2016

License Plate Reader Technology: Transportation Uses and Privacy Risks

Johanna Zmud

Jason Wagner

Maarit Moran

James P. George
Texas A&M University School of Law, pgeorge@law.tamu.edu

NCHRP 08-36, Task 136

License Plate Reader Technology: Transportation Uses and Privacy Risks

Requested by:

American Association of State Highway and Transportation Officials (AASHTO)
Standing Committee on Planning

Prepared by:

Johanna Zmud
Jason Wagner
Maarit Moran
Texas A&M Transportation Institute
James P. George, Texas A&M School of Law

The Texas A&M University System
College Station, Texas

November 2016

The information contained in this report was prepared as part of NCHRP Project 08-36, Task 136, National Cooperative Highway Research Program (NCHRP).

AASHTO
THE VOICE OF TRANSPORTATION

ACKNOWLEDGMENT

This study was conducted for the AASHTO Standing Committee on Planning, with funding provided through the National Cooperative Highway Research Program (NCHRP) Project 08-36, Research for the AASHTO Standing Committee on Planning. The NCHRP is supported by annual voluntary contributions from the state Departments of Transportation. Project 08-36 is intended to fund quick response studies on behalf of the Standing Committee on Planning. The report was prepared by Johanna Zmud, Jason Wagner, Maarit Moran, and James P. George. The project was managed by Lawrence D. Goldstein, NCHRP Senior Program Officer.

CONTENTS

LIST OF FIGURES AND TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
ALPR	automated license plate reader
AVST	audio video surveillance technology
CVISN	Commercial Vehicle Information Systems and Networks
DMV	Department of Motor Vehicles
DOT	Department of Transportation
DSRC	dedicated short range communications
FDOT	Florida Department of Transportation
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FTC	Federal Trade Commission
GIS	geographic information system
GPS	global positioning systems
HOT	high occupancy toll
HOV	High occupancy vehicle
IACP	International Association of Chiefs of Police
ISMS	information security management system
ISO	International Organization for Standardization
ITS	intelligent transportation systems
LPR	License plate reader
MAC	Media Access Control
MPO	Metropolitan planning organization
NCHRP	National Cooperative Highway Research Program
NIST	National Institute of Standards and Technology
OCR	optical character recognition
OECD	Organization for Economic Co-operation and Development
PARSS	Performance Registration Information Systems and Management based automated ramp screening system
PCI	Payment Card Industry
PII	personally identifiable information
RFID	radio frequency identification
SCC	Security Standards Council
TxDOT	Texas Department of Transportation
USDOT	United States Department of Transportation
VMT	vehicle miles traveled
WIM	weigh-in-motion

ACKNOWLEDGMENTS

The research reported herein was performed under NCHRP Project 08-36, Task 136 by the Texas A&M Transportation Institute (TTI), a member of The Texas A&M University System. Johanna Zmud of TTI was the Principal Investigator. Co-investigators were Jason Wagner and Maarit Moran of TTI; James P. George of the Texas A&M School of Law. Other members of the research team were Shawn Turner of TTI; and Michalis Xyntarakis and Anita Vandervalk of Cambridge Systematics.

The researchers would like to thank the following individuals for their assistance in the case studies and participation in interviews:

- J.D. Allen, Alliance Transportation Group
- Paul Clark, Florida Department of Transportation
- Jeff Davis, Port of Houston
- Stephen Davis, Port of Beaumont
- Anthony Guckert, The Traffic Group
- Dean Gustafson, Virginia Department of Transportation
- Dell Hamilton, Texas A&M Transportation Services
- Ed Hard, Texas A&M Transportation Institute
- Allison Hardt, Maryland State Highway Administration
- Eric Hemphill, North Texas Tollway Authority
- Fred Herrey, Florida Department of Transportation
- Steve Jack, Virginia Department of Transportation
- Stave Kalina, Arizona Department of Transportation
- Brian Kary, Minnesota Department of Transportation
- Tom Kelly, Federal Motor Carrier Safety Administration
- Casey Langford, Tennessee Department of Transportation and University of Tennessee
- Richard McDonough, New York State Department of Transportation
- Galen McGill, Oregon Department of Transportation
- Tyler Patterson, Washington State Department of Transportation
- Robert Pierce, Port of Galveston
- Guy Rousseau, Atlanta Regional Commission
- Erik Sabina, Colorado Department of Transportation
- Sean Strawbridge, Port of Corpus Christi
- Carlos Zaldivar, Miami-Dade Expressway Authority
- Beth Zelinski, Bay Area Toll Authority

ABSTRACT

NCHRP Report/Task 136: *License Plate Reader Technology: Transportation Uses and Privacy Risks*, presents a review of transportation uses of license plate reader (LPR) technology, relevant regulatory and judicial cases, and current trends in public opinion. Detailed case studies were completed for five transportation uses to assess current context, benefits, and challenges. Guidance on strategies and practices is provided to guide transportation agencies in balancing between beneficial uses of LPR data and the protection of individual privacy. These best practices should be understood as the minimum aspirations for an agency's policies, procedures, and controls. Due to the unique requirements of individual agencies and their differing geographies, uses, and experiences, no one set of best practices will be applicable to all organizations.

EXECUTIVE SUMMARY

Privacy is defined as the capability of individuals to determine for themselves when, how, and to what extent information about them is communicated to others. Privacy relates to the likelihood of disclosure of personally identifiable information (PII) about an individual and the magnitude of harm that might result. PII is information that by itself or in combination with other information can identify, locate, or distinguish an individual. License plate reader (LPR) systems consist of high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates into computer-readable data. The system automates the collection of license plate numbers. A license plate number does not identify a specific person; rather it identifies a vehicle. However, the license plate number may be linked or associated with an identifiable person through a linkage with other information about the individual. As a result, while license plate numbers are not inherently PII, their common affiliations and linkages with individuals constitutes an increased risk to privacy.

The use of LPR technology for transportation purposes is not new. Applications stem from the 1990s as technologies such as geographic information system (GIS), global positioning systems (GPS), and cellular telephones were identified as means toward safer and more efficient data collection, improved data quality, and reduced costs. LPR, like other new technologies of the time, was viewed as a "technological fix" for the cost challenges associated with capturing required information for transportation planning and policy making. The privacy risks associated with LPR use would be weighed against the real and perceived benefits of a particular use.

Five transportation uses were assessed regarding privacy risks: travel time estimation, access control, commercial vehicle screening, tolling and payment, and travel behavior analysis. Payment and travel behavior analysis uses were found to present the highest potential overall risk. Payment uses may link vehicle data from LPR to an individual user account that includes financial information. The presence of financial information contributes to a higher possibility of a problem occurring because of the opportunity for fraud, identity theft or economic loss. In contrast, travel behavior involved a high potential for harm because it was the use most likely to incorporate detailed information about individual's behavior. The opportunity for harm increases as individual actions are recorded at multiple locations and times, making it possible for an individual's actions to be tracked. The transportation use with the lowest privacy risk was travel time estimates, which match plates at two points in time. If license plate data cannot be linked to an individual, then PII is not at risk.

Researchers found that uses focusing on commercial vehicle activity, which may be operationally similar to passenger uses, present a lower likelihood of privacy problems for an individual because of the commercial environment of freight. Commercial vehicles are highly regulated and, although a driver is a private citizen, the activities of the driver and vehicle are associated with a commercial operation. This is not to suggest that commercial vehicle uses of LPR may not result in important privacy threats, but that the impact on an individual's privacy is comparatively lower for freight uses.

There are regulatory and legal aspects to assessing privacy risks, but the legal landscape is a moving target. Privacy protection in the U.S. is granted not by a single national law regulating privacy, as in Europe, but by a patchwork of federal and state laws and regulations. Recent U.S. Supreme Court decisions on individuals' locational privacy have been conflicting or left key questions unresolved. One of the most recent high court decisions indicated that "an individual lacks a reasonable expectation of privacy on open, public roads"; while another held that the "warrantless collection of location data over an extended period constitutes a search,"

and, therefore, violates a person's expectation of privacy. It is important to highlight, however, that LPR use is legal in all states with varying levels of restrictions, and it is unlikely that transportation agency users would face civil liability for their work with the technology. However, public concerns regarding privacy might curtail its future application for transportation purposes. Today, there remains a tension expressed in public opinion about the desire for more or less government intervention in privacy protection. A review of public opinion trends, as presented in Chapter 3 of this report, revealed that the more LPR use is seen as general surveillance, the more likely the public are to find it problematic.

The implementation of the best practices presented in this report will serve to mitigate privacy risks associated with LPR use. LPR systems fall into a special category of modern data collection technologies that have the potential to identify unique individuals. Thus, LPR application is likely to receive greater scrutiny in the future. The implementation of the following practices can serve as insurance against future privacy-related challenges.

- **Transparency and openness**: Agencies should notify or otherwise communicate the types of information they collect and how that information is used, disseminated, and shared to individuals within their jurisdictions.
- **Purpose specification**: Agencies should clearly communicate why they are collecting information and under what authority; a change in purpose requires an update of the communication.
- **Data minimization, retention, and use limitation**: Agencies should only collect information that is necessary to meet their specified purpose, retain it for only as long as needed, and restrict its use to only specified purposes.
- **Data quality and accuracy**: Agencies should ensure that data are accurate, of high quality, and – when relevant – enable individuals to review and correct any information.
- **Accountability**: Agencies should define explicit policies and procedures for complying with data protection principles.
- **Security**: Agencies should protect personal data with reasonable measures to prevent loss, unauthorized access or disclosure.

Because of uncertainty in the future legal environment, and in how the public perceives LPR use for transportation purposes, the research team recommends that agencies monitor evolving state legislation and judicial cases involving data privacy in general, and LPR use specifically, as well as public opinion trends in their specific jurisdictions.

CHAPTER 1. BACKGROUND

RESEARCH OBJECTIVES AND SCOPE

The objective of the research was to provide an analytic foundation for transportation agencies evaluating the use of LPR technology. The research identified the major transportation uses of LPR, their associated privacy risks, and best practices for mitigating those risks. This information will guide transportation agencies as they navigate the potential applications of technologies, such as LPRs, that streamline the acquisition and analysis of data and that automate or enhance many existing work processes. For example, the regular automated collection of information from traffic flows can enable agencies to better understand how their road networks function, identify trouble areas, and deploy targeted resources to improve operations. Automating data collection can also increase the efficiency of previously manual processes, like collecting tolls or screening freight vehicles.

The scope of this research is transportation uses of LPR and best practices for transportation agencies. However, LPR is frequently used by law enforcement agencies, and significant attention has been paid to these uses by the media and civil liberties organizations. An effort was made in this research to exclude law enforcement uses except where directly relevant to a transportation audience. The use of LPR to track stolen vehicles, enforce speed limits, conduct criminal investigations and other clear law enforcement operations are not included in this report. The most notable inclusion of law enforcement references is in the legal review. Law enforcement activity is a common focus of legal and statutory requirements related to privacy and LPR, and often applies to transportation agencies as well. In another example, commercial vehicle screening is often executed by officers from law enforcement agencies, but is considered a transportation safety and planning activity. The potential for, and risks from, "data bleed" between transportation agencies and law enforcement are also considered in this research.

The use of LPR technology for transportation purposes is not new. Applications stem from the 1990s as technologies such as GIS, GPS, and cellular telephones were identified as means toward more efficient data collection, improved data quality, reduced costs, and more flexible output products. LPR, like other new technologies of the time, was viewed as a "technological fix" for the cost challenges associated with capturing required information for transportation planning and policy making. However, even at the time, an opposing perspective viewed LPR as a "big brother-like" force with negative implications for individual privacy. "Privacy" is defined as the capability of individuals to determine for themselves when, how, and to what extent information about them is communicated to others. This tension between increasing transportation system efficiency and the specter of privacy risks for individuals exists today.

Thus, this research explored the privacy implications of major transportation use cases and provides information for transportation agencies in developing policies governing their use of LPR data that adequately address privacy concerns. In this research:

- The major use cases have been identified through literature review.
- Privacy implications were investigated through reviews of literature, state regulations, and applicable federal laws and court cases.
- State of the practice by transportation agencies was examined through case studies of the major use cases.
- Best practices were synthesized from literature review and case studies.

The following sections provide the context for the research by describing how LPR technology works, followed by an overview of privacy considerations.

LPR TECHNOLOGY

At their most basic, LPRs are a technology that enables organizations to automatically identify a vehicle by the alphanumeric characters on a license plate (Roberts and Casanova 2012). LPRs function through pairing cameras with a specialized computer software: cameras record an image of a plate, and then a computer translates the image into alphanumeric characters electronic systems can understand. Multiple cameras or video cameras are sometimes used to increase the likelihood a readable image is captured; a traditional high-speed camera is often paired with an infrared camera. Additional illumination, like visible or infrared flashes, is also commonly used. Low-quality images can decrease data accuracy, which is a common challenge associated with LPRs. Combining multiple camera and flash types creates redundancy, reducing the impact from poor lighting or glare, which commonly occurs at dusk or dawn periods.

Once the camera(s) capture an image of sufficient quality, the image is sent to a computer system that uses a series of algorithms to analyze the image, identify and isolate a license plate, and reduce and render the image into the essential alphanumeric characters. This process takes place in six steps (Table 1), and is illustrated in Figure 1 (Roberts and Cassanova 2012, p. 10).

Table 1. LPR Algorithm Processes to License Plate Identification

Algorithm Step	Description
Plate Localization	Finding and isolating the plate in the picture
Plate Orientation & Sizing	Compensating for plate skew and adjusting dimensions
Normalization	Adjusting for brightness and contrast
Character Segmentation	Finding and isolating individual characters on the plate
Optical Character Recognition	Translating images to digital text
Syntactical/Geometric Analysis	Checking characters and positions against state-specific rules to determine a plate's state of issuance

Source: Roberts and Casanova 2012, p. 10

Once the plate is isolated and characters segmented, the optical character recognition (OCR) algorithm makes a probabilistic guess as to which alphanumeric characters exist on the plate. If the image is low quality or other problems exist, the algorithm will have to make a lower-probability guess. When the computer's confidence in its guess is below a set probability threshold, the image and associated information are commonly sent to a human for review.

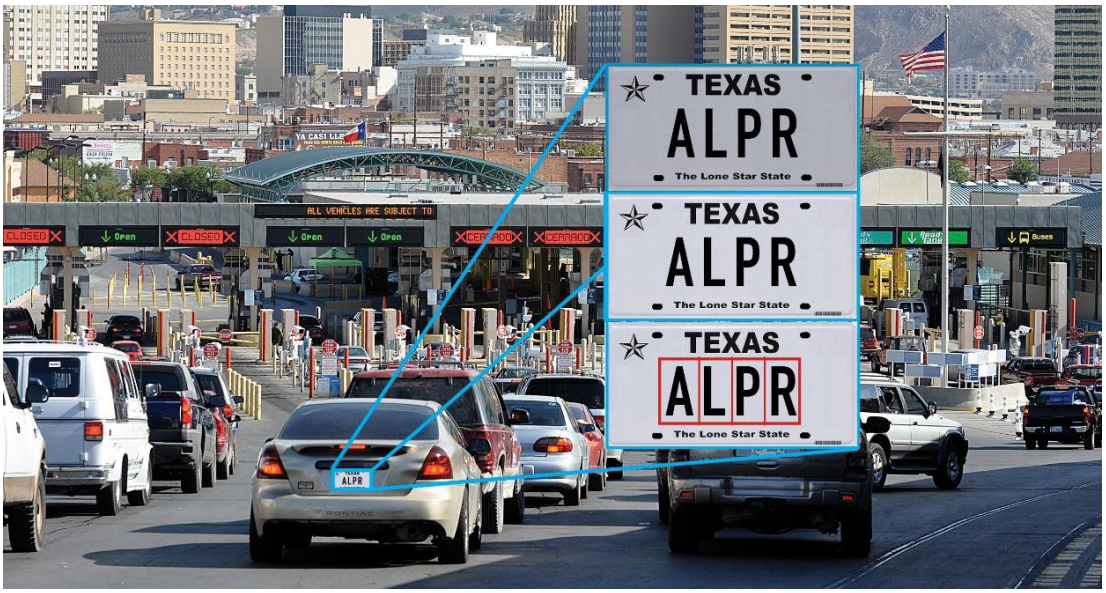


Figure 1. Illustration of the LPR Data Reduction Process

Beyond lighting conditions, there are a variety of factors that affect the probability a LPR system correctly identifies a plate, including

- Plate and character colors;
- Plate design;
- State of origin;
- Plate covers or obstructions;
- Plate location;
- Vehicle headways;
- Vehicle speed;
- Lighting and weather conditions; and
- LPR orientation and system quality.

