondary use is dignitary in nature in that it can undermine people's reasonable expectations as to the future use of the information about them. Another problem with secondary use is that data may be misunderstood when it is removed from its original context. What are the likely secondary uses of data collected by LPRs?

(4.) Aggregation is the gathering together of various pieces of information about a person. These issues are discussed in Section 1, Part C ADDRESSING THE CONCEPT OF PRACTICAL OBSCURITY above.

(5.) Breach of confidence involves breaking a promise to keep a person's information confidential. The harm caused by a breach of confidentiality is not simply that information has been disclosed, but that the promise made to the subject of the data has been broken. Protections against breach of confidentiality help promote certain relationships that depend upon trust, such as the relationship between citizens and their government. How will law enforcement agencies utilizing LPRs keep the license plate information confidential and secure?

(6.) Disclosure occurs when certain true information about a person is revealed that impacts the way others judge her character. The potential harm of disclosure involves the damage to an individual's reputation caused by the dissemination. Disclosure can also be a form of social control and carries with it the potential chilling effects associated with surveillance. How, when, and to whom will the data collected by LPRs be disseminated or disclosed?

E. FAIR INFORMATION PRACTICES

In 1973, the U.S. Department of Health, Education, and Welfare published a groundbreaking report responding to concerns that harmful consequences may result from the storing of personal information in computer systems. That report, entitled "Records, Computers and the Rights of Citizens," articulated several principles the Department deemed essential to the fair collection, use, storage, and dissemination of personal information by electronic information systems.[2] The report was one of the earliest acknowledgements by the federal

[2] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, Records, Computers and the Rights of Citizens: Report of The Secretary's Advisory Committee on Automated Personal Data Systems xx-xxi (1973), available at

government that the public's privacy needed to be protected against arbitrary and abusive record-keeping practices. The report also recognized the need to establish standards of record-keeping practices appropriate for the computer age.

The Fair Information Practices are a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. The practices include eight guiding principles that evolved from the 1973 report. Any privacy guidance for LPRs should consider incorporating the following principles.

(1.) Collection Limitation Principle – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Should certain criteria be met before using a license plate number acquired by an LPR to obtain the identity of the vehicle's registered owner?

(2.) Data Quality Principle – Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. How accurately do LPRs record license plate numbers?

(3.) Purpose Specification Principle – The purposes for which personal data are collected should be specified not later than at the time of data collection. Additionally, the subsequent use should be limited to the fulfillment of those purposes or other compatible purposes.

(4.) Use Limitation Principle – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: (a) with the consent of the data subject; or (b) by the authority of law.

(5.) Security Safeguards Principle – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. This document focuses on privacy issues and will not discuss specific, technical security measures.

(6.) Openness Principle – There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of its use, as well as the identity and usual residence of the data controller. Will privacy guidance and/or the privacy policy regulating the use of LPR data be made available to the public?

(7.) Individual Participation Principle – An individual should have the right to: (a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) have communicated to him,

---

http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. Where license plate data is not utilized to access the identity of the registered owner of a vehicle, it is likely that this principle would not apply; nevertheless, should this principle be given effect for LPR data subsequently used to identify an individual's whereabouts?

(8.) Accountability Principle – A data controller should be accountable for complying with measures that give effect to the principles stated above. Accountability issues are discussed in their own section of this document.

2. Potential Uses of LPR data

Identifying the intended uses of LPR data is critical to assessing the privacy impact of law enforcement agencies' collection, analysis, and maintenance of license plate data. Moreover, how government agencies use the data they collect is of significant concern to the public. In accordance with the Purpose Specification and Use Limitation principles discussed above, a sound privacy policy should clearly identify appropriate and intended uses of the data contained in the information system.

A review of the existing literature concerning LPRs reveals five primary uses of LPR data; each anticipated use carries with it certain privacy risks that should be addressed.

A. CRIME ANALYSIS

Police agencies utilize crime analysis to prevent and suppress crime, apprehend offenders, and recover stolen property.[3] Crime analysis is usually conducted on offenses with discernable patterns and trends that can be prevented or reduced through the implementation of directed action plans.[4] A review of existing police crime analysis operations reveals that burglary, robbery, auto theft, larceny, fraud, sex crimes, aggravated assaults, and murder are the crimes most appropriate for crime analysis.[5]

There are three types of crime analysis: tactical, strategic, and administrative. Tactical analysis is the first priority of police departments.[6] Specifically, tactical crime analysis (a) detects crime patterns and series by studying and linking common elements of crimes;[7] (b) predicts when and where future events will

[3] Steven Gottlieb, *et al.*, Crime Analysis: From First Report to Final Arrest 14-16 (1994).
[4] *Id.*
[5] *Id.* at 133.
[6] *Id.* at 15.
[7] A crime pattern is merely a set of similar offences happening in a specific geographical area while a crime series is a crime pattern that appears to be done by either the same person or group of persons.

occur; and (c) provides information to officers regarding specific crime problems and is intended to result in the arrest of a suspect.[8]

Strategic crime analysis concentrates on long-term crime trends and is used to project where police presence should be increased or decreased. Administrative analysis, unlike tactical- and strategic crime analysis, interprets crime statistics categorized by economic, geographic, or social conditions and provides information for grant applications, feasibility studies, and city council reports.[9] Thus, administrative analysis provides information useful in running a police department while tactical and strategic crime analysis is intended to help the police department protect the public and enforce the criminal laws.

When law enforcement agencies talk about using LPR data to check crime series information to determine if the same vehicles are in the area of different crime scenes, they are referring to tactical crime analysis. Tactical crime analysis is used to determine who is doing what to whom and focuses on crimes against persons and property. Categories of data considered most useful for crime analysis are those relating to:[10]

- Geographic factors[11]
- Victim descriptors
- Physical evidence descriptors
- Suspect descriptors
- Time factors
- Property loss descriptors
- Specific *modus operandi* factors
- Suspect vehicle descriptors

(1.) What presumptions are inherent in tactical crime analysis with regard to vehicles?
(2.) Is it presumed that the registered owner of a vehicle is always the driver at the time the license plate number is recorded by an LPR?
(3.) Is it presumed that an individual is always near the location where his automobile is parked?
(4.) Is it presumed that an individual always parks near the location he intends to visit or reside?
(5.) Is it presumed that a registered owner always knows the identity of who is driving his vehicle at any given time?

Shawn A. Hutton & Mark Myrent, Incident-Based Crime Analysis Manual 34 (ILL. CRIM. J. INFO. AUTH. 1999).

[8] *Id.* at 7.

[9] Gottlieb, *supra* note 3 at 15 (stating that administrative analysis essentially includes the "nice to know stuff.").

[10] *Id.* at 128. Experienced analysts have found that the importance of each factor differs depending upon the type of crime being investigated. For example, suspect vehicle descriptors are more useful in determining whether a pattern of thefts from vehicles exists than a pattern of strong armed robberies. See *Id.* at 318-320.

[11] Spot maps can be of great assistance to the analyst. Nevertheless, spot maps will only depict crime patterns; additional information is necessary to determine if a crime pattern is also a crime series.

