September 2014
Privacy Impact Assessment
for the
Texas Department of Public Safety (DPS)
Collection, Storage, Management and Use
of Automated License Plate Reader Data

Contents

System Management

1. a. Which DPS Division is the system sponsor?

Law Enforcement Support Division

b. Who is the point of contact for the system sponsor?

Skylor Hearn
Assistant Director
Law Enforcement Support Division
Texas Department of Public Safety
5805 North Lamar
Austin, Texas 78765
Phone: (512) 424-7901

2. a. Which DPS Division is the system developer?

Information Technology Division

b. Who is the point of contact for the system developer?

Jon Percy
Assistant Director / CIO
Information Technology Division
Texas Department of Public Safety
5805 North Lamar
Austin, Texas 78765
Phone: (512) 424-7175

Introduction

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

Currently there is no statewide strategy for jurisdictions within Texas to share LPR data.

DPS can fill this LPR data sharing void and also provide leadership to Texas law enforcement in other LPR areas of concern including: hot list generation, deployment strategies, and development of usage policy.

Data Sharing

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 law enforcement 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.

Pooling LPR data from agencies from across the state can aid in the investigation of cold cases and in the identification of larger or more expansive crime trends. LPR data deconfliction can more readily occur - one jurisdiction that has already identified a vehicle of interest can more easily share the LPR data concerning that particular license plate number with a law enforcement agency from another jurisdiction.

Hot List Generation

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 comes from a variety of sources – some generated by DPS and some by local agencies. DPS currently provides hot lists to LPR users consisting of extracts from Texas Crime Information Center (TCIC - refreshed every hour) and National Crime Information Center (NCIC - refreshed every 12 hours) files. Building on that set of data, DPS could expand the hot list provided to Texas law enforcement agencies to include items such as AMBER Alerts and Department of Homeland Security watch lists. The role of DPS in creating a standardized hot list file format is important because it will allow local agencies to leverage that statewide standard to drive down costs when dealings with LPR vendors. Additionally, the centrally generated hot list allows local agencies to largely defer to DPS the maintenance of the supporting documentation regarding why a particular license plate number is on the hot list.

LPR Deployment Strategy

Local, state and federal agencies within Texas have deployed LPR solutions within their jurisdictions and it is unknown if consideration was given to potential overlaps or holes in the geographic areas covered by LPRs. DPS could serve to coordinate the deployment of LPRs in Texas so the devices fielded maximize coverage and deliver a larger benefit to the entire Texas law enforcement community.

Development of Usage Policies

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

uploaded onto the LPR system. Additionally, agencies should determine policies for retention of LPR data and the appropriate usage of historical LPR data. DPS leadership could help provide a sound basis upon which law enforcement agencies can build meaningful LPR system policies that respect individuals' privacy rights while providing authorized users with the information necessary to ensure the public's safety.

General Privacy Considerations

A. LICENSE PLATE NUMBERS AS PERSONALLY IDENTIFIABLE INFORMATION (PII)

Although license plates function primarily to uniquely identify automobiles, 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, 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?

DPS will not maintain PII data regarding the registered owner of a vehicle in the LPR database. DPS also does not maintain the registered owner data in any databases overseen by the Department. Registered owner data is maintained by the Texas Department of Motor Vehicles (DMV).

(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?

In Texas, law enforcement is not the only entity that can access registered vehicle owner PII. Access to registered vehicle owner data maintained by the DMV is restricted by Chapter 730 of the Texas Transportation Code. Because registered vehicle owner data is not maintained in the LPR database, law enforcement can only gain access to registered owner PII according to the provisions of the aforementioned law.

(3.) What anticipated uses of recorded license plate numbers involve accessing personally identifiable information about the vehicle's register owner?

The vehicle owner's PII data is not casually or directly available to users of the LPR database. If law enforcement activities dictate access to owner PII is necessary to support law enforcement work, it must be done so under the authority provided to law enforcement by Chapter 730 of the Texas Transportation Code and be limited to only those reasons approved for access. This does not constitute a policy or law change from how law enforcement would access the PII data for a manually captured license plate. Anticipated uses include, but are not limited to, the potential identification of witnesses and suspects of criminal activity as well as enabling the LPR data for exculpatory purposes.

(4.) What anticipated uses of recorded license plate numbers involve the mere monitoring or otherwise identifying a vehicle?

LPR data will be used to identify vehicles whose plates are actively sought or monitored by law enforcement. Law enforcement databases, such as NCIC, list law enforcement interests in the plate number for reasons such as it may be a felony vehicle, a stolen vehicle, or a vehicle associated with a person of interest.

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 the use of LPRs does not violate constitutional privacy protections, this does not mean the public's perceptions of the use of this technology are addressed; nor should the fact license plate numbers are publicly displayed end the inquiry. It is likely 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?

The Department does not feel there is risk in informing the public about the intended use of LPR technology. We wish to be totally transparent on this topic and assure the public the LPR data will not be used as a tool of social control.

(2.) One of the most important notions underlying the Fair Information Practices 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?

This PIA is primarily intended to govern the use of data provided to DPS from non-DPS LPRs. The Department cannot comment on signage associated with LPRs not owned by DPS.

The Department does not have any issue with providing notice to the public with regard to the general placement of DPS owned LPR equipment. DPS owned LPR cameras will primarily be deployed in support of commercial vehicle enforcement (CVE). While the main usage of the CVE LPRs will be commercial trucks, passenger vehicle data will also be captured as a consequence of capturing commercial vehicle traffic. Signage along roads where DPS CVE LPRs are in operation could provide adequate notification to motorists their license plate may be electronically read and recorded by fixed or mobile cameras. The Department would have some issue with providing detailed LPR location information because specific information could provide bad actors with the opportunity to steal, vandalize or destroy the equipment.

The Department would have issue with providing notice to the public in deploying mobile or portable equipment owned or loaned to DPS when used to support criminal investigations due to the potential to alert the criminals associated with the investigation.

(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?

Driving is a privilege in Texas as evidenced by state laws requiring drivers to have licenses and vehicles to be registered and inspected. State government is tasked with providing a safe environment for motorists to exercise their driving privilege. Part of providing that safe

environment is the need to enforce all state laws, including criminal laws as well as traffic laws. The capture of license plate information has long been a tool used by law enforcement to support highway safety. The object of law enforcement is not to surveil the public--it is to protect and serve the public. Used appropriately, LPR technology allows law enforcement to more efficiently and effectively enforce the law.