When an image is recorded, the system also records and bundles additional contextually-relevant data – called metadata – into an aggregated file. The file often contains information including (Roberts and Casannova 2012, p. 13-15)

- The original contextual color image;
- A black-and-white rendering of the image;
- The OCR electronically-readable plate file;
- Longitude/latitude coordinates;
- Time and date; and
- LPR system ID.

Once the image is translated, the transportation agency uses the information – along with the associated metadata – according to their specific needs. Commonly LPRs are used to collect payments and tolls, screen freight, control access to parking and other facilities, and conduct travel

behavior analyses. Some other uses such as travel time estimation have fallen out of favor for a variety of reasons. There are also law enforcement uses that are outside of the research scope.

LPRs can function as either permanent roadside units or mobile on-board units. The most common incarnation transportation agencies use is the permanent roadside unit. Law enforcement agencies often use mobile units to perform surveillance or enforcement across a community, but transport agencies do not normally use these for their purposes.

DATA PRIVACY CONCERNS

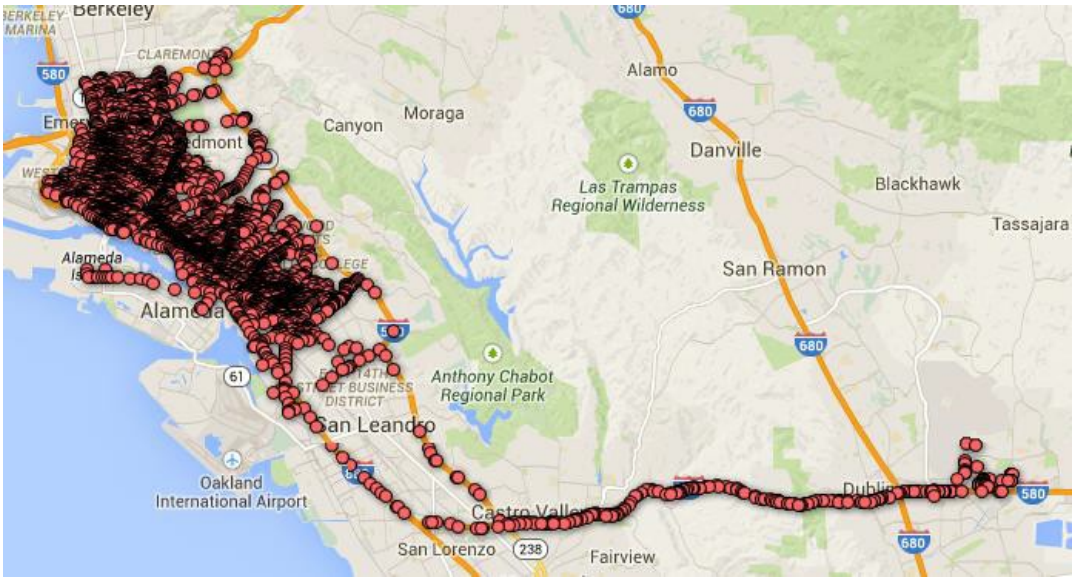
As with other technologies relying on public data collection, which can sometimes be personally identifiable or sensitive, there are concerns that the information collected from LPRs could be misused or insufficiently protected against privacy risks. Agencies must balance the benefits from using LPRs against the risks and concerns associated with misuse of sensitive data.

Privacy is defined as the capability of individuals to "determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967). This is particularly relevant to privacy of PII. The National Institute of Standards and Technology (NIST) defines PII as "any information about an individual maintained by an agency, including

1) Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
2) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

It is important to note that PII is a mutable and malleable concept; there is no single list of what constitutes PII. A single piece of data can be PII, provided it can be used to distinguish or trace an individual's identity, such as a social security number. Likewise, merging multiple pieces of individually innocuous data can become PII, even when the individual pieces are not (i.e., combining date of birth plus a personal address).

Similarly, a publically displayed license plate number, by itself, does not constitute PII. But when aggregated and/or combined with metadata (like location, date and time), or linked to associated information (like a Department of Motor Vehicles [DMV] record), a license plate number can become PII. With regard to metadata, special interest groups have protested widespread law enforcement use of LPR, which they fear – when aggregated and combined with metadata – would provide the government with detailed knowledge of where and when individual's travel (American Civil Liberties Union 2013). To illustrate this point, the Electronic Frontier Foundation created a graphic (Figure 2) depicting eight days of LPR reads from the Oakland Police Department (Gillula and Maas 2015). The data points represent 63,000 LPR reads, 48,000 unique plates, and 39,000 plates that were captured only once, using as few as two car-mounted LPR systems. The moveable LPR systems captured plate data from across Oakland, with a particular focus on low-income neighborhoods. When combined with census data or crime statistics, there are a number of ways that the data could be analyzed to identify individual patterns. In a similar case in Minnesota, the Minneapolis Star Tribune was able to track the local Mayor's location using databases with historic LPR data. This news story raised concerns, and set off a legislative debate about the proper balance between law enforcement needs and privacy protections (Roper 2014).



Source: Gillula and Maas, 2015

Figure 2. LPR Data from Oakland Law Enforcement

Advocacy groups worry that widespread and unfettered uses of LPR systems would harm individual's privacy by informing the government, or other actors if the information is released, to the daily travel patterns and location information of individuals. The American Civil Liberties Union (ACLU) has expressed concerns that long-term retention of license plate data, as well as sharing of this data among multiple agencies, creates an environment in which the data could be used abusively by individuals or by institutions. Such data, especially when amassed and stored for long periods, could be used inappropriately to identify religious, political affiliations, and personal relationships; betray frequent trips to the local gym, medical center, or bar district; and provide other intimate details about an individual they do not wish to publically divulge.

REPORT ORGANIZATION

After this introduction, the report is organized into the following sections:

- **Chapter 2:** Major Transportation Uses and Privacy Risk Taxonomy
- **Chapter 3:** Legislative and Judicial Review
- **Chapter 4:** Case Study Summaries
- **Chapter 5:** Best Practices
- **Chapter 6:** Conclusions and Suggested Research

CHAPTER 2. MAJOR TRANSPORTATION USES AND PRIVACY RISK TAXONOMY

Researchers reviewed current and potential transportation uses of LPR technology. Six use cases are presented in this section: travel time estimates; access; commercial vehicle screening; enforcement; payment; and travel behavior analysis.

Each use case is identified by the types of data collected, links to other data sets, and agencies involved as observed in the literature review for each use case. A summary of data types collected and links to other data sources for each use case is presented in Table 2. In most use cases, the data collected from LPRs were similar, and included the license plate number, photo, and the date, time and location it was taken. Freight screening and enforcement uses were noted for, in some examples, including photos of the vehicle and surrounding environment. LPR data was most commonly linked to vehicle registration data, individual user accounts or to other data points in the same study area.

Table 2. Summary of Data Types and Links by Transportation Use

Types and Links		Transportation Use Cases of LPR					
		Travel Time Estimation	**Access Control**	**Commercial Vehicle Screening**	**Enforcement**	**Payment**	**Travel Behavior Analysis**
Data Types	License plate numbers and photo	X	x	x	x	x	x
	Date, time and location	X	x	x	x	x	x
	Photo of vehicle and/or surroundings			x	x		
Data Links	Link to a user account		x		x	x	
	Link to vehicle registration				x	x	x
	Link to financial account information					x	
	Link to United States Department of Transportation (USDOT) freight registration account			x			
	Link two or more locations in a study area	X				x	x
	Link to Census data						x

Table 3 identifies agencies involved with each transportation use. Departments of transportation were commonly involved in five out of the six transportation uses of LPR. Other

frequent users include parking authorities, cities, transportation planning organizations, and enforcement agencies. Private organizations were also identified, including toll authorities, universities, airports and academic institutions.

Table 3. Summary of Agencies Involved in Transportation Uses

Agency Type	Transportation Use Cases of LPR					
	Travel Time Estimation	Access Control	Commercial Vehicle Screening	Enforcement	Payment	Travel Behavior Analysis
State Departments of Transportation (DOTs)	x		x	x	x	x
Cities		x		x		
Metropolitan planning organizations (MPOs), Transportation planning organizations	x					x
Commercial vehicle enforcement			x			
Traffic enforcement				x		
Toll authorities				x	x	
Parking authorities		x		x	x	
Universities, Airports or Medical Campuses		x				

It is important to note that several uses may overlap in practice, but they are distinguished here to highlight the aspects of each use that increase the probability and impact of privacy risk. The following subsections provide a detailed discussion of each transportation use. Combinations of uses are addressed further in the next section. In this section, the use cases are ordered loosely from lower threat to higher threat of privacy risk.

TRAVEL TIME ESTIMATION

Travel activity of vehicles on the road is commonly collected and used to calculate travel time estimates (see Figure 3). Estimated or predicted travel times are often relayed to drivers in real-time through variable message signs or other communication methods. This information is used in construction and work zones where traffic flow is atypical, but can also be used in travel demand management and intelligent transportation systems (ITS) programs.

Travel times can be collected manually, using a portable computer or through manual transcription of video. The development of LPR technology has offered a convenient and cost-

effective tool for this process. Travel time estimates can be calculated based on LPR scans at two or more points along a corridor. An LPR tag from one data collection site is matched to the same license plate at another location along the study area. This information is compared to calculate a travel time between these fixed locations. Only the LPR time stamps are used to calculate a travel time, which does not necessitate direct use of the license plate number or linking to other information.

Uses	**Data Types and Links**
Travel time estimation Communicating travel information Setting variable toll rates	License plate numbers and photo Date, time and location
Agencies Involved	**Issues**
DOTs MPOs, Transportation planning organizations Research/academic institutions	The Federal Highway Administration (FHWA) suggests destroying all license plate records once travel times have been computed to avoid potential privacy problems (FHWA 1998). Other technologies may provide an alternative technique for travel time measurements (ITS International 2013).
References	
In 2005, the Oregon DOT compared automated license plate reader (ALPR)–based travel time prediction results to probe-based travel time observations on a 25-mile stretch of rural highway. The results found no statistical difference between the predicted travel times and those observed by probe vehicles. The cameras read license plate numbers and associate them with time-stamped tags. According to Bertini et al. (2005), the license plate numbers are "privacy-protected" with encryption and sent to a central server. Data retention policies were not discussed in this report. This project contributed to the broad goal to determine whether LPR data could be used to present travel time estimates to drivers on the road and allow them to make travel decisions (Bertini, Lasky, and Monsere 2005). LPR technology is used to generate predictive travel time information in real time and present the information via variable messaging signs on roadways across England. Real-time journey times are collected based on license plate readings and combined with historic travel times. This report does not mention the retention time for data or strategies to anonymize the data (Burton, Crosthwaite, Simpson, and Billington. 2015).	

Figure 3. Travel Time Estimation Summary Details

ACCESS CONTROL

LPR technology is used for access control in ports, parking lots and other secured areas (see Figure 4). LPR for access may be used in any facility which restricts vehicles that may enter

and exit. In access uses, an LPR is typically mounted adjacent to an automatic barrier (e.g. gate, fence) at the entrance to a facility. It reads an approaching vehicle license and matches it to a list of authorized vehicles. A correct match will raise the barrier automatically. This system preempts the need for access card, radio frequency identifications (RFIDs) or other devices to be issued to new drivers.

Uses	**Data Types and Links**
Secure facilities (such as ports) Parking lots University parking permit programs.	License plate numbers and photo Date, time and location Link to user account
Agencies Involved	**Issues**
Cities Parking Authorities Universities and Medical Campuses Airports	Unlike travel time estimates, LPR data used for access control may be linked to other databases. Historical data may be saved from access management systems for business purposes or to provide data to customers.
References	
Project Seahawk was a port and intermodal security pilot project that included LPR installations at the Port of Charleston (US Department of Justice 2009). See private parking provider NuPark, a “provider of LPR focused parking solutions”. The company is headquartered in Cedar Park, TX (NuPark 2016).	

Figure 4. Access Control Summary Details

COMMERCIAL VEHICLE SCREENING

Truck screening, detection and compliance are common practices for state and national agencies (see Figure 5). LPR technology was one strategy identified in a National Cooperative Highway Research Program (NCHRP) study on innovative strategies for gathering truck activity data (Zmud, Lawson, and Pisarski 2014). Common issues that are screened for are expired registration, proper certifications, and oversize and overweight violations. It can also be used for speed monitoring (Oliveira-Neto, Han, and Jeong. 2009). LPR technology is used to identify trucks by license plate number and match the vehicle to existing databases for violations or other flags. LPR is often combined with other technologies including weigh-in-motion (WIM) devices and video imaging to detect over-size vehicles. Similar to open road tolling, LPR can be used to speed up these screening processes.

Uses	Data Types and Links
Screening Compliance WIM	License plate numbers and photo Date, time and location USDOT registration number Photo of vehicle and/or surroundings Truck size, weight and other defining features Truck LPR data may be linked to USDOT registration information and freight databases.
Agencies Involved	**Issues**
DOTs Commercial Vehicle Enforcement	Commercial vehicle uses may be less "alarming" to the public than passenger vehicles; drivers operate in a highly regulated environment already.
References	
Kentucky has 14 fixed inspection stations in the state for size and weight, safety registration and credentials enforcement of commercial vehicles. More than four million trucks passed through the stations in 2011. The trucks are weighed by the automatic WIM equipment but only 1% are inspected. Inspection stations are maintained by the Kentucky Transportation Cabinet and staffed by Kentucky State Police – Commercial Vehicle Enforcement. The Performance Registration Information Systems and Management based automated ramp screening system (PARSS) was developed in order to identify and screen every vehicle that enters the Boone County, Kentucky inspection station. The system is used to track for violations in safety and compliance. PARSS provides automated screening of trucks based on the license plate number and the USDOT number displayed on the vehicle. Two ALPR systems read the license plate number and jurisdiction from the front of the vehicle. The project tested two different LPRs in order to allow for a side-by-side comparison. In addition to LPR, the system included an automated USDOT number reader, a scene camera that allows for a general description of the vehicle for visual identification purposes, an interface linking to the existing WIM and truck sorting and tracking system, and a screening database containing national and state information regarding safety, registration and credentials. This database is updated daily. This is all connected to a computer in the inspection station. While the system is designed to be automatic, enforcement personnel are shown the LPR results and compared to the photographs so that corrections can be made immediately.	

Figure 5. Commercial Vehicle Screening Summary Details

ENFORCEMENT

LPR technology has been applied to transportation applications to enforce toll facility regulations, parking regulations as well as other traffic violations (see Figure 6). LPR is a foundation technology for all electronic open road tolling, because the license plate is the least common denominator for all vehicles passing through a roadway. Many toll facilities use an in-vehicle transponder to track users, but not all vehicles will be equipped with these devices. While LPR can serve as the central tool to facilitate toll use, more often it is used in combination with other technologies to identify violators and manage casual users who may not have a transponder unit. LPR can be used to identify violators of toll road vehicle occupancy or time of day restrictions. The license plate information is then linked to the registration data to send a violation

notice to the registered owner or to an enforcement agent in real-time. As noted earlier, law enforcement is not the focus of this research but in some cases law enforcement agencies may enforce transportation-related violations. Cities and parking authorities use LPR to check license plates for parking and traffic violations.