(6.) How do the presumptions involved in tactical crime influence when a license plate number collected by an LPR will be used to gather personally identifiable information about a vehicle's registered owner?
(7.) Are there ways that an individual's identity can be linked to a license plate number other than being a registered owner, perhaps through sex offender registration or gang member intelligence record?

B. ALERTS AND HOT LISTS

License plate numbers of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts are routinely added to "hot lists" circulated among law enforcement officers. These lists serve an officer safety function as well as an investigatory purpose.

Hot lists are typically transferred daily and can be updated by an operator/officer in the field. Hot list information can come from a variety of sources, including but not limited to, stolen vehicle information from the National Insurance Crime Bureau and 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 police departments can also interface their own hot lists to the LPR system.

LPRs function in such a way as to notify an officer when a license plate on the hot list is observed; this can be the case for both fixed and mobile LPRs. LPR data can also be searched retroactively to identify a time and location of where a vehicle on a hot list was observed by the LPR camera.

(1.) What are the criteria for adding a license plate number to a hot list that would interface with an LPR?[12]
(2.) Do these criteria include or consider the proper attribution of a license plate number to an individual?
(3.) Is the license plate number on a hot list essentially being used as a proxy for the individual's name or other personally identifying information?
(4.) How are partial license plates handled for hot list purposes? (This may be a data quality issue as well.)
(5.) There may be instances where a license plate is incorrectly included on a hot list, perhaps because of an error in data entry or because the license plate number was attributed to the incorrect person. Is there a process or system in place to remove license plate numbers from hot lists or LPR systems in

[12] For instance, in order to activate an America's Missing: Broadcast Emergency Response (AMBER) Alert. A juvenile (a) must have been confirmed as abducted; (b) is under the age of 16 or has a proven mental or physical disability; and (c) is in danger of serious bodily injury. There also needs to be enough descriptive information to believe that a broadcast alert will help. Are there similar, quantifiable standards for other hot lists?

response to identified errors? (This may primarily concern data quality but is added here in the interest of completeness.)

C. TRACKING INDIVIDUALS

Many of the justifications for LPRs include an element of tracking individuals. It has been suggested that sharing LPR data across jurisdictions can assist law enforcement officials in tracking the movements of drug smugglers, money laundering operations, documented gang members, sex offenders, individuals on parole or wanted on warrants, and missing persons.

In instances of mass evacuations, it has been proposed that LPRs could be used to track not only how many vehicles have left an area but also as a means of tracking who has evacuated in an attempt to respond to calls asking about the welfare or evacuation status of a relative.

LPRs have also been used to record the license plate numbers of vehicles visiting or parked at or near several locations, including but not limited to certain businesses, bars and night clubs, car dealerships, gun shows, and schools. The recording of these license plate numbers has occasionally been used to create a working database in the event a problem or violent crime occurs at some point in the future. As cars can't answer questions, any investigation utilizing these license plate numbers would involve identifying the registered owner of the vehicles whose license plates have been recorded.

It has also been put forward that LPRs can be useful in enforcing geographic limitations on the movements of sex offenders, probationers and parolees, and people subject to orders of protection. LPRs can record the license plate numbers of vehicles parked or observed near certain locations such as schools and day care facilities, or residences and work addresses of people protected by court orders. These locations and individuals' license plates can be added to LPR systems to bring any violations to an officer's attention.

(1.) This collecting of information is a type of surveillance similar to the use of cameras utilizing facial recognition software. The license plate reader isn't just recording an image, it is collecting license plate numbers in an electronic manner that can be used, perhaps at some future point automatically and in real-time, to access various types of information about the person(s) associated with that license plate.

(2.) The uses described above rely heavily on matching a license plate number to a unique individual. How is this done and how reliable is this process? (This is also a data quality issue.)

(3.) Not everyone owns or operates an automobile, especially in large cities. Does the utilization of LPRs to track individuals raise issues of selective enforcement (e.g., it's easier to track and identify "bad guys" with cars so

these people become the focus of enforcement efforts instead of people who are harder to observe/track due to their lack of cars)?

(4.) How will law enforcement agencies utilizing LPRs address the potential chilling effects of increased, potentially large-scale surveillance of license plate information?

(5.) Should there be some sort of triggering mechanism (e.g., articulable suspicion that a crime or other violation has occurred) to authorize access to the location information of individuals?

(6.) When using LPRs to enforce geographic limitations on certain offenders (e.g., probationers, sex offenders, persons subject to orders of protection, etc.,), should the location information about these individuals be limited to those instances where the subject's vehicle was observed in a prohibited area, as opposed to obtaining a listing of all the locations, dates, and times where the vehicle was authorized to be?

D. IDENTIFY PREVIOUSLY-UNDETECTED CRIMES

The American criminal justice system has never been based upon a theory of total enforcement of the criminal laws. Police departments' responsibilities have continually increased due to the rising number of criminal and regulatory offenses at every level of government; there have not been equivalent increases in police resources. Where more responsibilities meet limited resources, a system of selective enforcement was informally established in which public officials at all levels exercise discretionary powers to determine whether an individual enters the criminal justice system and how that individual progresses through the system.

Several of the proposed uses of LPRs concern identifying or observing previously undetected criminal conduct. Specifically, agencies seeking to utilize LPRs have identified several instances involving the commission of crimes that prior to the utilization of LPRs would not only have be extremely difficult to detect by police officers but would only have been discovered by the individual's chance encounter with authorities. For example, data collected by LPRs could be used to enforce geographic limitations on the movements of sex offenders, probationers and parolees, and people subject to various court orders.

LPRs could also be used to help implement programs intended to more efficiently bring certain crimes to law enforcement officers' attention. Several states have programs to combat auto thefts that permit vehicle owners to provide written consent for their vehicles to be stopped without cause during late evening hours. LPRs can provide an efficient means of implementing such programs.

The failure to obtain and provide proof of mandatory car insurance is grounds for several states to suspend license plates and driver's licenses. Unless these

vehicles are operated in such a manner as to raise the suspicions of a police officer, these uninsured vehicles would remain undetected. Operating an uninsured vehicle puts the public in danger in the event of an accident. Police departments have expressed interest in utilizing LPRs to identify vehicles with registrations suspended for failing to obtain mandatory insurance coverage.

LPRs, like surveillance cameras, are excellent tools to figure out what has already happened. Although LPRs may serve some deterrent effect provided their use is overt, they provide no real capability to prevent a crime from occurring.

(1.) LPRs may be perceived by the public as a way to automate the criminal justice system. What types of human review and verification are employed before data collected by LPRs is used to make a determination about an individual?
(2.) Given a police department's available resources, will certain crimes detectable by LPRs be focused on more so than others?
(3.) Is license plate data collected by LPRs more useful to prove a violation after it has been reported to a police department or should police departments have a policy of affirmatively reviewing all LPR data for potential violations?
(4.) Are concerns about inequality (e.g., discrimination against or in favor of reviewing certain neighborhood's LPR data) raised by only reviewing some LPR data as opposed to all data?
(5.) In order to identify vehicles that may be operated by individuals with suspended, revoked, cancelled, or expired driver's licenses (hereafter "unlicensed drivers"), it will be necessary for license plates to be linked to individually identifiable drivers. How will this be done?
(6.) It would seem that identifying vehicles potentially being operated by an unlicensed driver would be a real-time enforcement activity.