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 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, the information begins to paint a portrait of the individual's personality. It arises from the fact 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 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 the information.

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 a 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 information 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?

The Department plans to maintain limited data and that data will only be about the vehicle itself – not its owner. The owner of the vehicle still enjoys practical obscurity unless the vehicle is involved in the commission or suspected commission of a criminal act or if the vehicle has been identified as part of a public safety alert (AMBER, etc.). Only then is the vehicle owner data associated with the license plate of the vehicle read and recorded.

(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?

Law enforcement agencies collect LPR data to support law enforcement missions and goals. LE is also the steward of the data and will protect the data from being used in a manner inconsistent with the reason for its capture. Restriction of access to LE acquired LPR data helps ensure practical obscurity for the motoring public. Motorists will not have to worry a history of the movement of their vehicles will be available to advertisers, private investigators, debt collectors or anyone who has a financial, personal, or other interest in knowing the driving patterns. The release of this type of information to entities outside law enforcement could be a gold mine for bad actors looking for patterns in their potential victims' movements. Most importantly, Section 552.130 of the Texas Government excepts license plate data compiled by a governmental entity from the public information access provisions contained in Section 552.021 of the Texas Government Code.

(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?

The DPS LPR database will be a standalone database that could be used in conjunction with other databases. The LPR database will not have personal data about individuals, so any association of the vehicle data contained within the LPR database with a known individual would have to be made through an external source. The external source could make a connection between a certain license plate and a person of interest and then use the LPR database to track the movements of the vehicle associated with the individual who has committed or is suspected of committing a crime

(4.) Under what circumstances would the types of data identified in Issue 3 above be combined?

LPR pointer data may be loaded into investigative systems. In the event the LPR data is made available to law enforcement through these types of external portals, no registered owner data will accompany the license plate data.

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?

The Department does not consider the use of LPR technology to be surveillance – the LPR will not collect personal data. The data collected, while it can be later potentially linked to an individual to support a criminal investigation or humanitarian effort, does not contain PII data. Because the LPR technology only records the movement of a vehicle, the motoring public still enjoys practical obscurity and should not feel compelled to alter their behavior or feel inhibited in their vehicular movement.

(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?

Because the DPS LPR data will not contain PII data, it cannot be used in a way to control individual's movements or be used as a means to profile individuals. Additionally, the general location regarding the deployment of the LPR technology will be known to the public and LPR technology will not be used to capture and record vehicle data associated with political or religious gatherings.

(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?

The DPS LPR data will only be available for law enforcement usage. This includes criminal investigations and humanitarian purposes (assist with location of missing persons). Secondary use of the data by users of the LPR system will be prohibited in policy and enforced through formal user agreements and audits.

(4.) Aggregation is the gathering together of various pieces of information about a person. How will aggregation of LPR data impact the public?

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?

The DPS LPR database will be made available to law enforcement via the Texas Law Enforcement Telecommunications System (TLETS). As a conduit for criminal history record information, TLETS must meet technical security requirements articulated in the FBI's Criminal Justice Information Service (CJIS) security policy. The FBI audits DPS' compliance with that policy. Additionally, law enforcement connected to TLETS must ensure their systems are also compliant with the requirements contained in the CJIS security policy – DPS audits the compliance of the Texas law enforcement agency. In addition to security requirements, agencies accessing data from TLETS are required to conform to requirements associated with data use. Proper data use is defined in written policy and policy compliance is enforced through formal user agreements and audits.

(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?

LPR data will only be available to law enforcement to support the administration of criminal justice as defined in Article 60.01 of the Texas Code of Criminal Procedure and 28 CFR 20.3. Because PII data is not comingled with LPR data in the DPS LPR database, an individual cannot be impacted by disclosure of LPR data accessed in support of a criminal justice purpose unless that person has committed or is suspected of committing a crime, or is the subject of a humanitarian or exculpatory investigation.

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. 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?

Policy associated with prerequisites needed to access information regarding the identity of a vehicle's registered owner have been in existence for many years as law enforcement has demonstrated a need for this type of access long before the advent of LPR technology. Law enforcement access to vehicle owner data is governed by Chapter 730 of the Texas Transportation Code. Additionally, law enforcement will be provided policy documentation regarding access to the LPR data and audited on proper access and use of the data.

(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?

LPR technology allows for a 98% accuracy rate for the digital capture to optical character recognition and recording of the license plate number.

(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.

The data collected by LPRs is used in a two-fold process. The initial scan is run against a "hot list" to determine if the vehicle is an object of law enforcement interest. Most matches will require confirmation with the source of the hot list data prior to action being taken against the vehicle, but immediate law enforcement action may be taken against some hot list matches, such as vehicles identified in missing person alerts. The second part of the LPR data collection

is to preserve the captured plate information to assist future investigative, humanitarian or exculpatory efforts.

(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.

The DPS LPR database will not contain PII data, so PII data cannot be made readily available for disclosure. If linkage is made between the LPR data captured and data containing PII about the registered owner, it would only occur (a) with the consent of the data subject in the case of an exculpatory or humanitarian use; or (b) as authorized by Chapter 730 of the Texas Transportation Code. All linkage would take place outside the DPS LPR database.

(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.

Personal data will not be maintained in the LPR database. Any comingling of LPR data and PII data is done outside of the LPR database and in accordance to applicable policies and laws associated with access to the PII data. PII data regarding the register vehicle owner can be accessed by law enforcement via TLETS. TLETS is a secure law enforcement network and must adhere to the security requirements articulated in the FBI's CJIS security policy.

(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?

This PIA will be available to the public via the Texas DPS website.

(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, 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?

The individual participation principle does not apply in the case of the LPR database – no PII data is stored in the database. The PII data possibly associated with the LPR data is captured by the Texas Department of Motor Vehicles (DMV) through submission of identifying information provided by the vehicle owner at the time of vehicle registration. The Texas DMV has a process for registered vehicle owners to review and correct PII data associated with their registered vehicle.

(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 section 6 of this document.

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. Crime analysis is usually conducted on offenses with discernible patterns and trends that can be prevented or reduced through the implementation of directed action plans. A review of existing police crime analysis operations reveals burglary, robbery, auto theft, larceny, fraud, sex crimes, aggravated assaults, and murder are the crimes most appropriate for crime analysis.

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

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 governing body reports. 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 agency 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:

Geographic factors, time factors, victim descriptors, property loss descriptors, physical evidence descriptors, specific modus operandi factors, suspect descriptors, suspect vehicle descriptors

(1.) What presumptions are inherent in tactical crime analysis with regard to vehicles?