Uses	**Data Types and Links**
High occupancy vehicle (HOV), high occupancy toll (HOT), managed lane and toll violations, Parking and other traffic violations	License plate number and photo Date, time and location Photo of vehicle (including occupancy) and/or surroundings Link to vehicle registration database Link to toll user account
Agencies Involved	**Issues**
State DOTs Cities Parking authorities Traffic enforcement agencies Toll authorities	Data sharing conventions can directly impact the potential for privacy risks from LPR data uses. In 2015, legislation was being considered in Pittsburgh, PA, to allow license plate data collected by the Parking Authority be shared with the police force. The combination of multiple data streams and technologies can increase privacy risk. Most toll road and fee charging systems use a combination of technologies to manage the collection and enforcement process. [1]
References	
A study for the Texas Department of Transportation (TxDOT) demonstrated the use of LPR data to detect and enforce vehicle occupancy counts for carpool vehicles in an HOV lane. The LPR data is linked with additional photos that capture the vehicle occupancy. The vehicle is then compared to a "whitelist" of frequent carpool vehicle license plate numbers. The report notes that the integration of these three datasets necessitated "multiple layers of security to protect the privacy of this information" including password protection.	

Figure 6. Commercial Vehicle Screening Summary Details

PAYMENT

LPR can be used as a method of payment for toll roads, congestion pricing programs, and parking (see Figure 7). Open road tolling systems eliminate the need to stop at a tollbooth and allow drivers to travel at a normal speed. LPR data is used to link a passing vehicle to the

[1] For example, dedicated short range communications (DSRC) on-board units may be used for the primary payment method and LPR technology used for enforcement and casual-user transactions. DSRC offers higher accuracy at a lower operating cost, while LPR can address casual users and provide enforcement to overcome DSRC limitations. There may be value in this system in that LPR is only used in some transactions, possibly decreasing spending and reducing the number of people subject to the associated risk.

registered owner, who is then sent a bill that often includes an administrative fee for the processing. In parking management, the LPR system captures the license plate number along with the time and date. When the car later exits, the license plate is captured again and the fee is computed based on the data. This eliminates issues of lost tickets, swapped tickets, cashier fraud or stolen cars. LPR is more commonly used in the US for toll payment violation enforcement (see Enforcement), but some toll facilities that use electronic open-road tolling are using LPR systems more broadly for toll payment. As this type of tolling expands, the use of LPR for this purpose may increase as well.

Uses	**Data Types and Links**
Open Road Tolling Congestion pricing programs Parking fees	License plate numbers and photo Date, time and location Link to vehicle registration Link to toll user account Link to financial account information Link two or more locations in a study area (see Parking example above)
Agencies Involved	**Issues**
State DOTs Cities Toll Authorities Parking Authorities Private parking operators	Historical records could provide information on individual behavior and whereabouts. Link to financial information has the potential to result in more harmful impact from a privacy risk.
References	
LPR is a key technology used to facilitate the London Congestion Charging Program, including both enforcement and payment uses. More than 1,300 cameras are located within the charging area boundaries to record license plates of entering and exiting vehicles. The plates are matched against a database of account holders and charges are applied monthly to a debit or credit card. Drivers without an account can pay in advance or will receive a notice by mail (Transport for London 2016). Multiple tolled highways in Florida use all-electric tolling that relies on LPR to formulate monthly invoices for customers who do not use the SunPass transponders that are also offered as a method of payment. LPR capture the license plate information which is then linked to the vehicle registration data. “Toll-by-Plate” customers are charged a $2.50 administrative fee (Florida DOT 2016). On Virginia’s Elizabeth River Tunnels, a Pay by Plate option is available for one time/occasional use travelers or unregistered local residents. According to operator Elizabeth River Crossings, “By law, once the customer pays the invoice, Elizabeth River Crossings must delete all the information from the system within 30 days, so these accounts are not permanent” (Elizabeth River Crossings 2016).	

Figure 7. Payment Summary Details

TRAVEL BEHAVIOR ANALYSIS

Similar to the collection of travel time data, a network of LPR cameras can be used for the monitoring of entry and exit points over a network of roads to support other analysis (see Figure 8). Capturing the travel of individual vehicles on road segments can inform origin-destination matrices for transportation models and planning. In some cases, such as external station travel studies, the privacy risk would be relatively low because the LPR data does not require a link to other datasets. However, LPR data used for travel behavior efforts may be linked to other personal information such as vehicle registration and home or work locations. Matching license plates against vehicle registration data can be used to infer the ultimate origin or destination or demographic information about the traveler. By matching the license plate data to the DMV records, individual vehicle ownership data, such as vehicle makes, model year, vehicle body styles, fuel type, personal or commercial vehicles, can be obtained (Lee and Williams 2014).

Uses	**Data Types and Links**
Origin-Destination studies Travel behavior studies	License plate numbers and photo Date, time and location Two or more locations in a study area Link to vehicle registration data Link to Census Block-level demographic data samples (based on registered owner's home address)
Agencies Involved	**Issues**
DOTs MPOs Air Quality Management Agencies Research/academic institutions	What are the existing standards for researchers to get approval to match LPR data to vehicle registrations?
References	
In a conversion of Georgia's I-85 HOV lane to HOT lane, LPRs were used in a before-and-after study of the facility and its users. Several studies linked license plate numbers to the Georgia state vehicle registration database to identify the home location of the vehicle owners. This data was linked to Census block groups and that data was used for analysis. Data methods for personal information were not discussed in the research. See Khoeini et al. (2012) and D'Ambrosio et al. (2011). Automated road travel survey is a method that combines LPR data, motor vehicle records and census data, devised to improve upon an existing travel survey method (i.e., travel diaries). Researchers in Los Angeles used LPR data collected by the South Coast Air Quality Management District to link license plate numbers to California DMV registration records. Addresses from the registration database were used to match travelers to Census block groups, as a proxy for demographic information. In one study, LPR, or automatic number plate recognition, cameras provided the data used to analyze the impacts of a London Tube (metro) strike on the traffic travel times. The LPR technology scans and matches vehicle license plates at the entrance and exit of a travel link,	

with journey time data at 5 minute intervals. This study used camera data from 670 travel links totaling a length of 140 km. The data was used to calculate total travel times for sub-city areas, road links, segments, and time of day. It reviewed impacts on the network between the first day of each strike and the following days, changes in departure and arrival times, travel time variation throughout the day (in three broad areas of the network), and a comparison of inbound versus outbound traffic of the three broad areas.

Figure 8. Travel Behavior Analysis Summary Details

ANALYSIS OF TRANSPORTATION-SPECIFIC LPR DATA PRIVACY RISKS

To understand the data privacy risks specific to transportation uses of LPR, the research team developed a taxonomy for classifying LPR for transportation uses. A taxonomy provides a way of defining groups of things on the basis of shared characteristics and giving names to those groups. In this case, the taxonomy is based upon the concept of privacy risk.

Privacy risk is defined as a function of "*the likelihood that a data action causes problems for individuals, such as loss of trust or economic loss, and the impact of the problematic data action"* (Brooks and Nadeau 2015). A data action is defined as an information system practice that processes personal information. Collection, retention, logging, generation, transformation, disclosure, and transfer are examples of processing. One potentially problematic data action, for example, is surveillance – in which personal information is used to track the activities and whereabouts of an individual in a way that may not be proportional to the service being provided. However, in some contexts, surveillance via closed-circuit television cameras in public areas may constitute for some people a valued trade-off between privacy and safety or security.

Privacy risk can be simply represented by the equation in Figure 9.

Privacy Risk = **Likelihood of a problematic data action** x **Impact of a problematic data action**

Figure 9. Privacy Risk Function (Brooks and Nadeau 2015)

Healthcare provides another example of the trade-offs involved in evaluation of personal privacy risk. Electronic medical records include address information, physical attributes, family history, prescriptions, medical conditions, insurance and payment information about a patient. Electronic medical records may improve the quality and delivery of medical care, but these digitized records may also leave sensitive personal information vulnerable to a privacy breach. A breach may be accidental, such as if an administrator sends a test result to the wrong specialist, or intentional, if a criminal hacks a patient database to steal credit card information or a rogue employee uses secure data for blackmail. In any case, personal information in such a database can make an individual more vulnerable to privacy risk.

Privacy risk is a complex legal area that extends beyond the transportation focus of this research. How license plate data is used influences the degree of privacy risk. Guided by the model presented in Figure 9, researchers considered and classified transportation applications of LPR in terms of their likelihood of a privacy problem occurring and the potential magnitude of harm from the privacy problem. The research team applied these two criteria as a means of analyzing and categorizing the transportation use cases according to their privacy risk. The criteria allows a

sorting of the uses based on the probability of privacy problem resulting from a particular use, and the potential harmful impact of privacy risk to an individual created by the use.

Criteria 1 – Likelihood of a Privacy Problem

The likelihood of a privacy problem occurring is the probability that a data action will generate a problem for the typical individual whose personal information is processed. Various factors associated with a particular use will impact the probability that a privacy problem occurs, as summarized in Figure 10.

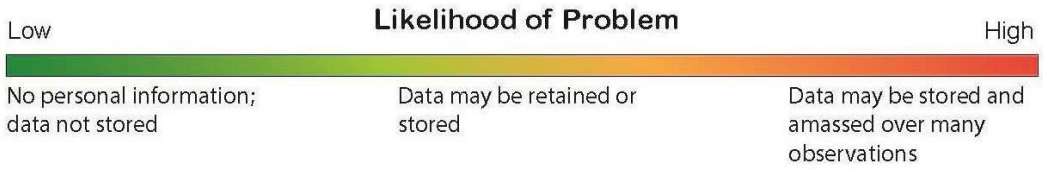


Figure 10. Relative Likelihood of Privacy Problems

Uses of LPR that involve real-time applications, such as travel time estimates that provide real-time information on roadways, raise fewer privacy concerns because personal information is not central to the use. In contrast, when LPR data is retained or stored (instead of deleted) to analyze behavior, the privacy risk increases because the sensitive data could be involved in a problematic data action. Stored data simply allows more time for the data to be disclosed through an intentional or accidental data action. Second, if recurrent information about an individual's actions over time are amassed, that information may be used to track a person's whereabouts and activities. Both of these situations increase the probability of privacy issues. Other factors include the government versus third-party ownership of data, and the geographic comprehensiveness of the database.

Criteria 2 – Magnitude of Harm from Privacy Problems

Privacy risk is a function of the magnitude of harm a data action creates, multiplied by the likelihood that the problematic data action occurs.

The harm, or loss incurred, due to a privacy problem may not always be straightforward to quantify. A data action that leads to financial losses such as credit card fraud, can be quantified in monetary terms. However, other losses may be ambiguous as agencies try to consider issues such as the effect of leaking embarrassing activity of individuals, variation of individual perceptions of privacy risk, and loss of public trust.

The magnitude of harm from a potential privacy risk increases as LPR data is linked to other data sources. The location of a particular license plate becomes far more meaningful, and risky, if it is linked to the registered owner of the vehicle. This factor, how LPR data is linked to other data sources, was used to classify the potential harmful impact of LPR use in transportation. Uses were evaluated based on the types of data collected and the links made to data sources other than LPR output. LPRs typically produce a time and date-stamped photo of a vehicle's license plate and the corresponding license plate number. Some applications supplement that basic data with photos of the vehicle, photos of the surroundings, or other characteristics of the vehicle. Other uses may require linking LPR data to sensitive information about a user, such as personal financial

information to enable payment applications. As LPR data linkages with sensitive data increase, the potential for harm increases (Figure 11).

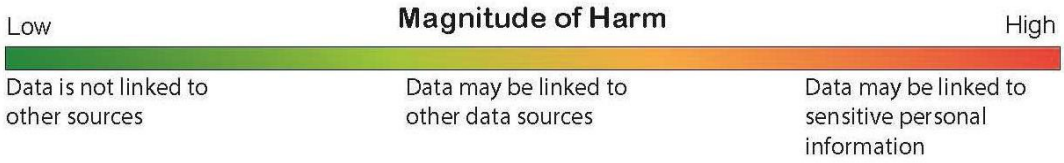


Figure 11. Relative Magnitude of Harm from Privacy Problems

Compiling the Taxonomy

The definition of privacy risk according to the criteria presented above was used to develop a simple taxonomy of LPR transportation uses. The taxonomy is presented in Figure 12. Privacy risks can be evaluated on the likelihood of a privacy problem occurring (y-axis) and the magnitude of the harm that could occur as a result of that problem (x-axis). Each use can be ranked on each criterion from low (green) to high (red).

A privacy risk can be low likelihood and low impact or high likelihood and high impact. Agencies can use this taxonomy to prioritize privacy problems. It also identifies problems where the likelihood and magnitude do not match up. A problem may have a low likelihood of occurring but, in the unlikely event it does occur, a very severe impact. The consequences of such an action may warrant mitigation even though the probability of occurrence is low.

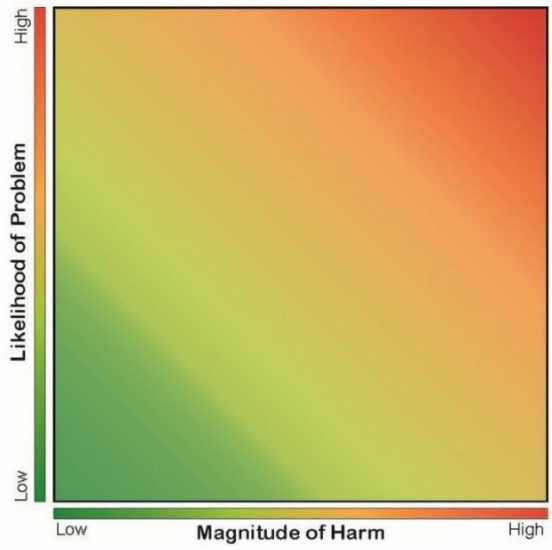


Figure 12. Visualizing Privacy Risk

Researchers reviewed five transportation use cases for LPR for privacy risk. The enforcement and payment uses were combined into one category “tolling and payment” for this analysis. The findings informed a classification of transportation uses for LPR in terms of their likelihood of a privacy problem occurring and the potential magnitude of harm from the privacy problem. The resulting taxonomy of privacy risk for transportation uses of LPR is presented in Figure 13. The uses are sorted based on the probability of a privacy problem resulting from a particular use, and the potential harmful impact of privacy risk to an individual created by the use.

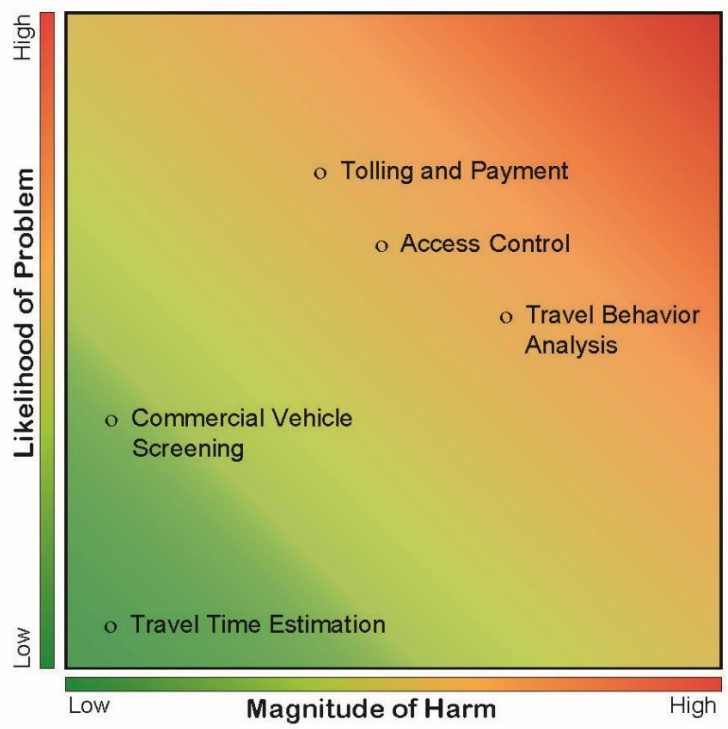


Figure 13. Privacy Risk for Transportation Uses of LPR

The privacy risk associated with LPR use would also be weighed against the real and perceived benefits of a particular use. However, what constitutes a "reasonable" use of LPR is subjective and beyond the scope of this taxonomy. Payment systems that offer obvious time or financial savings for one individual may justify the risk associated with giving up personal information. A traffic engineer may understand the benefits of improved traffic operations, but everyday travelers may not experience those benefits.