E. REVENUE COLLECTION

Many states suspend or revoke license plates and driver's licenses for an individual's failure to pay fees, fines, or taxes owed to governmental entities. Municipal police departments can also compile or receive lists of license plates issued multiple parking violations. LPRs can bring to an officer's attention vehicles whose owners owe outstanding debts to the government.

Revenue collection is distinct from the concept of revenue generation. LPRs do not create a stream of revenue for a jurisdiction in the sense that they generate the issuance of a ticket or citation. Rather, LPRs only help identify those who have already committed a violation or offence and, as a result, owe a fine.

(1.) It can be argued that LPRs are being employed to maximize compliance with the laws and regulations of the jurisdiction, which are presumed to promote

the public's safety and well-being. Nevertheless, it is likely that such activities will be perceived as a revenue collection measure.

(2.) Whereas law enforcement may access a great quantity of personally identifying information concerning individuals to investigate crimes and protect public safety, the balance between collecting revenue and preserving the public's privacy rights is considerably different.

(3.) Will revenue collection efforts potentially involve the transfer or LPR data to other non-law enforcement entities?

(4.) Local and state government agencies owed outstanding debts may only have limited personally identifying information of the debtor and very likely lack an individual's license plate number. Information obtained from these agencies must then be matched up to a license plate record contained in a department of motor vehicle record. Thus, the data from at least two sources is combined before it even goes into an LPR system. Do revenue collection efforts create additional data quality concerns with regard to linking individuals who owe the government fees, fines, or taxes to license plates?

(5.) Are there instances where a city department other than a law enforcement entity will be utilizing LPRs? If so, how does that affect the preparation of a Privacy Impact Assessment Report?

3. Collection

A. LICENSE PLATES PROVIDE ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Although license plates don't directly include personally identifiable information, they are frequently associated, by means of computer inquiries, with an individual owner. Thus, a license plate number serves as the gateway to personally identifiable information. In fact, many of the potential uses of license plate data rely upon the premise that the registered owner of a vehicle is actually driving it. The mere collection of information regarding individuals implicates privacy concerns. Fewer concerns are raised by the collection of information about individuals premised upon some reasonable suspicion that they are acting unlawfully. Great concerns regarding the public's privacy interests are raised when the government collects information about individuals for investigatory purposes absent any suspicion of criminal wrongdoing.

(1.) Exactly what information are LPRs capable of collecting?

a. Optical Character Recognition (OCR) of license plate numbers;
b. Digital images of license plates as well as the vehicle's make and model;
c. Digital image of the vehicle's driver;
d. Images of distinguishing features (e.g., bumper stickers, damage);
e. State of registration;
f. Camera identification;
g. GPS coordinates or other location information;

h. Date and time of observation;
i. Other data elements?

(2.) What information will agencies actually collect from LPRs?

(3.) What factors inform the balance of the amount of data collected to address privacy concerns while still meeting legitimate law enforcement needs?

(4.) How does the fact that license plate numbers constitute potentially identifiable information affect the compilation, access, analysis, and dissemination of LPR data?

(5.) Should certain criteria be met before using a license plate number acquired by an LPR to obtain the identity of the vehicle's registered owner? If so, what are the most appropriate criteria?

(6.) In most states, the minimum age for an individual to be issued a drivers license is below the age of majority. Thus, at any given time, LPRs may be collecting information concerning minors. How does this potential to collect information concerning juveniles impact the collection, analysis, dissemination, and retention of LPR data?

B. LPR DEPLOYMENT

LPR systems can observe and record over 1,000 license plates an hour in various lighting and weather conditions. LPRs can be fixed, mobile, or portable. A fixed LPR is permanently mounted, usually to a bridge or a pole, where as a mobile unit is permanently mounted to a marked patrol vehicle. A portable LPR can be moved from vehicle to vehicle or deployed in a covert configuration.

(1.) Notifying the public about the collection of license plate numbers by LPRs will differ significantly depending upon the type of LPR deployed.

(2.) Do the three manners of LPR deployment change or otherwise impact the privacy concerns surrounding the collection of license plate numbers? If so, should privacy policy guidance address the manner of deployment that causes the most privacy concerns or should any guidance address the manners of deployment separately so that agencies can select a manner of deployment that suits their needs best?

(3.) When will covert deployments be necessary for law enforcement efforts?

(4.) What are the advantages of covert deployments?

C. NOTICE OF DATA COLLECTION

Not only do the Fair Information Practices counsel collecting only that information that is relevant or necessary, but that the collection of data about individuals should be done with the knowledge or consent of the data subject.

Under the openness principle, agencies should provide notice about how they collect, maintain, and disseminate personal information. Complete notices generally include statements that: (a) describe the main purposes for the data's use; (b) identify the entity responsible for the data; (c) identify those who may

access or receive the data; (d) explain whether providing the information is mandatory or voluntary and the consequences of failing to provide the information; and (e) inform the data subject of any rights he may have to access the data and rectify errors.

(1.) Will privacy guidance and/or the privacy policy regulating the use of LPR data be made available to the public?
(2.) Would distribution of the privacy policy itself provide sufficient notice?
(3.) Is notification to individuals whose information has been collected made after covert deployment has been conducted? Should such a notification be made? What are the resource implications of providing this notice? Is this administratively burdensome?
(4.) Does the public know that the cameras they pass on roads are fixed LPRs by signage? By any other means?
(5.) How can the public be notified about an agency's utilization of mobile LPRs?
(6.) The Fair Information Practices also hold that agencies should communicate to affected individuals when personally identifiable information about them is requested or released to other parties. Should compliance with this requirement be applicable to LPR data? Would such compliance be unduly burdensome to the efficient administration of justice?

D. "OWNERSHIP" OF LPR SYSTEM DATA

Clearly establishing which entities have authority over and bear responsibility for the data contributed to the LPR system is of paramount importance. The concept of ownership, while complex in any plan to share electronic data, is critically important to identifying which entities are responsible for ensuring the proper management and treatment of the information as well as implementing any data quality safeguards.

(1.) What entity will ultimately be responsible for the operation of LPRs and the data collected by them?
(2.) What entity will ensure that data collected by LPRs is of sound quality?
(3.) What factors go into the determination of whether to share LPR data across jurisdictions?
(4.) Will the entity from which LPR data originates (i.e., the data "owner") maintain any controls on the subsequent uses and disseminations of the data?

E. LAW ENFORCEMENT COLLECTION OF LPR DATA COMPILED BY OTHER ENTITIES

Police and other criminal justice agencies are not the only entities utilizing or seeking to utilize LPR cameras. For instance, some shopping centers and individual stores are installing fixed LPR cameras at their entrances to capture license plates numbers. LPRs are also used by private companies that facility auto repossessions. Other government entities also collect LPR data; a county

agency responsible for operating a center for care of the elderly is interested in installing fixed LPRs to operate in conjunction with CCTV surveillance of the premises. Some of this privately collected LPR data may be made available to law enforcement agencies or actively sought after by police departments.