(a.) 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?

No. The registered owner may never actually drive the vehicle – it could be a spouse, child or another member of the house utilizes the vehicle, or a business owning multiple vehicles.

(b.) Is it presumed that an individual is always near the location where his automobile is parked?

No. It is only presumed an individual drove the car to or through the area where LPR cameras captured the license plate.

(c.) Is it presumed that an individual always parks near the location he intends to visit or reside?

No. It is only presumed an individual drove the car to or through the area where LPR cameras captured the license plate. It is presumed the driver will return to the vehicle at some point.

(d.) Is it presumed that a registered owner always knows the identity of who is driving his vehicle at any given time?

No. There may be multiple individuals other than the registered owner who have authorized access to a vehicle. There is no expectation the registered owner will always know which authorized user may have been driving the car at a specific date, time and location.

(e.) 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?

Presumptions used in the tactical crime analysis use of LPR data are vehicle-centric. The repeated appearance of a vehicle at times or places where crimes have been committed or are suspected of having been committed could lead law enforcement to seek information regarding the identity of the person who may have been operating the vehicle at those times or places. A nexus drawn between a vehicle and criminal activity would be the impetus to gather PII about the vehicle's registered owner in support of further law enforcement investigation.

(f.) 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?

While the LPR database will not contain PII data, external databases do contain linkages between a license plate and an individual's identity other than the registered owner. These external databases include, but are not limited to the sex offender registry and NCIC/TCIC "hot files" such as wanted persons, person of interest and felony vehicle file.

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?

At this time, the LPR hot file list produced by DPS contains data from the FBI's NCIC and Texas's TCIC files with associated license plate data. Current criteria for hot file entry is the license plate data must be for a vehicle for which law enforcement has an active interest and is already present in a law enforcement database.

(2.) Do these criteria include or consider the proper attribution of a license plate number to an individual?

The attribution of a license plate to an individual for records in the LPR hot file reflect the entry criteria associated to the source file (i.e. NCIC entry guidelines).

(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?

The license plate numbers in the DPS hot list reflect the vehicles of interest to law enforcement and are not proxies for an individual's PII. Any name or other personally identifying data in the hot list is strictly commentary and can be used to verify if the person operating the vehicle of interest may also be subject to criminal investigation.

(4.) How are partial license plates handled for hot list purposes? (This may be a data quality issue as well.)

Partial plates are not included in the Texas hotlist as the plate information is derived from NCIC/TCIC and follow the entry rules for those systems. Currently, the only time a partial plate can exist in the file is if the license plate number exceeds ten characters. In those cases only the first ten are entered. However, the entire number must be shown in the MIS Field. Partial license plates must not be entered.

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

Policy dictates when an LPR matches a record from the hot list, the agency receiving the match will conduct a real time search of the source file to determine if the reason for the alert is still valid. Any erroneous entries would be corrected in the source data file, which in turn updates the hot list. DPS updates TCIC derived hot lists every hour. The FBI NCIC derived hot lists are updated every 12 hours.

C. TRACKING INDIVIDUALS

Many of the justifications for LPRs include an element of tracking individuals. It has been suggested 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 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 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.

(a.) 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.)

The populations being described are generally required to provide law enforcement with information regarding the vehicles they regularly use. Because this information is self reported by the person in question, the match of the plate to the individual is highly reliable.

(b.) 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)?

The LPR is a force multiplier tool that will allow LE to more effectively track specific populations that use cars while freeing up additional resources to track individuals from the same population who do not use cars. The overall impact is not selective enforcement, but rather more efficient and effective enforcement because of ability to use LPR technology in place of human capital.

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

DPS does not believe the increased use of LPR will result in chilling effects because we strive to operate LPR in such a way as to preserve the motoring public's practical obscurity.

(d.) 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?

Information about an individual should not be casually accessed by law enforcement. The utilization of LPR does not change the protections currently in place that guard against the access to individual PII data. Policies and procedures are already in place to indicate when it is acceptable to access the location information of individuals.

(e.) 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?

The LPRs will be used to harvest location information for all populations. Geo-fencing activities will be conducted outside of the data harvesting procedures, with the geo-fencing working off hot list related constraints.

D. IDENTIFY PREVIOUSLY-UNDETECTED CRIMES

The American criminal justice system has never been based upon a theory of total enforcement of the criminal laws. Law enforcement agencies' 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 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 by permitting 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 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. Law enforcement agencies 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?

The data in the LPR database serves as tool to aid law enforcement in criminal investigations. Prior to taking adverse action against a suspect, investigators verify the information gathered during their investigations and determine if there is appropriate justification to go forward with determinations based upon the data at hand. The unsubstantiated existence of LPR data on its own is not enough for law enforcement to make a final determination about an individual; however, the LPR data can be used with other supporting information to assist LE with the furtherance of their investigations.

(2.) Given a police department's available resources, will certain crimes detectable by LPRs be focused on more so than others?

No crimes are detectable by LPR data alone. LPR technology and data will serve as a force multiplier, freeing up resources to be assigned to the investigation of other crimes whose detection cannot be aided through the use of LPR technology. Rather than focusing on LPR detectable crime, law enforcement can better fight all types of crime by leveraging the force multiplying aspect of LPR use.

(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?

LPR data can be a powerful tool in proving a previously reported violation. However, DPS feels LPR data matching against hot lists should be affirmatively reviewed and acted on in an

appropriate manner. Each LE agency using data from LPRs will ultimately be responsible for developing their own policies regarding the use of the data not matched against a hot list entry.

(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?

The DPS feels all LPR data should be considered when conducting trend analysis work. In support of a criminal investigation of cases limited to specific geographic areas, it may be appropriate to include only the LPR data from a particular area. This would not exclude the use of LPR data acquired in other areas if a nexus to a crime occurred in the other area.

(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?

At this time, DPS does not envision utilizing LPR to identify or associate "unlicensed drivers" with a specific vehicle.

(6.) It would seem that identifying vehicles potentially being operated by an unlicensed driver would be a real-time enforcement activity.

On the surface, detection of potentially unlicensed drivers would appear to be a real-time enforcement activity augmented by the user of LPR technology. However, multiple problems exist with regard to linking the unlicensed driver to a specific vehicle and such linkage would undermine the law enforcement presumptions inherent in the tactical crime analysis associated with license plate data.