A higher magnitude of harm was assigned to uses that linked LPR data to other data sources that could include personal or identifying information. Removing overt identifiers from data (such as name, address, and some identification numbers) does not ensure that the remaining information is no longer identifiable. Re-identification through links with other data is possible, even for some data that have been "anonymized." The uses discussed above range from involving no data links (travel time estimates) to potentially linking to sensitive personal information such as personal accounts and financial information (payment).

Payment uses and travel behavior analysis uses were found to present the highest potential overall risk. The risk is a function of a high likelihood of risk and a high magnitude of harm. Payment uses may link vehicle data from LPR to an individual user account that includes financial information. Financial information contributes to a higher possibility of a problem occurring because of the opportunity for fraud, identity theft or economic loss. In contrast, travel behavior involved a high potential for harm because it was the use most likely to incorporate detailed information about the behavior of individuals. The harm increases as individual actions are recorded at multiple locations and times, making it possible for an individual's actions to be tracked.

The lowest combined privacy risk was assigned to travel time estimates. If license plate data cannot be linked to an individual, then PII is not at risk. The literature indicated that travel

time estimation presents a low probability of a privacy problem due to its real-time application which allows for the LPR data to be deleted once the travel time is calculated. Travel time estimates also require no information other than the location of a matched license plate. LPR data is not linked to vehicle registration data or sensitive personal information about individuals. In contrast, for travel behavior analysis, LPR data may be retained or stored to analyze behavior and trends. This creates a higher probability of a problematic data action that discloses personal information inappropriately.

Researchers found that uses that focus on commercial vehicle activity, which may operationally be similar to passenger uses, present less of a likelihood of creating privacy problems for an individual because of the commercial environment of freight. Commercial vehicles are highly regulated and, although a driver is a private citizen, the activities of the driver and the vehicle are associated with a commercial operation. Freight carriers are held to a higher level of scrutiny when it comes to their operations on the road in part to protect individuals. Information about commercial vehicles, such as USDOT number, size, weight, travel schedule and routes, are closely monitored by federal and state regulations. This is not to suggest that commercial vehicle uses of LPR may not result in important privacy threats, but that the impact on individuals is comparatively lower for freight uses.

Several other factors were identified, but not included in the taxonomy, that could impact the privacy risks created by transportation uses of LPR. One factor is the use of ‘big data’ analytics to collect, link and analyze trends in diverse data sources. Advanced technologies increasingly produce data that is aggregated from individual travelers (including smart card data, video surveillance, emerging connected vehicle data, and data from mobile devices). Whether real-time or archived, this synthesis of information also increases the ability for a data user to be able to track the action of an individual through time and space. While this risk may be unlikely, it can be a serious concern for transportation agencies that are concerned with maintaining public trust.

CHAPTER 3. LEGISLATIVE, JUDICIAL, PUBLIC OPINION REVIEW

STATE LEGISLATIVE REVIEW OF LPR AND PRIVACY

Since 2010, 12 states enacted 14 pieces of legislation specifically addressing privacy concerns and the use of LPR systems. The states were: Arkansas, California, Colorado, Florida, Maine, Maryland, Minnesota, New Hampshire, North Carolina, Tennessee, Utah, and Vermont. LPR use is allowed in all of these states with various levels of restriction. As is often the case in our federalist system of government, these states took different approaches to addressing privacy concerns from LPR use. The laws target a variety of different entities, uses, and take different steps to reduce privacy risks from these sources.

The team analyzed and categorized state laws according to the transportation use cases. This was accomplished by reviewing the text of a particular law and determining if any of the measures placed requirements on (or otherwise addressed) any of these specific uses. The cross-walk between the laws and the transportation use cases contained some conceptual noise because of the language used in the legislation. For this reason, the research team made some minor modifications to the use case categories from those presented in the previous chapter (see Table 4). For example, while law enforcement is explicitly outside the scope of this particular project, it was a very common target of legal requirements.

Table 4. LPR Use Case Category Descriptions

LPR Use Case	Description
Access & Parking	Using LPR to control access to a parking facility, or for other security uses
Law Enforcement	Using LPR for law enforcement purposes other than traffic enforcement (e.g. criminal investigations or surveillance)
Traffic Enforcement	Using LPR to enforce toll, parking, and other traffic regulations
Commercial Vehicle Screening	Using LPR for monitoring and screening commercial vehicles, or enforcing freight-regulated regulations
Tolling and Payment	Using LPR to collect payment for tolling or other purposes
Travel Time Estimates	Using LPR to estimate travel times between two points
Travel Behavior Analysis	Using LPR to analyze individual's travel behavior
Does not specify	Either does not specify uses of LPR, or the language is vague

If a law addressed one of these areas in Table 4, the team recorded an "X" in the appropriate column in Table 5 on the following page. Laws could address multiple use cases, and frequently did.

Table 5. State Laws Addressing Privacy Concerns from LPR Use

Year	2013	2015	2015	2014	2014	2010	2014	2015	2014	2015	2014	2013	2014	2013
State	**AR**	**AR**	**CA**	**CO**	**FL**	**ME**	**MD**	**MN**	**NH**	**NC**	**TN**	**UT**	**UT**	**VT**
Legislative Information	HB 1996/Act 1491	HB 1744/Act 849	S.B. 34	HB 1152	SB 226	§2117-A	SB 699	SB 86	Sec 236:130	SB 182	SB 1664	SB 196	SB 51/222	Ch. 15 Sec. 1607/8
LPR Use Case														
Travel Time Estimates				X										
Travel Behavior Analysis				X									X	
Does Not Specify			X		X	X								
Tolling & Payment									X			X	X	
Commercial Vehicle Screening		X		X								X	X	
Access & Parking	X	X		X								X	X	
Traffic Enforcement				X		X			X			X	X	
Law Enforcement	X	X	X	X		X	X	X	X	X	X	X	X	X
Legal Requirement														
Requires LPR Training														X
Requires Security Breach Notification			X											
Designates LPR Data as PII, Sensitive, etc.			X		X	X								
Restricts Linkages to External Databases								X		X				
Audits LPR Use							X	X						X
Establishes Use Policy	X		X				X	X		X				
Requires LPR Use or Data Request Records	X		X				X	X		X				X
Restricts LPR Use	X	X	X	X		X	X		X			X	X	X
Restricts Data Use	X	X	X			X	X		X	X		X	X	X
Requires Data Destruction	X		X	X		X		X	X	X	X	X	X	X
Restricts Data Sharing or Access	X		X	X	X	X	X	X	X	X		X	X	X

Source: NCSL, 2015

Law enforcement was the single most frequently cited use case for privacy controls, with 13 of the 14 measures addressing law enforcement in some form or another (see Figure 14). In fact, five of the pieces of legislation focus exclusively on law enforcement uses of LPR.

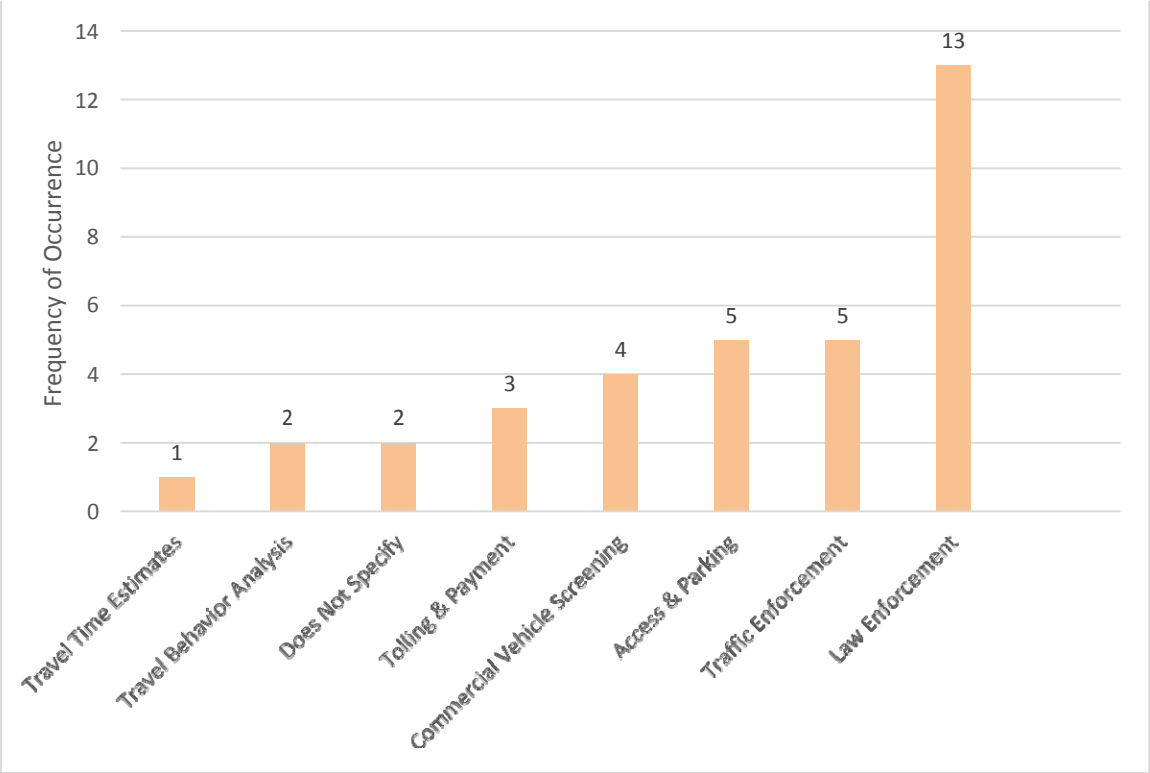


Figure 14. Frequency of Occurrence of LPR Use Cases Addressed in Legislation

The next most frequently cited use cases were the Access and Parking and Traffic Enforcement use cases, with each item included in five laws. Three laws fell under the Does Not Specify category, which meant that the law either did not provide specific areas to which it applied or the legislative language was sufficiently broad that it could apply to other uses beyond those specified. For example, Maine's law specifically points to some uses that it says are acceptable, but also uses broad language in one section that could authorize other uses.

Legal Requirements

The laws not only apply to a variety of different use cases, but also impose a variety of different requirements on these uses. The research team reviewed and analyzed the laws to identify different requirements, and recorded these requirements in Table 6 with an "X" in the appropriate category. Categories were developed by reviewing the laws and identifying requirements that frequently reoccur. The legal requirements categories are defined in Table 6.

Table 6. LPR Legal Requirement Descriptions

Legal Requirement	Description
Establishing Use Policy	Requires the entity using the LPR system develop a written policy guiding the entity's LPR activities and uses
Requiring Data Destruction	Requires data from LPR system be destroyed after a certain time period
Restricting Data Sharing or Access	Restricts who may access data, who it may be shared with, how it may be shared, etc.
Restricting Data Use	Restricts who may use data, how it may be used, etc.
Restricting LPR Use	Restricts who may use LPRs, how LPRs may be used, etc.
Requiring LPR Use or Data Request Records	Requires entities using LPR systems to develop, update, and provide information on use
Auditing LPR Use	Requires regular reporting or auditing of LPR use data
Designating LPR Data as PII or sensitive	Designates LPR data as PII, sensitive information, confidential information, or similar legal category with special legal protections
Restricting Linkages to External Databases	Restricts linking LPR data to other databases
Requiring LPR Training	Requires entities using LPR systems undergo training on their use
Requiring Notification of Security Breaches	Requires notification to the public or affected individuals if a security breach of the LPR system occurs

Several categories of requirements seek to improve oversight and create accountability for those using LPR systems. For example, a written use policy requires public agencies to develop a publicly available document detailing how, why, and/or when LPR systems will or will not be used, along with many other possible details. This forces agency leaders to consider the programs they are administering and write public policies guiding their use, which may result in leaders being held accountable if their agency fails to follow the written use policy. Similarly, requiring agencies to maintain records on how or when LPR systems are used, and then having a third party audit these records could also improve accountability.

Some other requirements focus more on the actual operation of LPR systems. For example, some states restrict who can or cannot use LPR systems (e.g., law enforcement can or cannot use LPR), or create requirements on when or how they can or cannot be used (e.g., traffic analysis is acceptable, but surveillance is not). Maine's legislation prohibits general use of ALPR systems, but exempts several specific groups and purposes: the Maine Department of Transportation can use LPRs to protect public safety and transportation infrastructure, and the Department of Public Safety and Bureau of State Police are granted permission for inspecting and screening commercial motor vehicles (Gierlack et al., 2014). Vermont's policy requires operators undergo special training before they can use LPR systems. California requires any entity operating an LPR system, "maintain reasonable security procedures and practices… to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure" (California 2015). There was substantial variation in the activities states specifically

banned or allowed, and it often seemed tied to regional concerns or issues. New Hampshire, for example, lists specific exits on a transit facility where LPR use is lawful.

Some of the most frequently occurring requirements focus on protecting or restricting the use of data acquired through LPRs (see Figure 15). Almost all of the laws either require the data from LPR be destroyed after a set amount of time, place restrictions on sharing the data, or restrict who may use the data and how it may be used. In SB 34, for example, California restricts data sharing by stating, "A public agency shall not sell, share, or transfer LPR information, except to another public agency, and only as otherwise permitted by law." Florida also restricts sharing, but through a different mechanism. Florida designates any PII found in LPR systems as "confidential," and makes this personal data no longer subject to open records requests.