(1.) Should LPR data collected by other agencies be managed differently than data collected by the law enforcement agency's own LPRs?
(2.) Should LPR data collected by a non-law enforcement agency be treated differently than LPR data collected by a law enforcement agency?
(3.) Does the sale of LPR data by a law enforcement agency resemble a commercial use? Because the Fair Information Practices were first developed to address commercial uses of data, would it be advisable for a law enforcement agency interested in selling its LPR data to incorporate the FIPs into its data management policies?
(4.) Would selling the data call into question an agencies' position that the data should be treated as confidential?

F. COMPILATION AND SUBMISSION OF "HOT LISTS"

Many of the potential uses of LPR data require the comparison of license plate numbers collected by an LPR to numbers contained on a previously compiled list. These hot lists may be compiled by the local police department utilizing LPRs or compiled by other state or federal government agencies. The purpose of these lists is to bring to law enforcement officials' attention whenever the vehicle or individual somehow associated with that vehicle is nearby so that police officers can act accordingly. Actions taken by police officers will vary depending upon the list that contains the vehicle's license plate number.

(1.) What hot lists are law enforcement agencies likely to utilize as part of an LPR program?
(2.) Under what authority are hot lists created and how does a license plate number get submitted or included on a hot list?
(3.) While some hot lists focus on identifying a particular vehicle (e.g., stolen cars, AMBER alerts, etc.), other lists seem to focus on trying to identify and locate specific individuals (e.g., sex offenders, wanted persons, etc.). What steps are taken to link an individual with a license plate?
(4.) Are the links between license plates and individuals verified or updated on a regular basis?
(5.) Various government agencies compile hot lists that law enforcement agencies may consider utilizing. Do hot lists developed by law enforcement agencies carry privacy implications different from hot lists developed by other government, but non-law enforcement agencies?
(6.) What is the range of actions police officials take when an LPR identifies a license plate number contained on a hot list? Do police take any steps to verify that a license plate number is properly on the hot list?

(7.) If an officer stops a vehicle due to its inclusion on a hot list, may the officer reveal to the driver the reason the license plate was added to the hot list or the name of the agency that created the hot list?

4. Access to and Dissemination of LPR Data

LPR systems that electronically collect, analyze, and share license plate number data have the potential to improve the criminal justice system by enhancing the types of data available to apprehend offenders and identify previously undiscovered criminal activity. LPR data, when appropriately shared, can reveal relationships among persons, places, vehicles, and activities that would not be readily apparent in a paper-based information-sharing environment.

A. SHARING LPR DATA AMONG LAW ENFORCEMENT AGENCIES

Police officials have a general duty to investigate crimes and criminal conduct. To fulfill this responsibility, police officials collect, analyze, disseminate, and retain a variety of information.

It has long been a basic tool of criminal investigators to start with known subjects, and, with proper authorization, to look for information about them and the people with whom they interact. LPR data could provide police officials with information concerning the possible location of individuals and, as a result, identify new individuals for investigation because of their connection with a suspect or incident location. Although some of the connections revealed by an analysis of LPR data may be tenuous, it is the role and responsibility of police officials to exhaust investigative leads.

(1.) It is axiomatic that the real-time operation of mobile and portable LPR units results in a police official's access to LPR data, most frequently in the form of notifications that officer is near a vehicle contained on a hot list.

(2.) There seems to be a distinction between (a) a notification to a police official that a vehicle bearing a license plate number that is also contained on a hot list and (b) accessing stored LPR data concerning the times and locations a vehicle was observed. It is proposed that these purposes for accessing LPR data be addressed separately. Can these purposes for access be referred to as: (a) "notification data" and (b) "historic LPR data"?

(3.) Should there be a triggering device before a police official can access LPR data contained in some type of data repository concerning the times and locations a vehicle was observed? If so, what should that trigger be (e.g., reasonable inference of criminal conduct, reasonable suspicion, demonstrable need to know)?

(4.) It is envisioned that LPR system data will be used in various forms of crime analysis. How will this crime analysis be conducted? What information will the results of the crime analysis contain and who may access these results?

(5.) Is the presence of a license plate number on a hot list, alone, sufficient to justify stopping a vehicle? After stopping a vehicle on the basis that it's license plate is on a hot list, should police officials have to verify that a license plate number is properly included on a hot list before taking any formal decisions regarding the vehicle or driver?

(6.) Although a location under the observation of an LPR remains fixed inside a local jurisdiction, many of the proposed purposes for collecting license plate data through the use of LPRs require the sharing of LPR data across jurisdictions. For example, in order to conduct an analysis of crime trends and series across jurisdictions may require submitting large quantities of historic LPR data to another agency or regional data repository. Alternatively, where another jurisdiction has already identified a vehicle of interest, it may be enough for a law enforcement agency to share the LPR data concerning that particular license plate number. How broadly will historic LPR data be shared across jurisdictions?

(7.) How will requests for LPR data be processed?

(8.) Will the originating agency impose any restrictions on the secondary dissemination of LPR data that it provides to other criminal justice agencies? If so, how will the originating agency ensure that those restrictions are followed?

B. SHARING LPR DATA WITH OTHER GOVERNMENT ENTITIES

Since the traditional sharing of investigatory information as a case progresses through the criminal justice system is already the subject of substantial amounts of case law and in some instance court supervision, this document does not address the subject. As a case progresses through the justice system, the LPR data is treated as any other type of evidence in the case. Thus, this document won't address the sharing of LPR data by a police department with a prosecutor's office.

One of the proposed purposes for the use of LPRs is to enforce geographic limitations on the movements of sex offenders, probationers and parolees, and people subject to orders of protection. This will require the exchange of license plate numbers, relevant geographic information, and actual observation data with agencies such as court clerks' offices, probation departments and departments of corrections.

Some individuals owe fees and fines to a variety of federal, state, and local governmental agencies. LPR technology can also be utilized as a tool to facilitate the collection of outstanding fees and fines owed to governmental entities.

(1.) For purposes of LPR data, are probation and corrections departments considered law enforcement agencies?

(2.) What types of LPR data will be shared with non-law enforcement agencies?

(3.) Under what circumstances should police officials share LPR data with non-law enforcement agencies?
(4.) What other government agencies are likely to request LPR data from a law enforcement agency and for what purposes?
(5.) Are probationers and those on parole or mandatory supervision required to provide a license plate number as a condition of supervision? Who may access such disclosures?
(6.) How does an individual who owes a governmental entity a fee or fine become associated with a license plate number?

C. PUBLIC ACCESS TO LPR DATA

A parallel can be made between the recordings of a license plate by an LPR to the recordings of a radio transponder used to electronically pay a toll. Individuals using radio transponders to pay tolls can frequently obtain a listing of the tolls they paid that includes the toll location, date, and time the vehicle passed the toll. This can be useful for monitoring the use of the transponder. In similar fashion, it is possible that agencies utilizing LPRs may receive requests for data as to the location, date, and time their license plate was recorded by an LPR.

LPR data, potentially including images of the vehicle and the driver, could be useful in line-ups, identifying vehicles involved in hit-and-run accidents, or seeking missing persons. In these and similar circumstances, law enforcement entities may want to affirmatively distribute LPR information to the public.