E. REVENUE COLLECTION

Many states suspend or revoke license plates and driver 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 they generate the issuance of a ticket or citation. Rather, LPRs only help identify those who have already committed a violation or offense 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.

DPS does not envision utilizing LPR technology to facilitate revenue collection.

(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.

DPS does not envision utilizing LPR data to facilitate revenue collection. Access to PII data to augment LPR data will only occur to assist criminal investigations and to protect public safety.

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

As DPS does not envision utilizing LPR data to facilitate revenue collection, we also do not foresee transferring LPR data to non-law enforcement entities for revenue collection or any other non-law enforcement or public safety activity.

(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?

DPS does not envision utilizing LPR data to facilitate revenue collection.

(5.) Are there instances where a state 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?

While the department does not know of all state agency uses of LPR technology, we are aware the Texas Toll Road Authority utilizes LPR technology to collect toll fees from users who access toll roads, but do not have a "toll tag" for billing purposes. The existence of those LPRs does not impact the preparation of a law enforcement PIA because toll users are noticed of the presence of cameras and they choose to utilize the toll roads.

F. REGULATORY ENFORCEMENT

A) Commercial Vehicle Enforcement

The Texas Highway Patrol Commercial Vehicle Enforcement Service (CVE) will deploy LPR technology as part of commercial motor vehicle electronic screening systems designed to improve the safety of Texas roads by reducing large truck and bus accidents and accident related fatalities, injuries and property damage; while also reducing the impact of commercial vehicle enforcement on safe and legal motor carriers.

CVE roadside and administrative enforcement personnel will utilize LPR technology to identify commercial motor vehicle and motor carriers determined to be in violation of state and federal motor carrier safety and credential regulations by a variety of means including electronic vehicle screening technologies that include but are not limited to scale systems with capabilities to identify overweight vehicles and loads, laser systems with capabilities to measure and identify over sized vehicles and loads, thermal imaging technologies with capabilities to identify defective tires and braking systems, radiological sensors with capabilities to detect and localize airborne radiological sources, chemical sensors with capabilities to detect and identify specific hazardous materials, including explosives, from air samples; and biological sensors with capabilities to detect and measure specific biological organisms.

(1.) Will the LPR cameras used for CVE regulatory enforcement purposes capture different data from that which is captured for non-CVE purposes?

In addition to capturing images for the purposes of extracting license plate image data, other images may be captured and processed to extract data for the purposes of CVE regulatory enforcement, including:

- Container identification numbers may be extracted from side images of intermodal containers.
- Motor carrier identification numbers may be extracted from side images of truck tractor doors.

• The status of Commercial Vehicle Safety Alliance (CVSA) decals may be extracted from side images of truck tractors and trailers.
• The presence and type of hazardous materials may be extracted from side images of trucks and intermodal containers with hazardous materials placards.

(2.) Will the CVE LPR cameras capture additional data on motor vehicles other than commercial vehicles subject to regulatory enforcement purposes?
Non-commercial motor vehicles that pass by CVE LPR cameras will have their door panel images captured. If commercial license information, such as motor carrier identification numbers, Commercial Vehicle Safety Alliance (CVSA) decals, hazardous materials placards or intermodal container identification numbers, is not extracted from the door panel image, the image is not retained by the CVE LPR.

B) Vehicle Emission Program
The Regulatory Services Division (RSD) of the DPS is tasked with administering the vehicle inspection program for the State of Texas. The vehicle inspection program certifies vehicle inspectors and inspection stations, monitors and ensures compliance with inspection standards, and supervises vehicle emission programs designed to meet federal clean air requirements. As part of the duties associated with Vehicle Emissions Program (VEP), RSD remotely monitors the emissions of vehicles in seventeen (17) Texas counties classified by the Environmental Protection Agency (EPA) as being in non-attainment status are required to have an emissions test in addition to the safety inspection. RSD utilizes LPR technology to associate remote emission readings to the vehicle that is producing the emissions.

(1.) Will the LPR cameras used for VEP regulatory enforcement purposes capture different data from that which is captured for non-VEP purposes?
The VEP LPR cameras are used primarily to associate the emission reading to the vehicle that produced the captured emission. The VEP LPRs do not capture any additional data than non-VEP LPR deployments.

(2) Will the VEP LPR cameras be deployed statewide?
No. The VEP LPR cameras will only be deployed in the seventeen (17) Texas counties classified by the Environmental Protection Agency (EPA) as being in non-attainment status. The number of counties monitored can change if the EPA determines that more Texas counties are in non-attainment status.

C) Habitual Toll Violators
The DPS is assisting the North Texas Tollway Authority (NTTA) in deploying remedies to stop habitual toll violators who are driving on NTTA toll roads and not paying for their use of the toll road. Under Senate Bill 1792, a law passed by the 83rd Texas Legislature, toll enforcement remedies, including vehicle bans, are authorized for all habitual violators—those with 100 or more unpaid tolls and two notices of nonpayment within a one-year timeframe, who continue to drive on the NTTA System and ignore requests for payment. Fixed and transportable LPR cameras will be used to identify habitual users and enforce provisions of SB 1792. Habitual violators who operate a vehicle in violation of the ban and are stopped by law enforcement on an NTTA road may be issued a citation (Class C misdemeanor). A second or further violation of the ban may result in the impoundment of the violator's vehicle if found on the tollway.

(1.) Will the NTTA LPR cameras be used exclusively on the NTTA toll roads?
Yes. The NTTA LPR deployment will be restricted to the toll road under NTTA administration.

(2.) Will the NTTA habitual violator data be available to LE as a component of the LPR hot file?

No. Action against habitual violators can only take place on the toll roads administrated by the NTTA. Data associated with habitual violators is of no value to LE not responsible for enforcement on the NTTA regulated toll roads.

(3.) Will the NTTA LPRs capture data on non-habitual violators that utilize the NTTA toll roads?

The NTTA LPRs will capture data for all vehicles that pass the LPR cameras deployed on the NTTA toll roads. The data captured will be the same as is captured for non-NTTA LPR deployments.

LPR Data Collection and Management

A. LICENSE PLATES PROVIDE ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Although license plates do not 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 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 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.

Typically, LPRs are 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;

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

The DPS LPR data repository will collect the post OCR plate number, state of registration, GPS coordinates of where the plate was scanned, the Originating Agency Identifier (ORI) of the agency that captured the plate, the camera identification number, and the date / time of the plate capture. Additionally, the LPR database will allow contributors to provide a hyperlink to the repository maintaining the original captured digital image (if applicable).