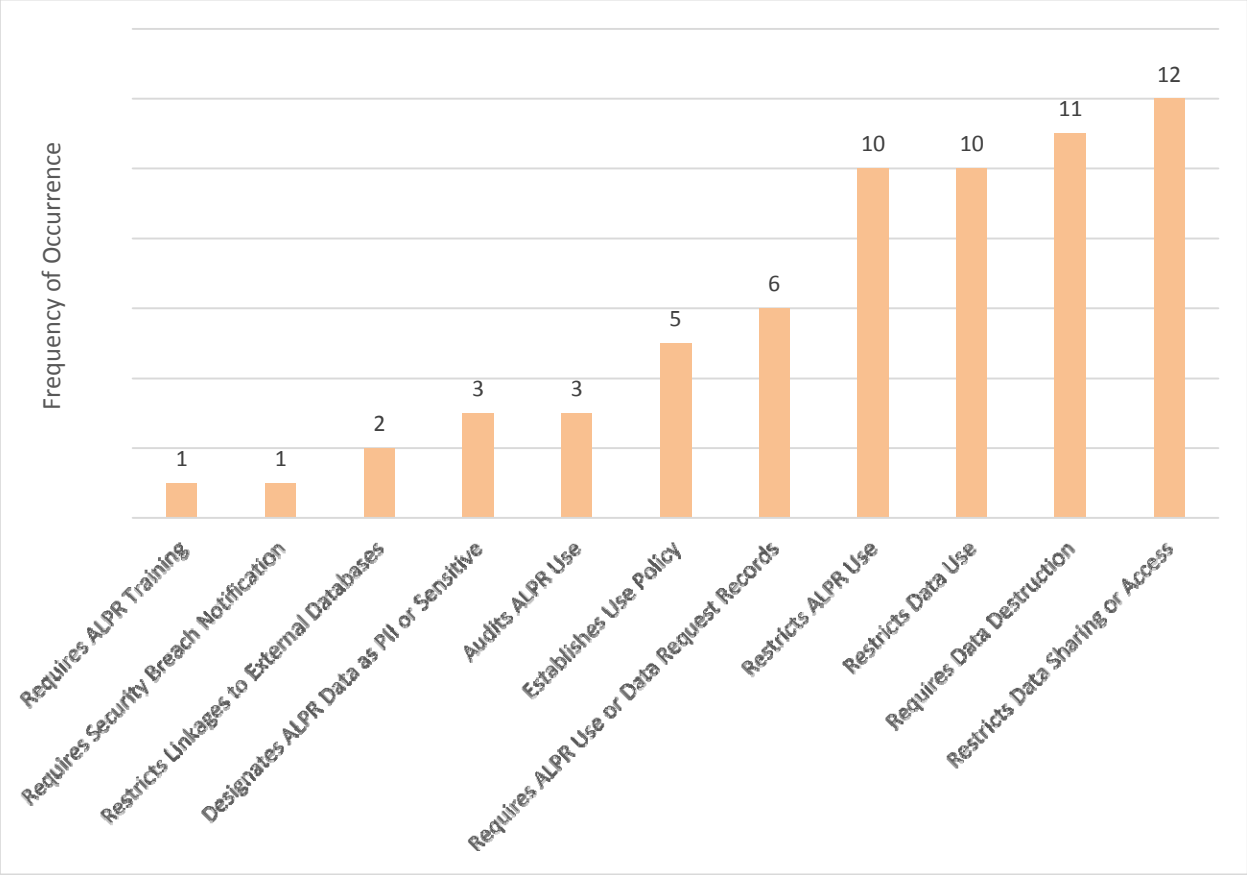


Figure 15. Frequency of Occurrence of ALPR Legal Requirements

Data destruction requirements also varied widely by states (see Table 7). Arkansas requires in HB 1996, for example, that any "Captured plate data obtained… shall not be preserved for more than 150 days." States often had some legal exceptions, however, when data might be held for longer periods. In this case, Arkansas allows that data "may be retained as part of an ongoing investigation," but requires that it be destroyed once the investigation or any criminal legal actions has completed.

Table 7. Data Destruction Requirements by State

State	Number of Days
Utah	14
Maine	21
California	60
Minnesota	60
Tennessee	90
Arkansas	150
North Carolina	365
New Hampshire	548
Vermont	548
Colorado	1,095

When states designate LPR data as PII, sensitive, or confidential, they often bestow a variety of different protections. Florida, as mentioned earlier, designates LPR data as confidential and makes it no longer subject to open records requests. Maine also makes LPR data confidential, which removes it from open records requests. In the event of a California public agency having a breach of personal information (which LPR data is considered) an agency must notify individuals in "the most expedient time possible and without unreasonable delay." In a somewhat unusual policy, Arkansas bans "captured plate data" from containing any personal data. Arkansas also specifically defines captured plate data as "the GPS device coordinates, date and time, photograph, license plate number, and any other data captured by or derived from any automatic license plate reader system." Some state and federal laws allow individuals to sue in court for privacy violations, including classes of individuals, and these can also result in significant fines or damages awards.

JUDICIAL REVIEW OF LPR AND PRIVACY

The judicial analysis and review discusses laws regulating privacy. These laws originate from several sources, each listed below with a brief notation as to that law's likely applicability to LPRs. Generally these laws pertain specifically to law enforcement agency use; LPR use by transportation agencies has not been raised.

United States Constitution

Article III of the Constitution imposes justiciability[2] requirements that limit federal courts' ability to hear claims. In particular, "standing" requires that plaintiffs allege an actual injury and not merely raise abstract objections to laws or policies from which plaintiffs themselves have not suffered. Justiciability requirements will either limit or eliminate claims brought against the use of LPRs by people who cannot show an actual injury. State courts have similar requirements, but are not viewed as strictly as federal courts.

[2] "Justiciable" means suitable for litigation, a concept which has special meaning in federal courts. To be justiciable, a legal claim must be "ripe" (actual and existing, not speculative), the plaintiff must have "standing" (have suffered an actual injury caused by defendant's conduct, and capable of resolution by a court), and the claim must not become "moot" (must remain ripe through the entirety of litigation). See Wright & Kane, Federal Courts 7th ed. (West) 133-42.

The First Amendment both supports and undermines privacy rights. The support comes from Supreme Court rulings (and some dissents) describing the First Amendment's protection of intellectual freedom. This freedom includes such things as free association, the right to refuse disclosure of one's membership in associations, and even the right to refuse disclosure of one's beliefs.

The First Amendment's conflict with privacy occurs with its protection of expression, such as when a news organization publishes illegally-obtained information. In these instances, the LPR data holder who negligently released information may have liability, not from the First Amendment itself (which merely protected the publication), but from other laws explained below, most notably the Fourth Amendment and certain statutes. We discuss the Fourth Amendment after briefly addressing the Fifth and Fourteenth because it has long been considered the most critical in protecting privacy from government intrusion.

The Fifth and Fourteenth Amendments' due process clauses create limited privacy rights regarding family, health, procreation, and sex. There is no indication in current litigation that these principles will extend to the use of LPRs. The Fifth Amendment's self-incrimination clause also protects privacy interests, but is expressly limited to criminal prosecutions and should not otherwise apply to LPR data.

The Fourth Amendment provides citizens reasonable expectations of privacy from warrantless searches or seizures by government entities, at both the state and federal level. This has traditionally been viewed as a limit on law enforcement operations, but in the past few years has been applied in purely civil cases. To be viewed as violating the Fourth Amendment protection, a state or federal entity must:

1. Engage in a search or seizure of a person or that person's property,
2. Without a warrant (or under none of the warrantless exceptions), and
3. In a setting where the person would have a "reasonable expectation of privacy."

A critical question is whether use of LPR constitutes a "search." There have been no Fourth Amendment cases directly related to LPR. In 1983, the Supreme Court's interpretation of the Fourth Amendment in *United States v. Knotts* held that there was no expectation of privacy regarding the location of any particular vehicle on public roadways (Eberline, 2008; Hermann, 2015). The case involved a radio transmitter that was installed to aid tracking suspected illegal drug manufacturers. More recently, in *United States v. Jones*, the Court addressed whether a Global Positioning System (GPS) tracking device attached to a car constituted a search. The Court's decision was split. However, the majority opinion held that the use of a GPS and the warrantless collection of location data over an extended period of time did constitute a search (Gierlack et al, 2014). The "mosaic theory" – a civil liberties theory of Fourth Amendment privacy law – posits, however, that when many individual ALPR readings of a single vehicle are combined to analyze the vehicle's movements over time, they constitute an invasion of privacy, even though each individual reading would not (Gutierrez-Alm, 2015).

It is difficult to predict exactly how the Court would resolve Fourth Amendment issues raised by LPRs. Fourth Amendment litigation regarding large-scale collection and analysis of LPR data had not, as of 2014, reached the U.S. Supreme Court, but lower courts have heard some cases (Merola and Lum, 2012; Gierlack et al, 2014). However, the legal expertise on the research team believes the Fourth Amendment will be the basis for lawsuits against LPR usage.

The lawsuit likely would be brought as a civil rights claim under 42 U.S.C. § 1983.[3] The ACLU has been active in seeking information on the extent of LPR use. Generally, this has involved filing federal Freedom of Information Act requests (or their state law analogs) and litigating any denials (Gierlack et al., 2014). These suits have sought to gather information on the amount and scope of data collected, rather than any direct effort to halt LPR use.

Federal Statutes

Congress has enacted a number of statutes protecting privacy in general and PII in particular. It is likely, but not certain, that federal statutes would govern only federal LPR data holders. At this point, the legal expert on the research team is not aware of any federal statutes directed specifically to LPRs or data obtained by them. However, the LPR function falls under at least one other general statute, the Privacy Act of 1974, which prevents the unauthorized disclosure of personal information held by the federal government. The statute's language is broad and would appear to include LPR information obtained or held by any federal agency or office, although there has not been any application of the Privacy Act of 1974 to LPRs.

LPRs may also fall under other general statutes protecting privacy. For example, the Federal Driver Privacy Protection Act of 1994 provides that, "A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity . . ." certain PII obtained by that DMV.[4] When government entities using LPRs have access to, or later obtain DMV information, this statute would apply.

When LPR use includes access to financial information (as with toll authorities), other federal statutes protecting financial information may apply. Most of these statutes are sufficiently narrow to specify their intended coverage, and do not allow use outside the statute's meaning, as with the Gramm-Leach-Bliley Act's focus on financial institutions.[5] On the other hand, plaintiffs with LPR complaints may attempt claims under a broad reading of these statutes, and in some instances the broad reading may succeed.

Privacy regulation in general ranges from none to considerable (the Health Insurance Portability and Accountability Act for example), and even where the laws exist, enforcement

---

[3] In 42 U.S.C. § 1983, Congress authorized private persons to bring legal claims in federal or state court against any state actor who acts under state law to violate the claimant's civil rights. The statute defines civil rights as "any rights, privileges, or immunities secured by the Constitution and laws." Acting under state law means acting "under color of any statute, ordinance, regulation, custom, or usage," and includes both actions authorized by state law and misuse of authority. See Monroe v. Pape, 365 U.S. 167, 172 (1961). The covered civil rights include privacy under the Fourth Amendment. See Soldal v. Cook, 506 U.S. 56 (1992) (not an informational privacy case, but holding that a police-assisted seizure of a mobile home for eviction purposes raised a Fourth Amendment claim, and was a proper § 1983 claim against both the police and the landlord). For an argument on the application to ALPRs, see Jessica Gutierrez-Alm, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 Hamline L. Rev. 127 (2015); ACLU, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, 2 (July 2013) available at https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record.

[4] See 18 U.S.C. § 2721.

[5] See 15 U.S.C. §§ 6801-6809 (1999). The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (1999) imposed privacy-safeguard requirements on "financial institutions" which it defines as "any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12" (which further defines "activities that are financial in nature.") Thus the Gramm-Leach-Bliley Act defines the statute's focus, and though broadly including financial institutions, by its text excludes other entities holding private data.

varies considerably. Any federal statutes that do apply to LPR functions will often have penalties that may include fines (civil or criminal), other criminal penalties, or a private cause of action authorizing an injured party to sue the agency or people within the agency. For example, the Privacy Act specifically provides civil remedies, including damages, and criminal penalties, for violations.

An individual claiming such a violation by an agency may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs against the agency. In addition, the court may direct the agency to grant the plaintiff access to his/her records, and when appropriate direct the agency to amend or correct its records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by the agency to comply with the Act. In the case of "criminal violations" of the Act, an officer or employee of an agency may be fined up to $5,000 for:

- Knowingly and willfully disclosing individually identifiable information which is prohibited from such disclosure by the Act or by agency regulations; or
- Willfully maintaining a system of records without having published a notice in the Federal Register of the existence of that system of records.

In addition, an individual may be fined up to $5,000 for knowingly and willfully requesting or gaining access to a record about an individual under false pretenses.

Because the use of LPRs is legal in all states, although with significant restrictions in some, it is unlikely that any public users of such systems would face civil liability as described above. Even if a litigant could identify a legal theory to support a lawsuit, the doctrines of sovereign and qualified immunity[6] would pose additional obstacles to a successful suit, at least under current law in most states (Gierlack, et al., 2014). Some federal and state statutes include an underlying regulatory structure that would have to be considered as noted below.

Common Law Privacy Torts

American common law recognizes four tort claims regarding privacy: (1) invasion of privacy or the unreasonable intrusion on seclusion, (2) appropriation of name or likeness, (3) public disclosure of private facts, and (4) holding someone out in a false light. Government entities (state or federal) should be immune from suit under these four common law theories unless the applicable Tort Claims Act (1) specifically waives immunity for that tort, or (2) is read

[6] Sovereign immunity is an ancient doctrine which in its absolute form bars legal claims against governments and government employees. Both the United States and the individual states have inherent sovereign immunity from lawsuits unless (1) the government entity waives immunity in what are typically called "tort claims acts," or (2) in the case of states, Congress abrogates (overrides) state immunity as it did in 42 U.S.C. § 1983 for civil rights violations. In spite of Congress overriding state immunity in § 1983, some parties retain absolute immunity. Judges acting in their judicial capacity are one example. See Pierson v. Ray, 386 U.S. 547, 553-554 (1967). Similarly, police and certain other government actors have qualified immunity from § 1983 claims, that is, they are not liable if they had a good faith belief that their actions were lawful or justified. In these two examples, the judge is immune from liability without the need to prove anything further while the police officer is immune only if he or she can show the action was done in a good faith belief of its legality.

to cover the tort under a broad negligence waiver.7 Non-governmental entities using LPRs will be subject to these tort claims.

Contract Law

Where data collectors have a contract with the people from whom data is gathered, the contract may impose privacy obligations on the collector, or alternatively may include waivers in which the subject of data collection agrees that certain information can be collected, aggregated, assessed, and/or transferred to other parties. To the extent that LPRs are used by government entities, there are likely no contractual issues to consider.

Professional and Fiduciary Obligations

Professionals such as doctors and lawyers and fiduciaries such as estate trustees have legal and ethical obligations that generally include protecting privacy interests, even in the absence of requirements under statute, regulation, or contract. As with contractually-imposed limits, it is unlikely that government-operated LPRs will have professional or fiduciary obligations to the owners of vehicles who have been subject to LPR data collection.

PUBLIC OPINION REVIEW OF LPR AND PRIVACY

Public transportation agencies use LPR data to aid in transportation planning, traffic monitoring, and traffic enforcement. Agencies use the data to assist the public in making better travel choices or in efficiently paying for transportation services and facilities. However, privacy advocates view the implementation of LPR technology as a serious privacy and civil liberties threat, especially when data are stored, retained, and shared (ACLU, 2013). While the actual privacy risks of different transportation uses of LPR data as examined in this report are often quite low, sometimes it is the perceptions of privacy risk that affects people's acceptance of the various LPR applications. There may be very low privacy risk for some LPR applications, but if people perceive a risk and raise concerns to policy makers or other decision makers – it may compromise agencies' ability to collect and use LPR data in the future.

Public attitudes about the privacy risks of LPR technology have not been tracked over time. However, public attitudes about privacy – in general – have been tracked over time, and these data can inform the current study. Gauging public sentiment about privacy risks is a complicated topic. This is because the value of privacy and consumer interest in protecting privacy are complex and ever-changing ideas: varying over time, from person to person, in different contexts and transactions, and in response to current events. As an example, a recent

---

[7] Some states' tort claims acts waive sovereign immunity for narrowly-defined and itemized claims. The Texas Tort Claims Act, for example, waives immunity for negligence by a state employee acting within the scope of employment who is involved in an auto accident (or with motor-driven equipment), or creates injury by misusing tangible property. See Tex. Civ. Prac. & Rem. Code § 101.021. In contrast, the Federal Tort Claims Act provides a broad waiver for "claims against the United States . . . caused by the negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment under circumstances where the United States, if a private person, would be liable. . . "28 U.S.C. § 1346(b). The waiver is re-stated, arguably more broadly, in a resulted statute providing for federal government liability "in the same manner and to the same extent as a private individual under like circumstances . . ." 28 U.S.C. § 2674. This broad nonspecific waiver is then followed by exceptions to waiver stated in 28 U.S.C. § 2680. Using this broad initial waiver followed by exceptions will likely require amendments to the statutory exceptions unless the government entity wishes to waive immunity for claims arising under new technology.

Pew Research Center Survey (2015) found that aside from social security numbers (SSN), which 95 percent of respondents considered to be sensitive information, data ranging from health information, phone and email message content, to one's romantic relationship history could all be viewed as sensitive depending on the context (see Figure 16). Of particular importance for our purposes, one's physical location over time was second to SSN in terms of perceived sensitivity – a key data element derived from LPR data.