(1.) Every state has a freedom of information or "sunshine" law that provides the public with access to information maintained by government agencies. How will such requests for LPR data be handled? Are any statutory exemptions likely to permit an agency to withhold requested LPR data?
(2.) Will all LPR data be considered limited to criminal justice agencies or otherwise be considered law enforcement sensitive? Does categorizing LPR data as law enforcement sensitive provide any additional privacy protections to the public? Are there any potentially negative consequences to law enforcement of treating LPR data as law enforcement sensitive?
(3.) Under what public safety circumstances might a police agency seek to disseminate LPR data to the public?
(4.) How might LPR data be disseminated to the public? What methods of dissemination would likely be used?
(5.) Would LPR data be used in a photo array/line-up situation?
(6.) What criteria would be used to determine whether to disseminate LPR data about missing persons? Do certain factors related to age and competency of the missing person influence the public dissemination of LPR data?
(7.) Electronic data systems can create substantial quantities of statistical summary information. LPR systems can generate reports detailing, among

other things, the number of (a) license plates recorded by a certain camera during a requested time period, (b) times a certain license plate is recorded passing a particular camera, and (c) "hot list" license plates spotted versus the gross number of license plates recorded. Will LPR systems be designed to generate statistical summary information regarding their operations? What types of statistical summary information would be helpful in administering an LPR system?

(8.) Who may have access to statistical summary information generated by the LPR system?

D. ACCESS AND DISSEMINATION OF "HOT LIST" DATA

For purposes of clarity, this document separates LPR data from Hot List data. Section 3 (E) COMPILATION AND SUBMISSION OF "HOT LISTS" provides background information concerning the various types of hot lists likely to be utilized as part of an LPR system.

(1.) Are there any limits to the access and dissemination of hot lists? Can hearsay rules provide some guidance on the dissemination and secondary dissemination of hot list data?

(2.) How will requests for hot list data pursuant to a sunshine law be handled? Are any statutory exemptions likely to permit an agency to withhold requested hot list data? Are such exemptions permissive or must an agency withhold data if an exemption can be applied?

(3.) Are hot lists considered the "property" of the agency that compiles it? Does that ownership carry with it ultimate responsibility for the accuracy and completeness of the data contained in the list?

(4.) Is a local law enforcement agency's use of hot lists required by any statute or rule? Is the use of hot lists optional?

(5.) Who is entitled to see what license plate numbers are contained on a hot list?

(6.) What is the basis of any limitations on the public disclosure of hot list information? Are limits on such disclosure mandatory in nature?

(7.) Should there be limits placed on the types of hot lists that will be uploaded into an LPR system?

5. Retention

Although data retention periods were once necessitated by physical storage constraints, electronic storage of records has made the destruction of criminal justice information largely unnecessary. Thus, whether to retain LPR data indefinitely is a matter of policy that should take into consideration, among other things, the justice system's future need for the information as well as the public's reasonable expectations of privacy in the data. It may be important to note here that the Fair Information Practices call for the destruction of personal

information when it no longer serves its original processing purposes. Thus, destruction is included in the concept of retention.

(1.) Ultimately, we must determine how long LPR data should be retained. Alternatively, a set of standards could be developed that would assist local police departments in establishing their own retention periods. Which approach best suits the needs of agencies seeking to utilize LPRs?
(2.) Images collected by LPRs can be separated from the text-only data generated by OCR software. Should the image data be treated differently than the text-only data for purposes of establishing retention standards? If so, why, and how do those reasons impact the retention periods of the data?
(3.) What is the difference between a tactical use of LPR data and strategic uses? How do these different uses factor into establishing a reasonable retention period for LPR data?
(4.) How do state records retention acts and other laws created to aid in government oversight affect the determination of how long to retain LPR data?
(5.) What existing laws, regulations, or policies, if any, currently govern the retention and destruction of LPR data?
(6.) What does it mean to destroy LPR data?
(7.) Is LPR data the type of information that may become stale?
(8.) What factors might inform the establishment of data retention standards for LPR data?
    a. Statutes of limitation exist to encourage prompt investigations and prevent stale prosecutions. How do statutes of limitations impact the retention of LPR data that may be collected near a crime scene? Do statutes of limitation also impact the retention of LPR data not directly associated with a specific criminal event?
    b. Information collected as part of an investigation may have usefulness beyond the life of the case. Not only could information be part of a continuing series of acts (important for statute of limitations purposes), but information may be useful to generate leads for the investigation of subsequent crimes or for crime analysis purposes. Although LPR data may be used to conduct various forms of crime analysis discussed in Section 2(A) CRIME ANALYSIS above; there is also a strong undercurrent of pure surveillance to the utilization of LPRs. How do the potential uses of LPR data weigh in favor of or opposed to longer retention periods for LPR data?
    c. The quality of LPR data will likely weigh into any determination as to how long to retain license plate information collected by LPRs. It is submitted that information of a higher caliber and reliability and that is accurately attributed to the right individuals will weigh in favor of a longer retention period than information that is of lesser quality or from a less reliable source that is inaccurately complied.

d. The level of trust that the public has that the justice system will maintain the confidentiality of the data and use it appropriately is a substantial factor. The lower the level of trust, the higher the public's desire may be to destroy LPR data after a shorter time period.
e. Using information technologies to implement sound policy controls is one way to promote the public's confidence in the justice system's ability to keep sensitive information confidential and limit authorized users' misuse of the data. What technologically implemented policy controls are available concerning LPR data?
f. The social desirability of maintaining vast quantities of surveillance data on the travels of individuals via their license plates is also a key factor in the establishment of a retention period for LPR data.

(9.) Should retaining LPR data automatically include the ability to search the information with analytical tools, or could the LPR data just be stored for limited purposes (e.g., audit or subsequent verification)?

(10.) Is there going to be one centralized repository for retaining license plate data from multiple LPRs?

6. Accountability issues

Transparency surrounding how LPR data is managed, regardless of whether LPR data itself is available to the public, is important to promoting public confidence in an LPR program. Accountability issues arise throughout all stages of the LPR program, beginning with an agency's decision to utilize LPRs, continuing through the policy development stages, and finally to the implementation of those policies.

A. DECIDING TO USE LPRS

At some point an agency should formally decide whether to implement an LPRs program. Logistical and privacy issues should be discussed and a formal determination to procure and utilize LPRs should be documented.

(1.) Which entities ultimately approve the use of LPRs?

(2.) What deliberative process was utilized to determine whether to use LPRs in the jurisdiction?

(3.) Which entities will ultimately control the use of LPRs and the data they collect?

(4.) What are the potential misuses of LPR data and how can they be safeguarded against?

B. ACCOUNTABILITY DURING POLICY DEVELOPMENT

Although the privacy issues identified in this document are varied, they can all be addressed by holding the agencies utilizing LPRs accountable for securing the information they collect and how they subsequently use that information. Agencies should strive to provide sufficient oversight and transparency in the development and implementation of a privacy policy.

(1.) The stakeholders of any information system are usually those individuals whose information is being collected and those individuals who are using the information. Who are the stakeholders of an LPR program?
(2.) Will these stakeholders be contacted or approached to provide comments into the policy development processes?
(3.) Is there any reason to exclude certain stakeholder groups from the privacy policy development process?
(4.) Will there be a public comment period concerning a proposed data management or privacy policy for the LPR program? Will policy development meetings be open to the public?
(5.) Who will ultimately be responsible for the development of a policy governing the collection, access, use, dissemination, and retention of LPR data? Who will be responsible for the adoption of such a policy?