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

The DPS LPR database will retain the minimum data needed to appropriately place the location of a vehicle over space and time and provide the information needed to determine what agency is able to place the vehicle. No PII or images will be retained by the LPR database. Through the retention of the basic "index" LPR data, DPS will be able to provide law enforcement with usable investigative data, while preserving the privacy of the motoring public.

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

The DPS LPR database itself will not contain PII data. While the LPR database will contain data that could potentially be linked to driver PII, access to the PII data is maintained in a different database and managed by a different agency and protected under the provisions of Chapter 730 of the Texas Transportation Code. Given the lack of PII data in the LPR database coupled with the protections afforded the link to PII data, potentially identifiably information will not directly affect the compilation, access, analysis or dissemination of LPR data.

(4.) 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?

The identity of a vehicle's registered owner should not be acquired unless the access provisions of Chapter 730 of the Texas Transportation Code have been met by the requestor.

(5.) 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?

The LPR database only contains vehicle data. Based solely on the data contained in the database, there is no way a determination can be made any of the drivers of the vehicles in the database are juveniles. The only time it could be determined a juvenile might have been driving a vehicle whose plate was contained in the LPR database is when the vehicle is involved in the commission or suspected commission of a crime or traffic accident. At that time, it is appropriate for law enforcement to have access to juvenile information to further the investigation of the crime in question.

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, whereas 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 or towed in a trailored configuration. Notifying the public about the collection of license plate numbers by LPRs will differ significantly depending upon the type of LPR deployed.

(1.) Do the three manners of LPR deployment change or otherwise impact the privacy concerns surrounding the collection of license plate numbers?

DPS feels the manner of collection does not impact privacy concerns.

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

Covert deployment could be necessary to aid in criminal investigations when law enforcement wishes to evade detection by the subjects of the covert operation.

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

Covert LPR deployments allow law enforcement to gather valuable investigative data without detection by the subjects of the covert operation.

C. NOTICE OF DATA COLLECTION

Not only do the Fair Information Practices counsel collecting only information relevant or necessary, but 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?

DPS will post this privacy impact assessment on the DPS public website.

(2.) Would distribution of the privacy policy itself provide sufficient notice?

DPS feels the public posting of this policy provides sufficient notice to the public.

(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?

PII data is not acquired at the time the LPR data is recorded, nor is it stored in the LPR database. Collection of PII data would occur outside the DPS LPR database.

(4.) Does the public know that the cameras they pass on roads are fixed LPRs by signage? By any other means?

DPS plans to make the public aware LPR technology is being deployed on Texas roadways. There are no plans to post signs indicating the specific location of fixed LPR cameras.

(5.) How can the public be notified about an agency's utilization of mobile LPRs?

The public will be made aware of the usage of LPR technology through press releases and publication of this PIA. The notifications will indicate the department will used fixed and mobile LPR cameras..

(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?

The DPS LPR database will only be available to law enforcement for law enforcement purposes. Any vehicle owner data obtained by law enforcement in support of a criminal investigation aided by LPR data is subject to the access requirements in Chapter 730 of the Texas Transportation Code. Chapter 730 does not require law enforcement to notice someone when their vehicle registration information data has been accessed.

D. "OWNERSHIP" OF LPR 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?

DPS will be stewards of the data contributed to the LPR database and will maintain the data in accordance with what is articulated in this PIA. However, the agency deploying the LPR is ultimately responsible for the operation of the LPR and the data collected by them. Roles and responsibilities regarding participation in the LPR database will be formalized in a user agreement.

(2.) What entity will ensure that data collected by LPRs is of sound quality?

The owning agency will ensure the data collected and submitted to the DPS LPR database is of sound quality.

(3.) What factors go into the determination of whether to share LPR data across jurisdictions?

The owning agency will have sole discretion with regard to the data they wish to promote to the DPS LPR database.

(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?

LPR data owners will enter into an agreement with DPS with regard to the subsequent uses and disseminations of the data. DPS will maintain the owning agency data in accordance with those user agreements, which will be based on the PIA. DPS will honor whatever retention time period the data owner wishes to be applied to their data and the owning agency will be able to remove their records from the LPR database at any time.

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 for 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?

LPR data owners will enter into an agreement with DPS with regard to the subsequent uses and disseminations of the data. DPS will maintain the owning agency data in accordance with those user agreements.

(2.) Should LPR data collected by a non-law enforcement agency be treated differently than LPR data collected by a law enforcement agency?

DPS will treat all LPR data in the same manner, regardless of the capture source.

(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?

DPS has no plans to sell LPR data. DPS does not own all of the data that will reside in the LPR database and would not sell the LPR data the DPS LPR equipment contributed to the file.

(4.) Would selling the data call into question an agencies' position that the data should be treated as confidential?

The majority of the data in the DPS LPR database will be not be owned by DPS; therefore, we will not sell the data.

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 an individual somehow associated with the vehicle is nearby so 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?

DPS currently provides hot lists to LPR users consisting of extracts from TCIC (refreshed every hour) and NCIC (refreshed every 12 hours) files. Building on that set of data, DPS could look to expand the hot list provided to Texas law enforcement agencies to include items such as AMBER Alerts and Department of Homeland Security watch lists. DPS cannot presume what other law enforcement agencies are 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?

The hot lists constructed by DPS are based upon existing law enforcement files (TCIC/NCIC). The entry criteria for these files are published by the FBI in the NCIC operating manual. Agencies contributing to these files are audited on a regular basis to ensure compliance with the entry criterion. Additionally, the source files require entering agencies to validate the information contained in these files on a regular basis.

(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?

For DPS hot lists, individuals are linked to license plates through the database from which the hot lists are extracted. These databases have entry criteria for these files geared toward accurately associating a license plate to an individual if such a linkage exists.

(4.) Are the links between license plates and individuals verified or updated on a regular basis?

The NCIC/TCIC files from which the hot lists are derived require entering agencies to review and validate the information contained in these files on a regular basis – this includes any linkage between a person and a license plate.

(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?

There are potentially greater privacy concerns regarding hot lists generated by law enforcement than those generated by non-law enforcement governmental agencies due to the type of data that may appear in the files. Information relating to vehicles in association with wanted persons is harvested from the NCIC/TCIC Wanted Person File. Vehicle information is also contained in the following NCIC files: Protection Order, Missing Person, Gang, Known and appropriately

Suspected Terrorists (KST), Supervised Release, Convicted Sexual Offender Registry, and the Immigration Violator.