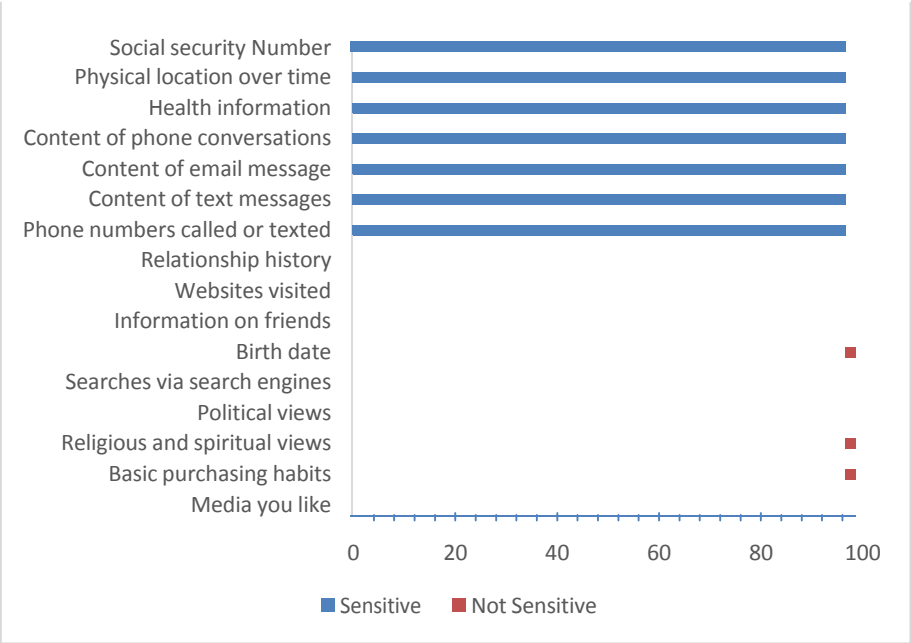


Figure 16. Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Research Center, November 12, 2014

Levels of Privacy Concern

Westin defined privacy as the "claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others" (Westin, 2003). He measured and tracked public sentiment regarding privacy in more than 30 privacy related surveys between 1978 and 2004. Through this work, Westin "segmented" the American public into three categories based on their reported levels of privacy concern (Kumaraguru and Cranor, 2005):

- **The Privacy Fundamentalists:** This group views privacy as an especially high value, rejects the claims of many organizations to need or be entitled to get personal information for their business or governmental programs, thinks more individuals should simply refuse to give out information they are asked for, and favors enactment of strong federal and state laws to secure privacy rights and control organizational discretion. This group generally chooses privacy controls over consumer-service benefits whenever these compete with each other.
- **The Pragmatists**: This group weighs the individual and societal benefits of various consumer products and services, the enforcement of public safety, and protection of national security against the degree of intrusiveness of the personal information collected. They believe that businesses and government should "earn" their trust before they accept

privacy risks. Where consumer matters are involved, they want the opportunity to decide whether to opt-in or opt- out of collection and use of their personal information.

- **The Unconcerned:** This group is generally trustful of organizations collecting their personal information, comfortable with existing organizational procedures and uses, is willing to forego privacy claims to secure consumer-service benefits, and does not in favor new privacy laws or regulations.

Temporal trends from the 1970s to early 2000s show that the distributions in the three categories vary over time, but in general, the percentages hover around 15–25 percent fundamentalists, 15–25 percent unconcerned, and 40–60 percent pragmatists (Westin, 2001).

As is often the case when characterizing public opinion, there is often a small group of concerned citizens, such as the fundamentalists who often can influence public policy on a topic. As an example, privacy fundamentalists have vocally expressed their views in many states, which led to the near elimination of LPR use for origin-destination surveys by many MPOs and state DOTs (Hard, et al, 2006). At the other side of the issue, the "unconcerned" represent a small group whose behavior also sways public policy on the topic by their lack of bother about protecting privacy. These two groups are in contrast to the privacy pragmatists who would still respond to external station surveys – weighing for themselves the personal and societal value and the relevance of the information collection activity against any perceived costs and risks. In recent years, as discussed below, the share of concerned individuals appears to be increasing.

Privacy Paradox

The large number of pragmatists has led to the observation that many individuals display paradoxical behavior when it comes to privacy – *that people express concerns about privacy and the capture of information in some contexts, but do not act accordingly in terms of the ways in which they may or may not safeguard their information* (Acquisti & Gross, 2006; Boyd & Hargittai, 2010; Debatin et al., 2009). For example in a 2014 Pew Research Center survey, people say they are concerned about privacy on the web and their cellphones. They say they do not trust Internet companies or the government to protect it. Yet they keep using the services and handing over their personal information (Madden, 2014). The phenomenon where people's privacy concerns do not seem to affect their behavior has come to be called the privacy paradox (Barnes, 2006). Hence, the privacy paradox describes a discrepancy between attitudes and behavior. So far, however, this paradox has not been fully explained. Underlying factors have been identified as a lack of risk awareness, a lack of awareness of possible tools to protect privacy, and a tendency to underestimate the privacy dangers of self-disclosure.

But more recently, privacy as a public policy and societal issue has become linked with notions of security and surveillance, and the potential link between attitudes and behavior has strengthened. The Pew Research Center (2015) examined American's thoughts about privacy, as indicated in the word cloud presented in Figure 17. People associated privacy with ideas of personal information—private, confidential. Beyond the frequency of individual words, when Pew grouped the answers into themes, the largest block of answers ties to concepts of security, safety, and protection. As the links among privacy, security, and surveillance become more established, people start to alter their behavior as noted below.

What comes to mind when you hear the word "privacy"?

Figure 17. Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Research Center, November 12, 2014

Changing Public Opinion and Shifting Behavior

Public opinion regarding privacy and security seem sensitive to the context of current events: terror threats, cyberattacks, and revelations regarding governmental surveillance all seem to affect American's views. Terrorist attacks have generated increased anxieties, for example. After the San Bernardino and Paris shootings in late 2015, a Pew Research Center survey found that 56 percent of Americans were more concerned that the government's anti-terror policies have not gone far enough to protect the country, compared with 28 percent who expressed concern that the policies have gone too far in restricting the average person's civil liberties (Rainie and Madden, 2016). Just two years earlier, after Edward Snowden's revelations about National Security Agency surveillance programs, a plurality said they were more concerned that anti-terror programs had gone too far in restricting civil liberties (47 percent), rather than not far enough in protecting the country (35 percent).

Simultaneously, other findings suggest Americans are becoming more anxious about their privacy, especially in response to growing numbers of security breaches. Globally, 1 billion data records were compromised in 2014 (Frank, 2016). In a PricewaterhouseCoopers survey on cyber threats, 76 percent of corporate executives said they were more concerned about cyber threats than in the previous 12 months, and 79 percent had detected a security breach in the past year.

Perhaps in response to such events and issues, several studies have captured changing attitudes relating to privacy. A 2014/2015 survey by Pew Research Center found that post-Snowden, 17 percent of respondents had changed their privacy settings on social media; 15 percent use social media less often; 15 percent have avoided certain apps and 13 percent have uninstalled apps (Rainie and Madden, 2015). More recently, a 2015 study by the National Telecommunications and Information Administration found that nearly half of Internet users in the U.S. refrained from online activities due to privacy and security concerns (Goldberg, 2016). Forty-five percent of online households reported that these concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the internet, and 30 percent refrained from at least two of these activities. Identity theft was the top reason for refraining from online

activities – cited by 63 percent of respondents – followed by financial fraud, noted by 45 percent. Nineteen percent of internet-using households—representing nearly 19 million households—reported that they were affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to the survey. Similarly, 22 percent of internet-using households that used a mobile data plan to go online outside the home experienced an online security breach. These figures all reinforce the growth of concerns regarding data privacy and security in recent years.

Implications for LPR Data Collection

In the U.S., there remains a tension expressed in public opinion about the desire for more or less government intervention in privacy protection. Privacy protection in the U.S. is granted not by a single national law regulating privacy, as in Europe, but by a patchwork of federal and state laws and regulations. The U.S. has taken a passive stance on privacy legislation, leaving companies to self-regulate privacy practices.

As the agency responsible for privacy protection, the Federal Trade Commission (FTC) issued best practices in 2012 to protect privacy and give Americans greater control over the collection and use of their personal data. The FTC goal was to balance the privacy interests of consumers with innovation that relies on information to develop beneficial new products and services (FTC, 2012). Only when firms fail at self-regulation does the FTC step in. The practices focus on four key concepts:

- Notice of collection and intended use (purpose limitation)
- Informed consent
- Citizen access to information about themselves
- Responsibility to keep data secure and accurate

In an LPR context, these practices are often challenging to uphold because data linked to a person are often:

- Not provided by a subject
- Results from opportunistic sensing system (that is one in which an individual may not know his/her movements are being captured)
- Identified ex-post from the integration of LPR data with other data.

LPR is a "sensing" technology that the public may view as a means of surveillance (ACLU, 2013). Thus, the public may become increasingly concerned about its use in law enforcement and perhaps, by transportation agencies. As such, Americans' views about privacy and surveillance are relevant to transportation agencies forming policies on these matters.

According to 2015 surveys by the Pew Research Center, a majority of Americans believe it is important – often "very important" – that they be able to maintain privacy and confidentiality in commonplace activities of their lives (Madden and Rainie, 2015). Most strikingly, these views are especially pronounced when it comes to knowing what information about them is being collected and who is collecting it. These feelings also extend to a desire to maintain privacy when moving around in public. Survey results from early 2015 show:

- 93 percent of adults say that being in control of *who* can get information about them is important; 74 percent feel this is "very important," while 19 percent say it is "somewhat important."

- 90 percent say that controlling *what* information is collected about them is important—65 percent think it is "very important" and 25 percent say it is "somewhat important."
- 88 percent say it is important that they not have someone watch or listen to them without their permission; 67 percent feel this is "very important" and 20 percent say it is "somewhat important."
- 63 percent feel it is important to be able to "go around in public without always being identified." Only 34 percent believe being able to go unnoticed in public is "very important" and 29 percent say it is "somewhat important" to them. In both cases, all adults, regardless of age or gender, express comparable views.

In this current climate, trust that the collector of the information will keep data secure becomes very important. But according the Pew Research Center surveys, Americans have little confidence that their data will remain private and secure. Just 6 percent of adults say they are "very confident" that government agencies can keep their records private and secure, while another 25 percent say they are "somewhat confident." This means that over 50 percent do not feel confident that government agencies can keep their records safe and secure.

Out of broad concerns about the protection of personal information, a large portion of respondents reported that they had engaged in some everyday obfuscation tactics and privacy-enhancing measures. Some of the more common activities reported by Pew included:

- Refusing to provide information about themselves that was not relevant to a transaction (57 percent have done this).
- Using a temporary username or email address (25 percent have done this).
- Giving inaccurate or misleading information about themselves (24 percent have done this).

Transportation agencies need to be aware of the changing landscape of public opinion and associated behaviors relating to privacy. LPR systems fall into a category of modern information technologies (such as the internet and mobile phones) with the potential to magnify individual uniqueness, thus, raising privacy challenges. At the same time, state regulation and judicial decisions have fallen behind rapid progress in information technologies. Recent U.S. Supreme Court decisions on individuals' locational privacy have been conflicting or left key questions unresolved. One of the most recent high court decisions indicated that "an individual lacks a reasonable expectation of privacy on open, public roads"; another held that "warrantless collection of location data over an extended period constitutes a search," and, therefore, violates a person's expectation of privacy. The more LPR use is seen as general surveillance, the more likely courts and the public may find it problematic. It is important to highlight, however, that extensive LPR system use is legal in all states with varying levels of restrictions, and it is unlikely that transportation agency users would face civil liability for their work with the technology. However, public concerns might curtail its future application for transportation purposes.

CHAPTER 4. CASE STUDY SUMMARIES

Case studies were conducted to examine the similarities and differences in the application of LPR to specific use case contexts. These case studies were based on the transportation use cases identified in the privacy risk analysis presented in Chapter 2. By design, use cases were selected to represent a range of low to high privacy risk, with an emphasis on higher-risk uses. The five case studies were based on interviews with 25 subject matter experts and transportation practitioners from state and local government agencies, supplemented by literature searches in some cases. Literature review and a snowball sampling technique were used to identify agencies that might employ LPR for the specific use, and email was used to contact individuals to serve as expert interviews for case study data collection. Snowball sampling is used to identify hard-to-locate interview subjects, and functions as a chain referral: after finding someone with knowledge on the specific use case, the researchers asked for assistance to help identify people with similar knowledge and familiarity. Approximately five persons were interviewed for each case study.

The full questionnaire is included in the appendix, but as a summary, the interview topics included:

- For what purposes they use LPR,
- Associated benefits and challenges,
- Training practices regarding data use and control,
- Data retention and destruction practices,
- Data mining or data sharing practices,
- The existence of written data privacy policies or procedures.

The following subsections are organized according to the case studies: how LPR is used in travel time estimation, access and parking, commercial vehicle screening, tolling and payment, and travel behavior analysis.

TRAVEL TIME ESTIMATION

Travel time, or the time required to traverse a route between any two points of interest, is a fundamental measure in transportation. The knowledge of travel times on road networks is of vital importance for road operators as well as for passenger or commercial vehicle drivers. Operators can use travel time information to improve control on their networks. Drivers can choose their optimal route based on the available traffic information and their individual preferences. LPR systems can be used to record the location of a vehicle at two different points in time. Optical cameras capture images of license plates of oncoming or receding traffic and use video image processing to "read" the license plates. License plate numbers can then be matched at sensor locations downstream to generate travel speeds. These speeds can be averaged to compute travel times for specific periods (e.g., peak versus non-peak) or for real-time use through wireless communications. Several exploratory and pilot studies using LPR were conducted in the late 1990s and early 2000s. However, the current literature search and interviews with three state DOTs and two consultants reveal that LPR for travel time studies has become a somewhat dated approach, supplanted by other technologies, such as Bluetooth, for travel time estimation. The findings are summarized below. Since we could not locate any

agencies using LPR systems for travel time estimation, not all topics are addressed in this case study summary.

History and Current Context

In 1998, the FHWA's Travel Time Handbook presented an overview of travel time data collection methodologies to provide guidance to transportation professionals and practitioners in the collection, reduction, and reporting of travel time data (Turner, et al., 1998). LPR was identified as one of the primary strategies for travel time data collection. Other techniques included "active" test vehicles (i.e., floating cars), passive ITS probe vehicles (i.e., cellular phone tracking and GPS), and emerging and non-traditional techniques (i.e., aerial surveys, WIM sensors, video).

In the mid-1990s, the United Kingdom Highways Agency, through its National Traffic Control Center project, began using ALPR systems to collect vehicle flows and speeds every five minutes, 24 hours a day, and seven days a week to provide real-time traffic information (Dalgleish and Hoose, 2008). About this same time, U.S. agencies were also exploring the utility of LPR for this purpose through field tests and pilot evaluations. While Great Britain's use has continued, the research team could not find any U.S. transportation agencies that are currently relying on LPR for travel time estimation.

In the U.S., experience with LPR for travel time studies has mainly been in form of field tests that evaluated the effectiveness of various travel time data collection methods side-by-side. Volpe Center conducted field tests of several travel time data collection methods in 1993. LPR was tested in Boston, Massachusetts; Seattle, Washington; and Lexington, Kentucky (Liu and Haines, 1996). The ultimate goal was to develop a nationally uniform program of travel time data collection and reporting in support of congestion management. The evaluation ended with the conclusion that there was no best solution for capturing the desired information. The weaknesses with LPR included problems with data collection and processing accuracy. In 1995, the Volpe consultant was contracted by Washington State DOT to perform surveys of travel times for two HOV corridors in Seattle (Woodson et al., 1995). It concluded that significant post-processing efforts were needed to improve license plate matching results. In 2010, Seattle DOT announced it was the first city in the nation to use LPR on city streets for travel time estimates. By 2013, it had begun the process of replacing LPR with lower-cost Bluetooth readers.