C. ACCOUNTABILITY PROVISIONS CONTAINED IN A PRIVACY POLICY

The Fair Information Practices, Section 1 (E) above, provide that a data controller should be accountable for complying with measures that give effect to privacy protections contained in its policies. There are several means of ensuring that agencies utilizing LPRs or the data collected by LPRs are complying with any applicable policies regarding their use.

(1.) Will LPRs systems utilize programmatic audit logs that document system notifications to users, user queries, and other entries into the LPR computer systems? What information should be contained in such a log?
(2.) Will the LPR system log maintain primary and secondary dissemination logs? How detailed do dissemination logs need to be?
(3.) Who will be responsible for monitoring use of LPR data and conducting audits of the use of LPR data?
(4.) Who will be responsible for investigating allegations that LPR data has been misused?
(5.) Are entities that receive LPR data going to be made subject to the terms of the privacy policy? Should entities that receive LPR data from an originating jurisdiction be required to identify an individual responsible for ensuring that the LPR data is properly managed?
(6.) Should individuals be able to challenge an agency's compliance with LPR policy provisions?
(7.) If individuals were permitted to allege misuse of LPR data or that an agency is otherwise failing to abide by LPR policies, how would such allegations be filed and how could frivolous challenges be avoided?
(8.) Do existing models for filing complaints about police service provide a sound framework for LPR complaints?
(9.) Are periodic compliance audits by an independent agency desirable? If so, what sorts of compliance issues should be audited? Should such audits

examine the LPR data itself as well as the appropriateness of the dissemination of the data?

(10.) What sort of penalties for non-compliance should be devised?

7. Data quality

Information quality is a multidimensional concept encompassing critical relationships among multiple attributes. For instance, the quality of a particular set of information can be expressed, among other ways, as the extent to which the data is: (a) available or easily and quickly retrievable; (b) appropriate for the task at hand; (c) regarded as true and credible; (d) easy to interpret and apply to different tasks; (e) correct and reliable; or (f) unbiased, unprejudiced, and impartial. Together, these attributes contribute to the validity of the information as it is used to make informed decisions. Good information quality is the cornerstone for sound decisions by justice practitioners and inspires trust in the justice system and in the agencies that use information.

Data quality concerns implicated by the operation of an LPR program will focus on the quality of the license plate data collected by the LPR cameras, as well as the quality of the information contributed to the system in the form of hot lists. The sharing of LPR data across jurisdictions is also likely to be affected by the quality of the system's information.

A. ACCURACY OF LPR COLLECTION OF LICENSE PLATE NUMBERS

(1.) Is there any human review of LPR data collection?

(2.) What is the accuracy of LPR cameras in their collection and recognition of license plate numbers? Is there an accuracy percent given by manufacturers (i.e. 98% of license plates are read with optical character recognition (OCR) accurately)? Is there an accuracy percent observed by individuals operating LPR cameras? Are these percentages comparable?

(3.) Several things may negatively affect LPR camera's ability to recognize a license plate, such the amount of contrast between a particular state's background and the color of the license plate's characters. Are there any known difficulties with LPR OCR software? For example, do LPRs have difficulty identifying certain novelty or out-of-state license plates?

(4.) What entity will be responsible ensuring the data collected by LPRs is of sound quality?

(5.) What entity will be responsible for identifying inaccuracies in LPR data and correcting them?

(6.) Regular and systematic audits are one way of ensuring that the quality of information used by justice practitioners remains high; there is considerable precedent for subjecting law enforcement information systems to data quality audits. Will LPR systems be subject to a routine audit requirement? What will be involved in implementing such a requirement?

(7.) Restricting the sharing of potentially inaccurate data is one way to limit the possibility that users in receipt of the information will act upon erroneous information. If the data collected by LPRs is of uncertain quality, will agencies restrict the sharing of their LPR data?

B. ACCURACY OF INFORMATION CONTAINED IN HOT LISTS

Many of the potential uses of LPR data depend in large part upon the quality of the hot lists that will be uploaded into police department computer systems. Little is publicly known about these hot lists and how they are compiled.

(1.) For what reasons are hot lists compiled?
(2.) Which hot lists concern officer safety and which do not?
(3.) Should hot lists that are officer safety related be treated differently than those that are not related to officer safety?
(4.) Because hot lists are compiled by different agencies, are there different rules governing access to the contents of each list? For example, is a hot list from a department of revenue containing license plates with outstanding parking tickets publicly disclosed while a hot list compiled by a police department containing sex offender license plates not?
(5.) Are there statistics concerning the accuracy of data contained in hot lists?
(6.) Is there any method for an individual to challenge their inclusion (or the inclusion of their vehicle's license plate number) on a hot list? If so, who provides this method, the list's authoring agency or the police department that is uploading the hot list into the LPR system?

C. PARTIAL LICENSE PLATES

There are several instances where witnesses are only able to provide partial license plates. As partial license plates are, by definition, incomplete, they create data quality concerns. Nevertheless, partial license plates serve important investigative purposes.

(1.) How do LPR systems handle notifications where partial license plate numbers are involved?
(2.) Should there be different policies concerning the entry of partial license plates onto hot lists or other notification lists?

D. RIGHTS TO ACCESS AND CHALLENGE LPR DATA

(1.) To what extent, if any, should individuals be afforded a right to review and challenge information about them or their license plates collected by an LPR? What factors would help to make this determination?
(2.) There would probably have to be a limitation on this right where it would interfere with a pending investigation.

(3.) Should the right to access and review, if granted, also include a listing of individuals and agencies to whom the information was previously disclosed?
(4.) If it were appropriate to grant individuals a right to access and challenge LPR data about them, what types of administrative procedures would need to be developed?
(5.) Could existing access and review provisions (e.g., those created for Criminal History Record Information) serve as a guide to access and review of other types of justice information? Should a provision be considered that is similar to the section of the Fair Credit Reporting Act that permits the subject of the information to append a narrative to the record that explains his version of it?

8. Intelligence issues

Intelligence analysis is a time consuming and labor-intensive process that focuses on organized crime such as narcotics smuggling, money laundering, gangs, terrorism, and auto theft rings.[13] Specifically, intelligence analysis is the study of criminal relationships and establishes links between known or suspected criminals and other suspected criminals or organizations.[14] It links suspects to criminal organizations or events to determine who is doing what with whom. This goal of intelligence analysis, to determine who is doing what with whom, does so by focusing on the relationships between persons and organizations. Surveillance information, including field observations and travel information collected by LPRs, about suspects and those associated with him are a key part of this type of crime analysis.[15]

There is concern about the government collecting information and creating dossiers about people in the absence of probable cause.