(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?

DPS cautions agencies that the match of a vehicle against a hot file listing is not, on its own, justification to take action against the vehicle. User agreements with the users of the DPS hot lists instruct the agency to verify the hot list match with a real-time query to the database that was the source of the match and further directs the agency to take the appropriate confirmation steps prior to taking adverse action against the vehicle.

(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?

If the driver of the vehicle is found to be the true subject of interest associated with the vehicle's license plate, the driver will be made abundantly aware (through arrest or citation) of why the vehicle was added to the hot list file. If the driver is not the subject of interest associated with the vehicle's license plate, an officer may disclose the reason for the stop as long as the dissemination does not compromise the law enforcement value of the data.

LPR Data Access and Dissemination

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 help reveal relationships among persons, places, vehicles, and activities not 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.) 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"?

DPS believes there is a distinction between LPR data access for the purpose of notification and for the purpose of historical queries. The difference between the two access uses is important to understand because it drives how the data is used. The notification usage is prospective – the hot list provides law enforcement with license data associated with vehicles that are the subject of law enforcement interest to be compared against LPR captures as the captures occur. The hot list data is derived from external databases and is not stored in the LPR database.

The historical LPR data use is retrospective – agencies with a legitimate law enforcement need to find a specific vehicle can query the LPR database to find data relating to where the vehicle may have been in the past. The geo-spatial location of the vehicle can provide law enforcement with information to further their criminal investigations.

(2.) 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)?

Access to the DPS LPR database will require the inquiring agency to indicate the purpose for which the search is being requested – i.e. criminal justice purpose. DPS will log all access requests and use the log information as a means to audit an agency's appropriate use of access to the LPR data.

(3.) 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?

The historical LPR data will enable various forms of crime analysis; for example, DPS will be able to trace the movements of felony vehicles over time (in hindsight) that travel specific routes from the border on a regular basis and help determine patterned movements associated with drugs / money / human trafficking. This type of data will be useful to inform deployment of personnel to interdict this type of traffic. The results of this type of crime analytics would be made available to the law enforcement community.

(4.) 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?

DPS cautions agencies that the match of a vehicle against a hot file listing is not, on its own, justification to take action against the vehicle. User agreements with the users of the DPS hot lists instruct the agency to verify the hot list match with a real-time query to the database that was the source of the match and further directs the agency to take the appropriate confirmation steps prior to taking adverse action against the vehicle.

(5.) 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?

The DPS plans to house historical LPR data from Texas law enforcement from across the state. It is important to keep in mind the LPR database will only contain "index" data about a license plate captured by LPR. The more robust, detailed data will remain with the jurisdiction that captured the information.

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

Law enforcement agencies wishing to query the DPS LPR database will launch the request in a pre-defined query format through the Texas Law Enforcement Communication System (TLETS).

(7.) 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?

The data contained in the DPS LPR database is strictly "index" information – detail information about the capture is maintained by the owning capture agency. The requesting agency will have to reach out to the owning agency to obtain additional information and it is up to the owning agency to allow access and set conditions for the disseminate of the information to the requestor.

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?

DPS considers probation and corrections to be criminal justice agencies which would be entitled to access to LPR data.

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

DPS does not envision routinely sharing LPR data with non-criminal justice agencies. The data shared would be related to the purpose of the dissemination.

(3.) Under what circumstances should police officials share LPR data with non-criminal justice agencies?

DPS does not envision releasing LPR data to non-criminal justice agencies on a routine basis. Release would be considered on a case by case basis in order to support exigent circumstances such as locating a missing person or accounting for vehicles during an evacuation.

(4.) What other non-criminal justice government agencies are likely to request LPR data and for what purposes?

Not knowing other agency interest in LPR data, it is hard to predict which, if any, governmental agencies are likely to request access to LPR data.

(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?

The NCIC "Supervised Release" file allows for the entry of license plate information for individuals on supervised release. Plate information from the Supervised Release file is contained in the LPR hot list, but is not maintained in the DPS LPR database. Access to the Supervised Release file is available through TLETS to authorized Texas criminal justice agencies.

(6.) How does an individual who owes a governmental entity a fee or fine become associated with a license plate number?

The DPS does not envision using the LPR data to assist with the collection of fees. However, linkage between fines and a license plate could be easily made in the cases of parking tickets, toll fees, and uninsured vehicles.

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 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?

The responsiveness of the request will be tied to the type of data requested. LPR hot lists do not contain PII data and thus could be exposed to the public. However, some hot list data would need to be redacted because its release could compromise a criminal investigation or national security. The legacy LPR data contained in the DPS LPR database will be governed through the user agreements executed with the owners of the LPR data. The user agreements indicate legacy data remains the property of the contributing entity and DPS can only disseminate the data to criminal justice agencies for criminal justice purposes. Request for data from the LPR database should be made to the owners of the LPR data.

The Texas Attorney General has consistently ruled information relating to a motor vehicle title or registration issued by a state agency or country, including license plate numbers, is excepted from public release under section 552.130 of the Texas Government Code. These rulings directed government agencies to withhold license plate number information from release to the public, while section 730.007 of the Texas Transportation Code provides for certain permitted disclosures of this type of information, such as disclosure by a law enforcement agency in carrying out its functions.

(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?

The legacy LPR data contained within the DPS LPR database should be considered law enforcement / criminal justice sensitive. The intention of the data collection is to support the administration of criminal justice. Bulk release of the data could impact the privacy of the motoring public as the data could be used for non-criminal justice purposes such as advertising or surveillance by private investigators.

(3.) Under what public safety circumstances might a police agency seek to disseminate LPR data to the public?

The DPS LPR database will have very little data useful to the public. One use may be the release of the last recorded location for a vehicle associated with a missing or wanted person.

(4.) How might LPR data be disseminated to the public? What methods of dissemination would likely be used?

During those few circumstances when it would be useful to disseminate LPR data to the public, DPS envisions releasing the data through our Media and Communications Office in the form of a public service announcement in support of finding a missing or wanted person.

(5.) Would LPR data be used in a photo array/line-up situation?

The DPS LPR database will not contain images; hence LPR photo line-ups will not be a system feature.

(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?

The release of the LPR data would have to materially contribute to the effort of trying to locate the missing person. The age of the person would not impact the public dissemination of the data. The decision to disseminate would be based on the ability to link the missing person to a specific vehicle – regardless of if the missing person was purported to be the driver.