In 1996, the Center for Urban Transportation Research demonstrated LPR use for the collection of traffic data (including travel times) for the Hillsborough County congestion management system in Florida. The evaluation determined that the method offered substantial time savings, but that it had high equipment costs (Turner et al., 1998). In 2008, Florida DOT conducted a small pilot of LPR use on I-10 in Tallahassee to generate travel time estimates. The agency already owned the units being used for commercial vehicle enforcement. After the pilot, LPR was never widely implemented for cost reasons. Now the agency uses location data from a private sector data aggregation firm (i.e., HERE) and Bluetooth for travel time estimation. In 2000, Oregon DOT led the Frontier Travel Time Project, which was a demonstration project for travel time and incident information on rural highways. LPR was selected as a test technology. The study determined that LPR data could be used to present real-time travel time estimates to drivers on the road (Bertini et al., 2005). However, recent communication with Oregon DOT indicate that the agency does not use LPR for travel time estimation; only for enforcement purposes at scale sites by the Motor Carrier Division.

In 2004 and again in 2009, the Maryland State Highway Administration contracted with the University of Maryland to assess LPR system reliability for use in travel time estimation. The 2004 study revealed that the LPR system under-performed – it produced a low match rate at a high cost (Chang and Kang, 2005). The 2009 study found that overall performance of LPR technology had improved over the years. While the research was positive, the Maryland State Highway Administration never pursued LPR use for this purpose due to the departure of key individuals.

Virginia DOT previously used LPR for travel time estimation, but now has a contract with INRIX, a private-sector data aggregation firm, for crowdsourced data, and typically uses this and other sources for travel time – not LPR.

Information about LPR System

Because ALPR systems require high-quality video with specific lighting and plate size specification, there are high equipment costs, as well as extensive training and technical knowledge requirements. Most agencies have not purchased equipment. In the pilots and evaluations conducted, agencies preferred that vendors or consultants perform the video collection and processing activities.

Data Storage and Retention

Since the research team could not locate any agencies using LPR systems for travel time estimation, it was not possible to uncover any current information on data storage and retention practices. However, the FHWA travel time data collection handbook advised that after license plates have been matched and travel times computed, all records should be destroyed or deleted to alleviate potential privacy issues (Turner et al., 1998). In the small pilot conducted by Florida Department of Transportation (FDOT) in 2008, LPR data was destroyed once the travel time was computed, immediately after a license plate passed the second reader. This practice also obviated the necessity to comply with open records requests.

Technical Issues

Cost is a significant barrier to LPR use for travel time estimation, especially when compared to newer technologies. For example, in order to instrument a four-lane arterial, a minimum of eight sensors is needed (four at each corridor location, two in each direction). Sensor prices, around 2010, averaged $10,000 each, resulting in an $80,000 price tag to cover a four-lane arterial (Wang et al., 2011). In comparison, for example, Bluetooth sensors are much less expensive and simpler to use. Each device equipped with Bluetooth traveling along a roadway (e.g., smartphones, on-board receivers) uses a unique electronic identifier known as a Media Access Control (MAC) address. These are anonymous, and not tied to a specific individual. Bluetooth MAC addresses can be anonymously detected at multiple points by Bluetooth readers, which are relatively easy to construct and customize. MAC addresses are matched between each Bluetooth reader to estimate travel times.

Privacy Issues

The matching of license plate reads at two different locations and points in time does not produce PII. However, an LPR does record license plate numbers, and potentially camera images or video of vehicles, which could be used to identify vehicle owners by cross-referencing motor

vehicle records. For this reason, for example, when conducting a small pilot, FDOT used only the last 3 digits of the license plate and dropped the remaining characters and associated data. Even so, depending on the implementation, drivers may be identified by video or camera images. That said, researchers had no indication from the case study interviews that LPR was no longer being used by agencies for travel time estimation because of privacy reasons. Instead, it was supplanted by less-costly and easier-to-use sources of the information.

Summary of Travel Time Estimation Use Case

LPR performed comparatively well in evaluations over the past two decades. However, interviews with consultants and state DOT staff indicated that though the LPR system technology has improved in its collection and processing accuracy, it has been overtaken by newer technologies, (e.g., Bluetooth, GPS in probe vehicles, data aggregators like HERE and INRIX) that are thought to have significant cost and efficiency advantages. Privacy risks are inherent in the use of LPR for travel time estimation because personal information about an owner can be identified by matching a license plate against other databases. This risk did not appear to be the primary reason that LPR has been supplanted by other information sources.

ACCESS CONTROL

LPR technology can be used to control, monetize and monitor access to ports, parking facilities and other secured areas. LPR for access may be used in a facility that restricts, monitors, or charges vehicles entering and exiting a parking lot. In one variation of access uses, an LPR is mounted adjacent to an automatic barrier (e.g. gate, fence) at the entrance to a facility. It reads an approaching vehicle license and matches it to a list of authorized vehicles. A correct match will raise the barrier automatically. This system preempts the need for access card, RFIDs or other devices to be issued to new drivers.

Parking enforcement can also occur through a mobile LPR camera checking the plates of registered vehicle to determine if a vehicle is in violation. In this sort of use, for example, a customer submits his or her vehicle's license plate number to the enforcing agency, and purchases parking credit associated with the plate (University of Kansas, 2016). An enforcement officer then uses an LPR system, usually mounted on a vehicle, to scan license plates and check to see if the vehicle either has permission to park, or if purchased credit associated with the plate has elapsed. This sort of use is typically employed by a city, university, or other organization that manages parking for a large number of vehicles.

As a final variation, organizations can use LPRs for passive data collection and surveillance: monitoring vehicles that enter a controlled facility and checking plates against terrorism, abduction, or other wanted person HOT lists to ensure a facility remains secure. Ports or other security-oriented facilities are likely to employ LPRs for this sort of use.

The research team reached out to eight different organizations that seemed likely to use LPR systems to control access to parking facilities, including ports and universities. Only two of the organizations reported using LPR for access control, and most reported that they either did not use the systems, or did not respond to interview requests. The results of these interviews are summarized below.

History and Current Context

The use of LPR systems for parking enforcement dates to the mid-2000s, when in 2007, the city of Calgary, Canada, implemented a parking enforcement system called ParkPlus

(Calgary Parking Authority, 2016). System users input their license plate number when registering and purchasing their parking, and mobile enforcement vehicles equipped with LPR cameras automatically check the plates to determine if the associated vehicle has overstayed its purchased time. The ParkPlus system has reduced the amount of work city employees must perform by automating parts of the enforcement process. The innovative system, which is still in use today, was so successful it received the 2009 Institute of Transportation Engineers Best Practices award (Tannery Creek Systems, 2010). Since the mid-2000s, the popularity and use of LPR systems for parking enforcement and control has increased steadily, with several major cities and universities adopting them – although other parking methods, like magnetic strips and RFID chips, are still commonly used.

To better understand the current uses of LPR systems for parking enforcement and access control, the research team spoke with two organizations currently using the system: a port in a major southern city, and a state university. The organizations used the LPR systems in very different settings and manners, and as such, their challenges, benefits, and experiences were relatively unique.

The port's Chief of Police explained to researchers that they use the LPR system as a layer of security for their facility: following the events of September 11, 2001, Congress passed the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), which created several requirements designed to increase security at the nation's ports. The port adopted the use of LPRs as a means of monitoring access to their secured facility, and ensuring that high-risk vehicles – those associated with terrorism watch lists, abduction cases, or wanted vehicles – are identified. The port deployed the camera systems at three locations throughout the port: at both main entrances to the port, and at the passenger pick-up/drop-off zone. Vehicles are scanned as they enter the facility, and the scans are automatically checked against internally-stored HOT lists to identify potential high-risk vehicles.

The university uses its LPR system in a somewhat-different manner, although several characteristics of the use are the same. The university has two types of LPR systems: one set of fixed cameras is located at the entrance and exit of a gate-operated parking facility. The cameras scan vehicles as they enter and exit the facility; if a vehicle stays in the parking lot longer than the time paid for, the LPR system notifies the parking system that a violation has occurred, and an enforcement officer is dispatched to cite the vehicle.

The second system the university uses is mobile, mounted on transportation services vehicles, and used to check for scofflaws or locally-wanted vehicles on campus. The representative explained that if an individual has four or more parking violations with the university on record, they are designated a scofflaw in an internal database, and the mobile LPR unit checks license plates against it. If the LPR system identifies a scofflaw, the information is sent to the transportation systems supervisor. In addition, the university receives HOT lists from the local police department of wanted vehicles. The LPR database loads these vehicles into an internal database, which the mobile system also checks against. If a locally-wanted vehicle is identified on campus, the university notifies the local police department.

Information about LPR System

The port facility Chief of Police noted that they own three camera systems, and are in the process of purchasing a replacement LPR system. He explained that they had some technical challenges with the LPR systems, which are discussed in greater detail below. The port uses the LPR system primarily for surveillance and security purposes. The port receives HOT lists

containing the license plates associated with high-risk individuals, like terrorists or flight-risk criminals. LPRs strategically placed at the port's entrances, exits, and passenger pick-up/drop-off areas scan license plates and check them against the HOT lists.

The university owns eight cameras across the fixed and mobile uses. Two cameras are located at both the entrances and exits of the parking facility, for a total of four fixed cameras. Four cameras are also equipped for the mobile use, with two cameras affixed to the front and back of two vehicles. The university does not use LPR for its primary parking management system, which relies on hang-tags with a magnetic stripe, but uses the fixed LPRs to control a single parking facility and the mobile systems to apprehend chronic parking violators. At least two major universities have recently converted their parking management systems to LPR-based systems, including Texas Tech University and the University of Kansas, although neither of these organizations participated in case study interviews for this report (Texas Tech University, 2016; University of Kansas, 2016).

Data Storage and Retention

The port reported that, as a policy, they store all photography data from all 200 cameras at the port for 90 days. As new data accrues, the old data is automatically deleted from the system. The Chief explained that if there was a security incident, investigators could come out and view the data within 90 days.

The university reported that, per university policy, they store all LPR data for 30 days. The respondent explained that the university policy, which was developed by a committee of academics and community stakeholders, established a minimum storage time of 14 days and a maximum of 30 days. They picked 30 days for business purposes: if a customer challenges a violation, the transportation services would have a record to reference as evidence.

Data Security and Access

The Chief of Police at the port explained that the LPR data is deemed "security related," and as such, is subject to special protections. If personnel want access to the data, they must request it through the chief. The data is stored in a secured environment at the port, which is itself a highly-secured facility. The chief explained that no one is allowed unescorted access to the port unless they have both the correct credentials and a specific documented purpose for being there. He explained that none of the data is released to anyone outside the port, since the data deals with the security of the port – such data is protected under state law.

The port adopted the LPR system in response to the Maritime Transportation Security Act of 2002, and the SAFE Port Act of 2006, both of which created a variety of requirements designed to increase the security of ports after the terrorist attacks on September 11, 2001.

The university representative explained that their data is secured on a local server, and access is managed through a secured, password-protected, log-in system. Only individuals with a business need are granted access through their log-in credentials.

Sharing Data

The port made it clear that they do not share data with other organizations. As security-related data, state law prohibits it from being shared. They do not access the LPR systems of other ports or agencies. When checking vehicles against law enforcement HOT lists, the port downloads the data directly to their internal database, which does not require sharing data with

law enforcement. The chief stated that in his seven-year tenure at the port, he had never had another organization request their LPR data.

The university indicated that they share some data with the local police department in limited situations. As explained above, the university receives HOT list data from the local police department identifying the license plates of locally-wanted vehicles. If the university's mobile unit identifies a locally-wanted vehicle, they notify the local law enforcement to the positive identification. In addition, if a hit-and-run situation occurs in the parking facility with fixed LPRs, they can use the data to identify the offender, at which time they will send the data to the local police department. They do not share actual video data unless law enforcement specifically requests it. If the university's on-campus law enforcement requests the data, they will review the request, and share the data.

Technical Issues

The port reported that they had technical challenges with their existing camera system, but were in the process of purchasing a new system that did not have such limitations. The chief explained that the entrances to the ports have multiple lanes, but the current camera system did not have a wide enough lens to capture the vehicles across all lanes. He also mentioned that their camera system was set up to scan the front plate of vehicles, which can be problematic for commercial freight vehicles: in commercial freight, the plate on the front of a tractor may not correspond to the plate on the attached trailer. As a result of these issues, the port is in the process of acquiring new LPR camera systems.

The university reported that the largest technical challenge they experienced with LPR systems was the initial implementation. The representative stated that their situation and needs were unique, and the vendor's product did not meet their needs. As a result, they developed a custom application to interface with the LPR system.

Privacy Issues

The port did not report any specific privacy challenges. This could be a result of the relatively tight control over the data at the port. As discussed above, the port views LPR data as security-related, and as such, no one can access the data without the chief of police's permission. They do not share data with other agencies, and any HOT lists are downloaded from external sources and stored internally.

The university reported that they have received questions about their LPR system, but the interviewee did not feel these rose to the level of a challenge. They had curious individuals inquire about the cameras and their use, but no individuals have objected to the system. The university trains its staff on a regular basis about data security and privacy issues through online courses with quizzes to ensure retention of key elements. The university also formed an interdisciplinary committee to review audio and visual surveillance practices across campus, and the committee created policies and standards governing such practices.

Awareness and knowledge of applicable laws and regulations

The port interviewee seemed knowledgeable about state and federal laws governing security and data at the port. Throughout the interview, he referenced several state and federal laws that had influenced their use, including the SAFE Ports Act, and the Maritime Transportation Security Act of 2002, both of which address surveillance and security at the nation's ports.

Laws and regulations were not mentioned in the discussion with the university. The university representative mostly focused on internal policies, and ensuring its system was in compliance with these rules and regulations.

Neither the port nor the university transportation services reported spending a significant number of man hours to addressing privacy issues. When asked about the occurrence of privacy issues, both organizations reported few, if any, issues. The lack of public concern or privacy issues may be a factor in the limited deployment of resources.

The university established an oversight committee, separate from the transportation department, to oversee and review audio and visual surveillance activities across the university. The committee developed a policy governing audio visual surveillance, and reviews any requests to install such equipment.

Internal Policies

The port mentioned that they severely restrict data access; any individuals who wish to access the data must go through the port's chief of police.

The university representative emphasized that their use of LPR systems is consistent with a university policy governing the use of audio video surveillance technology (AVST). The policy was developed by a committee of academics and community stakeholders, and establishes "standards for installation, relocation, and use of approved AVST equipment and the circumstances in which recorded material may be reviewed or released." The committee responsible for creating the regulations also serves as an oversight body, and is charged with reviewing and approving any audio/visual surveillance.

Conclusion

Some transportation agencies currently use LPR technology to control and secure access to a facility, although there are other technologies commonly used like RFID or magnetic stripe cards. The uses, experiences, and challenges interviewees discussed all varied, although none reported significant privacy issues.

As an especially security-conscious organization, the port uses the LPR system primarily as a tool to increase security at the port. The LPRs monitor access to the port, and alert staff if a high-risk vehicle enters the facility. The port follows an internal policy and destroys data after 90 days, and does not share their data with law enforcement agencies. The port reported some technical challenges regarding their cameras failing to provide sufficient coverage, although they did not struggle with privacy issues.

The university transportation department uses LPRs to monitor and monetize access to a parking facility, and for mobile surveillance on campus. The university follows a detailed policy regarding audio and video surveillance on campus, which establishes standards requiring training, designates how surveillance equipment and related data can be used, determines when data can be shared or when it must be destroyed, among other provisions. The transportation department often referenced the university policy, and the representative knew it requires the data to be destroyed after 30 days. The only technical challenges reported had to do with customizing the software to fit the agency's needs.