(1.) In what circumstances could LPR data be considered the type of surveillance data that may qualify as intelligence information?
(2.) Is intelligence data information collected on "bad guys" before they commit a crime or is it somehow related to information collected during the investigation of a crime that has already been committed?
(3.) How is intelligence information different from surveillance information? Is there a distinction?
(4.) Do the provisions of the Privacy Act and the Department of Justice's intelligence systems regulations sufficiently protect the privacy interests of individuals under the surveillance of LPRs? If not, what protections should be

[13] Gottlieb, supra note 3 at 27, 33.
[14] *Id.* at 27.
[15] *Id.* at 28-31.

included in a policy designed to regulate the sharing of LPR information across jurisdictions?

9. Security

Privacy and security, while related, are not the same thing. Although privacy cannot be maintained without security, security alone does not guarantee privacy interests are being respected. The goal of this document is to identify the privacy issues that should be addressed prior to an agency's implementation of an LPR program. As such, this document acknowledges that security is a component of ensuring the effectuation of privacy policies, but does not go into particulars regarding technological security safeguards such as user IDs, passwords, encryption, and firewalls, which are best left to IT professionals.

A:3

Appendix 3: List of Acronyms used in the PIA Report

DPPA	Driver's Privacy Protection Act, 18 U.S.C.A. §§ 2721-25
DMV	Department of Motor Vehicles
FOUO	For Official Use Only
GPS	Global Positioning System
IACP	International Association of Chiefs of Police
LEIM	Law Enforcement Information Management
LPR	License Plate Reader
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

A:4

Appendix 4: Footnote Reference List

[1] Most LPR systems capture multiple images of the same vehicle and then use the best image; other systems are capable of capturing more than one vehicle per second.

[2] Erika McCallister *et al., Guide to Protecting the Confidentiality of Personally Identifiable Information (Draft)*, Special Publication No. 800-122, 2-1 (U.S. Dept of Commerce, National Institute of Standards and Technology, Jan. 2009) (adopting the definition of PII contained in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*).

[3] *See Id.* at 2-2.

[4] *But see In re Charter Commc'ns*, 393 F.3d 771, 774 (8th Cir. 2005) (holding an IP address does not identify a user's name or mailing address); *Klimas v. Comcast Cable Comm'cns, Inc.*, 465 F.3d 271, 276 n.2 (6th Cir. 2006) (noting "that IP addresses do not in and of themselves reveal 'a subscriber's name, address, [or] social security number.' That information can only be gleaned if a list of subscribers is matched up with a list of their individual IP addresses."); *Johnson et al. v. Microsoft*, C06-0900RAJ Or. Granting Def.'s Mot. S.J. 7 (W.D. Wash. June 23, 2009) (ruling that "In order for 'personally identifiable information' to be personally identifiable, it must identify a person. But an IP address identifies a computer, and can do that only after matching the IP address to a list of a particular Internet service provider's subscribers.").

[5] On at least two occasions the U. S. Supreme Court has been confronted with whether an individual can be required to identify himself to the police during a Terry stop, but decided those cases on other grounds. *See Brown v. Texas*, 433 U.S. 47 (1979) (holding the underlying seizure illegal thereby avoiding the constitutional question) and *Kolender v. Lawson*, 461 U.S. 352 (1983) (holding a statute requiring a suspect to identify himself to police officers during a Terry stop void for vagueness and refusing to decide the issues of the constitutionality of compulsory identification). It wasn't until 2004 in *Hiibel v Sixth Judicial District Court of Nevada*, 542 U.S. 177, that the Court concluded that requiring suspects to identify themselves did not violate the Fourth or Fifth Amendments.

[6] The Act defines "personal information" as an "individual's photograph, social security number, driver identification number, name, address...telephone number, and medical or disability information"; the term does not include information on vehicular accidents, driving violations, and driver's status. 18 U.S.C. § 2725(3). In 2000, the Act was amended to create a new class of "highly restricted personal information." This includes an "individual's photograph or image, social security number, and medical or disability information" collected or maintained by a DMV. 18 U.S.C. § 2725(4).

[7] 18 U.S.C. § 2721(b)(1).

[8] 18 U.S.C. § 2721(b)(2).

[9] 18 U.S.C. § 2721(b)(4).

[10] The term For Official Use Only is used within the U.S. Department of Homeland Security to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. LPR data may also fall into the federal information categorization of non-classified information being implemented pursuant to Executive Order 12958; under that system of categorization, LPR data may also be considered Controlled Unclassified Information (CUI) and may more specifically fall under the CUI category "Controlled, Special Dissemination." *See* Executive Order 12958 as amended by Executive Order 13292 at 68 Fed. Reg. 15315 (2004); *see also* White House *Memorandum for the*

Heads of Executive Departments and Agencies: Designation and Sharing of Controlled Unclassified Information (CUI) (May 7, 2008) available on-line at: http://www.archives.gov/cui/documents/designation_cui.pdf.

[11] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490 (Jan. 2006).

[12] *Id.* at 493.

[13] One resident of a municipality considering the installation of LPRs who "[didn't] see too much harm in [LPRs]" admitted that a LPR system "still has the taint of Big Brother." Demian Bulwa, *Tiburon may install license plate cameras*, A-1 San Francisco Chronicle (July 10, 2009) http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/07/10/MNT6189U0U.DTL.

[14] As discussed in Part 4, LPR cameras can be fixed or mobile and can be deployed in an overt or covert manner.

[15] Solove, *supra* note 11 at 511.

[16] *Id.* at 514.

[17] *Id.* at 515.

[18] *Roberts v. United States Jaycees*, 468 U.S. 609, 617-618 (1984).

[19] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-343 (1995) (citing *Talley v. California*, 362 U.S. 60, 62 (1960) (internal quotations and footnotes omitted)).

[20] *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958). *See also Brown v. Socialist Workers' 74 Campaign Comm.*, 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations").

[21] Solove, *supra* note 11 at 521.

[22] *Id.*

[23] *Id.* at 522.

[24] *Id.*

[25] The DPPA implements these three suggestions and specifically makes it "unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted [by the Act]." 18 U.S.C. § 2722(a); *see also* text accompanying *supra* notes 6-9.

[26] Solove, *supra* note 11 at 507.

[27] *Id.* at 508.

[28] *See U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 764 (1989).

[29] *Id.* at 507.

[30] *Id.* at 508.

[31] *Id.* at 508-511.

[32] Moreover, there are no assurances that an inquiry into the license plate number will lead to the registered car, as in the case of stole license plates.

[33] *Id* at 527.

[34] *Id.*

[35] *Id.* at 531.

[36] Intl. Assn. of Chiefs of Police, *2007 Resolutions*, 51-52 (Oct. 16, 2007) available on-line at: http://www.iacp.org/resolution/2007Resolutions.pdf.

[37] Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria. 28 C.F.R. §23.3(b)(3).

[38] Technology is continually advancing. If LPR systems evolve to a level where they can read and compile data other than license plate numbers, the policy discussions contained in this Report will need to be supplemented.

[39] Steven Gottlieb, *et al.*, *Crime Analysis: From First Report to Final Arrest* 14-16 (Alpha 1994).

[40] *Id.*

[41] *Id.* at 133.

[42] *Id.* at 15.

[43] A crime pattern is merely a set of similar offences happening in a specific geographical area while a crime series is a crime pattern that appears to be done by either the same person or group of persons. Shawn A. Hutton & Mark Myrent, *Incident-Based Crime Analysis Manual* 34 (Ill. Crim. J. Info. Auth. 1999).