(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?

The DPS LPR database will be an aggregation of data captured by local agencies and will not be able to generate minutia level reports. Statistics available would include the number of records submitted by agency and overall number of records in the file. Hot list hit reports would have to be generated by agencies that actually use the hot lists in conjunction with their LPR deployment.

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

DPS believes the volume statistic for the DPS LPR database would be public information unless the disclosure of the information is determined to interfere with the detection, investigation or prosecution of crime.

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?

The limits on the access and dissemination of hot lists generated by the DPS are governed by a user agreement executed between DPS and authorized criminal justice agencies.

(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?

The hot lists themselves are excepted from public disclosure under Texas Government Code 552.130. Even if the DPS LPR hot lists could be released to the public, they would be of little use without access to the databases from which the lists are derived. For example, the hot list data is derived from the FBI's NCIC and Texas' TCIC which contain license plate information from the Vehicle, License Plate, Wanted Person, Protection Order, Missing Person, Gang, Known or Appropriately Suspected Terrorist (KST), Supervised Release, Convicted Sexual Offender Registry, and the Immigration Violator Files, but PII is not provided within the hot list data itself. Authorized criminal justice users will be able to access the source databases to

acquire any PII data associated with plate information contained in the hot lists. The general public would not have access to those source databases, resulting in the hot file listing being nothing more than a list of license plates of interest to law enforcement.

(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?

Because the DPS hot lists are generated from CJIS systems, the hot lists themselves fall under the stewardship of the department in its role as the FBI's CJIS System Agency (CSA). The accuracy and completeness of the data is tied to the systems from which the data is derived. DPS updates these hot lists on a regular basis – DPS TCIC data is updated every hour, FBI NCIC data is updated every 12 hours. Agencies choosing to utilize the DPS hot lists are required to update their local LPR hot lists as the updates become available, ensuring the information deleted from the source databases are also deleted from all local hotlists. The agreement also requires users to confirm hits derived from the hot lists are still active in TCIC/NCIC, at the earliest reasonable opportunity, in accordance with current hit confirmation policy.

(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?

The use of the DPS provided hot list is not required and is totally at the discretion of the local agency.

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

The public would be able to see the plates contained on the hot list not redacted for investigation or security reasons.

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

Some data from the hot list may be subject to redaction because its mere presence on a publically available list could compromise a criminal investigation.

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

DPS will control and limit any hot list data used on LPRs operated by the department. Local agencies will enjoy the same autonomy with regard to what hot lists are utilized by LPRs deployed in their respective jurisdiction.

LPR Data 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 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.) Data collected in a centralized LPR database can be logically separated based on the source of the data. Should the data be treated differently based upon the source for purposes of establishing retention standards?

The data contained in the DPS LPR database belongs to the agency that contributed the data to the database. The DPS has designed the LPR database to be able to honor any retention / destruction schedule desired by the contributing entity – hence retention lengths in the DPS LPR database may be different depending on the wishes of the contributing entity. If a contributing entity does not put a limit on the length of time the DPS LPR database may retain their data, the retention period will default to 3 years. DPS plans to retain data acquired by DPS operated LPR devices for 3 years. The 3 year retention schedule will be periodically reviewed to determine if it meets the needs of law enforcement. Based upon the review, the schedule may be lengthened or shortened. Any changes to the length of retention will be published in an updated privacy impact assessment.

(2.) 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?

Tactical use of LPR data will enable the detection of crime patterns and series by studying and linking common elements of crimes in order to predict when and where future events will occur. The strategic use of LPR data would concentrate on long-term crime trends and would be used to project where law enforcement presence should be increased or decreased.

Because the legacy LPR data is needed to support both types of analysis, the data requirements associated with developing usable models factors into the decision of how long to retain the legacy LPR data.

(3.) 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?

The Texas State Library requires state agencies to adhere to the retention period for data according to specific retention schedules. The retention schedule for DPS generated LPR data is 3 years.

(4.) What does it mean to destroy LPR data?

LPR hot list data is continuously refreshed on a daily basis. Old versions of the LPR hot lists are not retained as the list is kept current according to the source. Legacy LPR data retained in the DPS LPR database subject to destruction due to expiration of retention timeframe or the wishes of the contributing agency is deleted from the database and is not stored or accessible after it is deleted.

(5.) Is LPR data the type of information that may become stale?

LPR hot list can become stale. For this reason, hot lists derived from TCIC data are refreshed every hour and NCIC derived hot list data is refreshed every 12 hours. Legacy LPR data does not become stale because it is a geo-spatial historical chronology of a vehicle's movement.

(6.) 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?

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. Because of these issues, statutes of limitation concerns are not applicable to LPR retention periods.

b. 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.

All LPRs used by DPS will be maintained in accordance with manufacturer recommendations. Users of DPS LPRs will be trained to assure the proficiency of the operators with the LPR. The contributor agreement DPS exercises with the local agencies will require them to properly train the LPR operators and to maintain the equipment in accordance with manufacturer recommendations.

LPR Data Accountability issues

A. ACCOUNTABILITY OF DATA SHARING SYSTEM

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 the 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?

The stakeholders for the DPS LPR database are the members of the criminal justice community. The Texas criminal justice community has deployed LPRs around the state of Texas and is capturing the license plates of vehicles within their jurisdictions. The data from these plate captures will be forwarded to the DPS LPR database, where they will be exposed to queries by other members of the Texas criminal justice community. The query aspect of the system will be open to all authorized criminal justice practitioners, regardless of whether they contribute to the file.

(2.) Will these stakeholders be contacted or approached to provide comments into the policy development processes?

These stakeholders will not be able to participate in the system unless they agree to be bound by the provision articulated within this privacy impact assessment. Because there is no state requirement for local criminal justice to use the DPS LPR system, the DPS will welcome comments to the policy development process so we can address any concerns that may prevent a stakeholder from participating in this program.

(3.) Is there any reason to exclude certain stakeholder groups from the privacy policy development process?

DPS welcomes comments from all stakeholder groups.

(4.) 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?

As the owner of the DPS LPR database, the DPS will ultimately be responsible for the development of policy surrounding the data within the LPR database. The policy will include direction on the submission, access, use, dissemination and retention of the data within the DPS LPR database. The data owners will be responsible for the development, implementation, and enforcement of policies related to their systems and data.

B. ACCOUNTABILITY PROVISIONS CONTAINED IN A PRIVACY POLICY

The Fair Information Practices, Section 1 (E) above, provide 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 agencies utilizing LPRs or the data collected by LPRs are complying with any applicable policies regarding their use.

(1.) Will LPR 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?

The DPS LPR database will log query request made against the LPR data by criminal justice agencies. The logs will contain sufficient data to determine who made the query, when the query was made and the purported purpose of the query.

(2.) Will the LPR system log maintain primary and secondary dissemination logs? How detailed do dissemination logs need to be?

The DPS LPR system will only log primary disseminations. It will be the duty of the original inquirer to log any secondary dissemination of the data received from the DPS LPR database.

(3.) Who will be responsible for monitoring use of LPR data and conducting audits of the use of LPR data?

The DPS will audit local criminal justice agency usage of the DPS LPR system as a part of the current triennial audit of criminal justice agencies which access CJIS systems through the DPS.

(4.) Who will be responsible for investigating allegations that LPR data has been misused?

DPS will be responsible for investigating allegation of misuse of the DPS LPR system. The DPS already has a methodology in place to investigate potential misuse of any CJIS system when the potential misuse is reported. DPS will leverage the existing investigative process to investigate reports of LPR misuse.

(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?

The DPS LPR data will be made available through the Texas Law Enforcement Telecommunications System (TLETS). Entities with authorized access to TLETS must agree to be bound by the privacy protection policies associated with the data they access. Currently, all agencies using TLETS must identify a Terminal Agency Coordinator (TAC) who is responsible for ensuring all users from their agency have access to the required training and policy documents associated with the data they seek to access.

(6.) Should individuals be able to challenge an agency's compliance with LPR policy provisions?

Individuals concerned about a specific agency's adherence with the DPS LPR access policy provisions are able to report the agency's alleged non-compliance to DPS for subsequent investigation.

(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?

Individuals are able to send allegations of LPR data misuse to the department in writing via the US Mail or to the DPS email system. This PIA will be on the DPS website, so potentially frivolous challenges can be avoided because the complainant will know what data is maintained in the LPR database as well as what data will be retained from each query made by an authorized agency. It is hoped this information would help a potential complainant determine if their complaint is justified and verifiable prior to making an allegation.

(8.) Do existing models for filing complaints about police service provide a sound framework for LPR complaints?

The existing model for complaints about TLETS related system misuse is appropriate for adjudicating allegations of LPR misuse.

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

Agencies found to be non-compliant with TLETS related access policy are subject to sanction, up to and including termination of access.

LPR 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.) What is the accuracy of LPR cameras in their collection and recognition of license plate numbers?

The industry standard given by manufacturers is 98% of license plates are accurately read with optical character recognition (OCR). This percentage assumes the plate is not damaged nor does it have an object blocking a clear view of the plate (i.e. trailer hitch).

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

DPS can only control the quality process for DPS deployed equipment. However, DPS will publish best practices for the contributing entity to adopt if they wish to use them.

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

The entity capturing the data will be responsible for identifying and correcting inaccuracies in LPR data they contribute to the DPS LPR database. DPS will provide the contributors with a methodology to facilitate these types of corrections.

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 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?

Hot lists are compiled to provide LPR operators with an offline list of plates of interest to law enforcement. LPR systems compare the license plate data acquired by the LPR camera with hot list data to quickly determine if further action should be taken with regard to the vehicle bearing the matched plate.

(2.) Which hot lists concern officer safety and which do not?

The hot lists prepared by DPS are only differentiated by source – either FBI data or Texas DPS data. The data in both files is derived from databases that contain criminal justice information, some of which concerns officer safety.

(3.) Are there statistics concerning the accuracy of data contained in hot lists?

There are no statistics associated with the accuracy of the data contained in the hot files provided by DPS. However, the data in the DPS hot lists are derived from databases with strict entry criteria and whose records are subject to regular periodic validation by the agency providing the data to the source database.

(4.) 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?

Because the data contained in the DPS provided hot files is derived from either TCIC or NCIC entries made by a specific agency, challenges should be addressed to the agency that entered the plate information into the system of record. Any changes to the records will be updated when the hot lists are refreshed. The TCIC-based hot list is refreshed every hour while the NCIC-based list is refreshed every 12 hours.

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?

Partial plates are not included in the Texas hotlist as the plate information is derived from NCIC/TCIC and follow the entry rules for those systems.

(2.) Should there be different policies concerning the entry of partial license plates onto hot lists or other notification lists?

There are no policy issues surrounding partial plates for DPS provided hot lists. Currently, the only time a partial plate can exist in the source NCIC/TCIC file is if the license plate number exceeds ten characters. In those cases only the first ten are entered. However, the entire number must be shown in the MIS Field. System rules dictate partial license plates must not be entered.

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?

The data contained within the DPS LPR database is promoted to the database by the agency that captured the plate. Any challenges regarding the limited plate data contained in the DPS LPR should be addressed to the agency that captured the data.

(2.) 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?

The DPS LPR database will only contain data about the capture of a specific plate on a specific date and at a specific time. Because only the presence of a public capture of a license plate with no associated PII data is in the file, it is not appropriate to grant individuals a right of access to the LPR data. Without accessing registered vehicle owner data, it would be impossible for criminal justice agencies to determine if a person who sought access had any right to access data about a plate in question.

Use of LPR Information for Criminal Intelligence

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. Specifically, intelligence analysis is the study of criminal relationships and establishes links between known or suspected criminals and other suspected criminals or organizations. 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. 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?

The DPS LPR capture data cannot be construed to be intelligence data. The data is contained in the database is incident data. The data reflects information detailing a vehicle bearing a specific license plate was seen at a specific location at a specific time. The data is collected on all vehicles that pass by the LPR equipment and no specific populations are surveiled unless as a part of a covert criminal investigation.

(2.) Is 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?

Covert capture of LPR data is conducted in support of a criminal investigation of vehicles involved in the commission or suspected commission of a crime. Non-covert capture of LPR data is not targeted to a specific population and provides criminal justice entities with real-time notifications of matches against a hot list of vehicles for which criminal justice agencies have an active interest. LPR captures that do not result in a match provide criminal justice agencies with a geo-spatial chronology of a vehicles past movements without associating the vehicle with an identifiable person. This historical data can be used to assist with future criminal justice purposes.

LPR Data 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 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.

However, the security used to protect the LPR system data and access must meet the requirements articulated in the FBI's CJIS security policy.

A current copy of the CJIS security policy can be found at http://www.txdps.state.tx.us/SecurityReview/index.htm