[44] Shawn A. Hutton & Mark Myrent, *Incident-Based Crime Analysis Manual* 7 (Ill. Crim. J. Info. Auth. 1999).

[45] Gottlieb, *supra* note 39 at 15 (stating that administrative analysis essentially includes the "nice to know stuff.").

[46] *Id.* at 128. Experienced analysts have found that the importance of each factor differs depending upon the type of crime being investigated. For example, suspect vehicle descriptors are more useful in determining whether a pattern of thefts from vehicles exists than a pattern of strong armed robberies. See *Id.* at 318-320.

[47] Spot maps can be of great assistance to the analyst. Nevertheless, spot maps will only depict crime patterns; additional information is necessary to determine if a crime pattern is also a crime series.

[48] *See* Jerry Ratcliffe, *Video Surveillance of Public Places*, 8-11 (U.S. Dept of Justice, Office of Community Oriented Policing Services Feb. 2006) (referring to closed-circuit television surveillance of public spaces).

[49] U.S. Dept. of Justice, *Recommended AMBER Alert Criteria*, (LT000498, Apr. 2005) available on-line at: http://www.ncjrs.gov/html/ojjdp/amberalert/PocketCard.pdf.

[50] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, Records, Computers and the Rights of Citizens: Report of The Secretary's Advisory Committee on Automated Personal Data Systems xx-xxi (1973) (hereafter "HEW Report"), available at http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[51] *Id.*

[52] NAT'L CRIM. JUST. ASS'N, Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems 22 (NCJA 2002) (hereafter "NCJA Guideline"), available at http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf

[53] Barbara Crutchfield George, *et al., U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 752 (2001).

[54] This is sometimes referred to as the *Openness Principle*, under which there should be a general policy of openness about developments, practices, and policies with respect to personal data. Under this principle, means should be readily available of establishing the existence and nature of personal data, and the main purposes of its use, as well as the identity and usual residence of the data controller. *See* NCJA Guideline *supra* note 53 at 31.

[55] *See* Part 4 of this Report; subsection (c) is intended to include law enforcement monitoring of certain identified individuals' compliance with travel restrictions and identification of previously-undetected crimes.

[56] Although not always the case, fixed LPRs frequently capture "transient vehicles" driving through a jurisdiction whereas mobile LPRs collect license plate data from local vehicles. Thus, fixed LPRs may further regional law enforcement goals whereas mobile LPRs may be of more value to local law enforcement agencies.

[57] Parking enforcement bureaus are not considered law enforcement in many jurisdictions.

[58] In many jurisdictions, parole and probation officers are peace officers with specific powers of arrest; in those instances, the sharing of information with such officers should be considered the sharing of LPR data among law enforcement agencies.

[59] Critical infrastructure is defined as those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. U.S. Dept. of Justice, *The National Criminal Intelligence Sharing Plan*, 13 (October 2003) (hereafter "NCISP") available on-line at http://www.it.ojp.gov/documents/NCISP_Plan.pdf.

[60] U.S. Dept. of Justice, *Fusion Center Guidelines—Developing and Sharing Information in a New Era*, 17 (August 2006) (hereafter "Fusion Center Guidelines") available on-line at http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

[61] *Id.* at 29.

[62] Although statistical summary information is unlikely to create privacy concerns, the sharing of LPR data related to a license plate number may raise privacy issues.

[63] LPR data may include images of vehicle occupants.

[64] Official criminal history record information is collected and maintained to compile crime statistics, assist a court in imposing an appropriate sentence, and to help corrections officials make prisoner placement decisions. Criminal history records are also maintained to implement sentence enhancement provisions for recidivists and are also used to ensure that civil disability and offender registration statutes are properly applied. *See* U.S. Dept. of Justice, *Use and Management of Criminal History Record Information: A Comprehensive Report*, 101-127 (NCJ 187670, Dec. 2001) available on-line at http://www.ojp.usdoj.gov/bjs/abstract/umchri01.htm.

[65] *See* 68 Fed. Reg. 14140 (2003).

[66] A threshold issue exists as to whether a contextual image taken by a LPR camera and the data associated with that image (including but not limited to the OCR text of the license plate and the date, time and location of observation) are considered records under the law of the jurisdiction.

[67] If so, those records may have different retention periods; specifically, the query-response record would likely be maintained for purposes of monitoring system use as opposed to supporting criminal investigations.

[68] Characteristics of crimes that may extend or toll a statute of limitations vary from state to state. Generally, statutes of limitations are extended in cases involving *inter alia* certain thefts involving a breach of fiduciary duty, identity theft offenses, and certain sex offenses; statutes of limitations are typically tolled *inter alia* when the defendant is not residing in the prosecuting jurisdiction or when a material witness is on active military duty.

[69] Such crimes typically include conspiracy and thefts by deception that continue over a period of time.

[70] The 9/11 Commission Report found that it took between two and four years to plan and carry out the attacks against the World Trade Center.

[71] Public confidence in a law enforcement agency's ability to maintain the confidentiality of LPR data could be reduced due to the scope of that jurisdiction's freedom of information act.

[72] U.S. Dept. of Justice, *Information Quality: The Foundation for Justice Decision Making*, 1 (Feb. 2008) available on-line at http://www.it.ojp.gov/documents/IQ_Fact_Sheet_Final.pdf.

[73] *Id.* at 2.

[74] Law enforcement agencies should not strip the image from the OCR information in order to save storage space; the OCR information cannot be verified without the contextual photo.

[75] Delaware and Rhode Island are able to use formats of 123456 and 123-456, respectively, while several populous states use seven-character formats, including 1ABC234 in California, AB1-C234 in Texas, A12-3456 in Illinois, and ABC-1234 in New York, Pennsylvania, Ohio, Georgia, North Carolina, Virginia, and Arizona.

[76] This is also common in the area of vanity license plates.

[77] Mandatory audits are routinely conducted of official criminal history record information (CHRI) repositories to measure the accuracy, completeness, and timeliness of their data. *See* 28 C.F.R. § 20.21(e). These audits are one of the reasons the justice system and society have deemed official CHRI records reliable enough on which to base important decisions affecting individuals' liberty interests.

[78] U.S. Dept. of Justice, Federal Bureau of Investigation, *National Crime Information Center Mandatory Minimum Standards Curriculum for Full Access Terminal Operations*, LPF-17; LPR-22 (1992) available on-line at: http://www.eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=ED354315&ERICExtSearch_SearchType_0=no&accno=ED354315.

[79] *See* 28 C.F.R. § 20.21(g)(1).

[80] *See* 28 C.F.R. § 20.3(d) (excluding investigative information from the definition of criminal history record information).

[81] See K. A. Taipale, *Technology, Security And Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123, 151 (2005).

[82] The DPPA contains a similar requirement; see 18 U.S.C. § 2721(c).

[83] Where LPR system policies are considered too detailed, law enforcement agencies may consider developing a guidance document to inform the public, in general terms, of practices and procedures developed to address privacy concerns surrounding LPR data.

International Association of Chiefs of Police
515 North Washington St.
Alexandria, VA 22310
1-800-THE-IACP
www.theIACP.org