COMMERCIAL VEHICLE SCREENING

LPR systems are used in many states for screening and inspection of commercial vehicles, and the enforcement of related regulations. It is one of several technologies that are

used to automate and increase the efficiency of commercial vehicle screening and the enforcement of safety and other commercial vehicle regulations. Interviews with three state DOTs and the Federal Motor Carrier Safety Administration (FMCSA) provided information on commercial vehicle screening uses of LPR, benefits and challenges associated with LPR use, and procedures and policies implemented that impact the privacy risk associated with the use of LPR data.

History and Current Context

Commercial vehicles are required to comply with a number of regulations imposed by the state in which they operate. Vehicles that operate in more than one state are also subject to federal laws, most of which are overseen by FMCSA. State and federal regulations for commercial vehicles include compliance with registration, safety, vehicle size, vehicle weight and operational requirements. These regulations are designed to increase safety, monitor the damage caused by heavy vehicles on roadways, and ensure that commercial vehicles comply with applicable transportation regulations.

LPR technology can identify trucks by license plate number and match the vehicle to existing state and federal motor carrier databases (some of which are public record) for registration information, safety profiles or violations. LPRs are found in virtual weigh stations and roadside enforcement systems designed to screen and inspect commercial vehicles for compliance with safety and other regulatory requirements. Two DOTs reported using LPR cameras on highway main lanes to screen passing commercial vehicles before they even enter a weigh station. FMCSA reported that LPR are more commonly used at inspection stations and weigh station ramps for sorting trucks.

The uses of LPR technology related to commercial vehicles include the following specific purposes:

- **Vehicle Screening** – Without LPR, vehicles may be screened manually by an enforcement agent who reads the license plate and/or USDOT number and compares it to a computerized database. The main benefit of LPR reported by one DOT is the ability to automate this screening process. An alternative method for electronic screening would be with a transponder system. Screening can be undertaken in roadway main lanes or as commercial vehicles enter a weigh station ramp. Electronic screening leverages LPR to identify a truck, link it to a database of motor carriers, and make an automated decision if a person needs to review this truck - without manual intervention.
- **Regulatory and Safety Compliance** – Commercial vehicles are screened for non-compliant permits, or expired registration, oversize and overweight violations, out-of-service orders or other safety violations. One DOT also noted that they oversee regulations related to the transportation of hazardous materials, such as expired hazmat placards.
- **Weight Enforcement** – Traditional and virtual weigh stations are designed to allow enforcement agencies to detect and sort passing trucks without requiring the vehicle to stop. This allows for selective screening so that only non-compliant trucks or trucks with a high possibility of being non-compliant are stopped for inspection. Compliant vehicles can be allowed to bypass the inspection station. Another DOT noted that LPR helps the agency understand and monitor the impact of trucks on the use and deterioration of state roads. Estimates of truck travel are used to evaluate the use and deterioration of state roads. Over-weight and over-size vehicle monitoring enables the DOT to verify their

estimates of truck travel and to better plan for the impact commercial traffic has on the roadways.

The main benefit of LPR is to automate and increase the efficiency of screening and monitoring passing commercial vehicles. By automating the screening process and allowing some trucks to bypass inspection stations, interviewees noted that these systems allow agencies to focus resources on carriers that require more attention than others.

FMCSA assists states with improving and expanding regulatory compliance and enforcement activities to "*improve safety performance and remove high-risk carriers from the Nation's highways.*" FMCSA provides research support, technical assistance and grant funding (FMCSA 2014). The Commercial Vehicle Information Systems and Networks (CVISN) is a FMCSA program to improve safety by helping states improve commercial vehicle safety, improve efficiency of electronic screening and simplify enforcement operations (CVISN 2016). CVISN grants are offered to states to deploy, operate and maintain information systems and networks for the CVISN program, including LPR systems. According to CVISN program documentation, several states obtained LPR systems through the CVISN federal grant programs in 2013 and 2014 (FMCSA 2016).

The three state DOT interviewees all reported the use of LPR readers for commercial vehicle activities. Commercial vehicle screening and compliance activities are sometimes managed in partnership with, or entirely by, law enforcement agencies such as departments of motor vehicles or departments of public safety. While the focus of this research is on transportation uses, and not law enforcement, researchers recognize that these activities may occur simultaneously. This is particularly true for commercial vehicle screening and compliance. The use of LPR to track stolen vehicles, enforce speed limits, conduct criminal investigations and other pure law enforcement operations are not included in this summary. Agencies interviewed did not suggest that LPR devices for commercial vehicle screening are used for law enforcement activities outside of commercial vehicle activity.

Information about LPR System

In a 2014 NCHRP study, LPR technology was identified as an innovative strategy for gathering truck activity data (Zmud, Lawson, and Pisarski 2014). It can support agencies in identifying commercial vehicles or companies with expired registration, out-of-service orders, improper certifications, and oversize/overweight violations. It can also be used for speed monitoring (Oliveira-Neto, Han, and Jeong. 2009).

All three state DOTs report that they own their LPR equipment. In one state, LPR equipment is owned by the DOT, while a vendor provides maintenance and support. In a second case, installation and training on using the equipment is provided by the vendor. One state currently has three LPR units, and is constructing at least four more sites. In another state, 20 of 22 virtual weigh stations include LPR technology. In the remaining two, images are still taken of the vehicles, but they do not use optical recognition software to read the license plates.

In weigh stations and enforcement systems, LPR is often combined with other technologies such as USDOT number readers, WIM devices, detection loops, video imaging to detect over-size vehicles and even magnetometer sensors.

Data Storage and Retention

Commercial vehicle LPR data may include or be linked to the following data:

- License plate numbers and photo
- Date, time and location
- USDOT registration number
- Registration, compliance and
- Truck size, weight and other defining features
- Photo of vehicle and/or surroundings

Commercial vehicle LPR data may be linked to USDOT registration information and local freight databases. In one state, an overhead photo of the truck, photos of license plate, OCR result, confidence interval of OCR result, and photo of USDOT numbers are packaged together under a unique ID. This is then linked to the truck weight, length, axles, axle weights, axle spacing as well as a date and time stamp. The data file is given a tracking number and a flag for weight violation. All the data are aggregated into a single transaction record and screened against a local database for potential violations of the vehicle or the carrier.

One DOT reported that data is only collected on vehicles that meet certain criteria, specifically Class 4 vehicles and above. No personal vehicles are tracked. The DOT launched a public awareness campaign to inform the public that they were not looking at personal vehicles, enforcement of speed limits, or even the drivers of commercial vehicles.

Data are stored according to the organization's guidelines: no data on personal vehicles, 120 days for commercial vehicle images, and 3 years for vehicle information. They reported that data are not used for general data mining or any other studies.

Data Security and Access

Agencies reported a range of policies to secure and manage LPR data. In no case was an agency able to provide a written policy that dictated their LPR policy. Some states have overarching privacy policies that provide guidance. A data retention period maximum was the most common control used for LPR data.

One state's commercial vehicle LPR databases are only accessible to staff in their enforcement and compliance division. Access for these users is further controlled with user IDs and password protection. This system of role-based security grants different levels of access based on a set of five or six role types (e.g. administrative). This is defined in the agency-wide user manual and data security standards.

Another state's commercial vehicle LPR data is managed by and accessible to their operations division. Operations staff must login with their employee number and password, and when they do, access information is recorded.

Data Sharing

One DOT reported that it does not share data with other agencies or departments, but are considering data sharing with other states for log-book verification: truck drivers log travel in different states, which could be confirmed by LPR readings from other states. The DOT has also received requests from other states to confirm whether a particular truck has passed through the state. They provide this information, and outside staff do not receive access to the actual

database. Data are not currently shared with traffic or law enforcement agencies because the cameras do not collect information on personal vehicles.

One DOT has a sharing agreement with partner agencies involved in commercial vehicle enforcement across the state to share data. Partners include the city DOTs and port and bridge authorities. Standard Commercial Vehicle Information Exchange Window data is shared, but each organization collects its data independently. They also accept requests for data from other vehicle enforcement agencies (only), for example for amber alerts.

Technical Issues

LPR systems do not reliably read all license plates. Interviewees suggested that LPRs capture 50 to 75 percent of all plates seen by the reader, and readability is decreased by snow, ice and grime. According to one DOT, higher rates suggested by LPR technology vendors do not account for plates that are thrown out due to irregularities.

Another challenge is that license plate numbers are linked to a motor carrier, but not necessarily to the company that owns the vehicle. Independent truck drivers may lease trucks with multiple companies per year, working for one carrier, so a USDOT number reader can be used to provide more detailed information. One DOT noted that LPR may be about 75 percent accurate alone, but as it is combined with other technologies at weigh stations, this rate increases.

Other technical difficulties were not reported. LPR devices are often introduced as one feature in a technology package to enable roadside enforcement and/or a virtual weigh station for commercial vehicles. Several DOTs reported that these systems are installed and maintained by a hired vendor. The vendor will train staff on using the equipment and provide maintenance.

Privacy Issues

The use of LPR for commercial screening purposes may raise fewer privacy concerns than uses that target personal vehicles for two reasons: commercial vehicles are highly regulated and screening is a codified approach to help ensure safety on public roadways. In this use case, scrutiny is placed on the activities of private motor carriers and commercial trucking companies – not individual citizens.

One DOT reported that the largest issue they faced was the initial public outcry when they introduced electronic screening on public roadways. A campaign was used to inform the public about their activities, and assured the public that personal vehicles and drivers are not targeted.

No DOT reported subpoena requests for LPR data. FMCSA has considered if there are PII information risks, but reported that this was not a significant concern because commercial vehicle license plate information is not linked to an individual. The license plate number is only linked to the motor carrier.

Awareness and Knowledge of Applicable Laws and Regulations

In one state, DOT staff were keenly aware of ongoing legislative debates related to LPR regulation. The privacy risks debated tend to focus more on law enforcement uses, but DOT staff follows the situation to stay abreast of changes that may impact their operations. Another DOT representative noted that even if an agency has a clear legal right to use LPR for commercial screening, it is also “good policy to develop good policy.” Agencies should strive for a balance between public safety needs, and real and perceived privacy issues from the public. It was also

noted that LPR use is limited by the respective laws in each jurisdiction. Data retention is not regulated federally, but each state can impose its own retention period. This matters more for some tasks than others. For example, verifying hours of service using e-screening data may only take about 8 days. A compliance investigation of a carrier could require 6 months of historical information.

DOT representatives did not report any significant efforts to specifically address privacy issues. All had considered the issue, but generally reported that this was not a major problem and commercial screening was described as a routine task. In one state, training is provided to teach the staff manning an enforcement station on how to coordinate the system generally, but this training does not focus on data privacy issues. Typically, the screening process is set up by the vendor, and the data is collected automatically and reviewed by staff to facilitate any manual screening or enforcement activities.

Internal Policies

The DOTs interviewed reported no written or formal guidance on privacy controls but each reported on specific guidelines to control data access and storage. Two DOTs reported that they only collect data on vehicles that meet a certain weight classification (Class 4 or above). One DOT also noted that commercial driver information is stored in a distinct database, and the existing databases for motor carriers and commercial drivers are not linked.

In one state, LPR data is only collected for Class 4 vehicles and higher. Images of Class 1-3 are taken, but once the filtering is applied, the images are immediately deleted. Class 4 vehicle images are captured and reserved for 120 days. At that time, the “overview” image is deleted; this is the actual photo of the vehicle, which could hypothetically be used to identify vehicle color, year, model, make, and possibly the driver. Although the DOT interviewee reported that it does not do this, it was noted that some jurisdictions may use this image for other purposes, like seatbelt enforcement. After 120 days, this DOT saves the license plate image itself, the system interpretation of the license plate number, and the related sensor information. This is saved for 3 years in the core system, and then remains stored in archives.

Summary of Commercial Vehicle Screening Use Case

LPR are one of several technologies used in many states to more efficiently and automatically screen for regulatory compliance and to enforce safety and other commercial vehicle transportation regulations. While DOTs reported that LPR devices are not entirely accurate or reliable, they are commonly being used to automate screening and enforcement activities. It was also noted that LPR readers are more effective and more useful when applied with other technologies – such as DOT readers and WIM scales.

Several procedural guidelines are used to control the privacy risks of LPR data use. Commercial vehicle screening in two states only records images of Class 4 or larger vehicles, which excludes all passenger vehicles. One state has a main lane LPR device that takes photos of all vehicles, but personal vehicles (class 1-3) are deleted immediately and discarded permanently. Data retention policies are also commonly instituted to control LPR data. Finally, two DOTs reported that they limit access to the data to a small department or group and use user identification and password controls.

A 2009 FHWA study on the operation of roadside enforcement technologies, including LPR, reported concerns from motor carriers related to data retention, usage, and privacy. FHWA noted three suggestions from motor carriers (Krupa and Capecci 2009):

- Institute 30 to 90 day maximum retention periods for data collected.
- Collect data only for "specific safety goals or other tangible goals."
- Protect important operational data, customer data and unique identifiers of carriers.

LPR use for commercial vehicle regulatory screening, compliance and enforcement occurs in a highly-regulated environment, and privacy risks are traditionally not a major concern. The regulation and monitoring of truck activity is a widely accepted public safety activity that occurs with or without the use of LPR. LPR and other technologies are primarily introduced in commercial vehicle purposes to lessen the burden of manual screening and enforcement – which can lead to savings for both the enforcing agencies and the commercial vehicle operators. Motor carriers are more willing to accommodate this automation because they recognize the efficiency gains they receive can translate into time and monetary savings.

TOLLING AND PAYMENT

Many state and local transportation agencies use LPR systems as a tool for tolling, often either for payment collection or enforcement purposes. Two state DOTs and three local toll operators provided information on experiences, benefits and challenges with the tool.

History and Current Context

The application of LPR to tolling began in the late 1990s in the context of open road tolling or electronic toll collection. The major advantage was that toll road users were able to drive through the toll plaza at highway speeds without having to slow down to pay the toll. This technology automates toll collection and enforcement by taking a picture of a license plate, translating the image into computer-readable alphanumeric characters, and checking this information against databases for account or address information (in the case of pay-by-mail or enforcement). LPRs are more efficient and less costly than using humans as the primary collection or enforcement mechanism; this, coupled with their ease-of-use made them an attractive tool.

The state DOTs and tolling agencies interviewed used LPR for toll collection on an ongoing basis, although the operational details varied. Both DOTs said LPR systems are primarily used for tolling, although they have used LPRs to accomplish other data collection purposes, including as a supplementary data source for travel time estimation, travel behavior analysis, and identifying candidates for surveys. One DOT also mentioned they use LPR to comply with Homeland Security requirements, by checking license plates of vehicles on ferries against national databases.

Local toll agencies used LPR for both toll collection and enforcement, and these systems were sometimes segregated for each of the two purposes. Once the plate is translated to readable characters, the toll system checks its user database to match the license plate characters with an existing account; if none is found, the toll authority checks the plate against vehicle registration databases to identify the correct mailing address to send the bill.

The enforcement process is similar, although the exact practices vary slightly among agencies. One local agency conducts periods of special enforcement, for example, where they used LPR to identify frequent violators and would inform local law enforcement partners to their violation and location on the facility. One of the DOTs stated they did not use it for enforcement, but the local law enforcement agencies did use the systems for this purpose.

Information about LPR System

In discussing hardware, the agencies frequently expressed how easy the systems were to purchase, install, and operate. They mentioned LPRs are a well-developed technology with many of the bugs worked out, and the vendors are professional and offer "great products."

All of the interviewees stated their organization owned the LPR equipment, with the exception of one DOT, who stated that they own the systems on two specific routes, own but do not operate the equipment on two other facilities, and eight other roads were privately held and operated. There was variation among the specific arrangements, with some being concessionary leases and others operating as public private partnerships. The DOT stated that they owned "quite a bit" of LPR equipment across their state. One local toll agency reported that they owned and operated the LPR systems on their entire network, with the exception of one geographically-distant road, which they outsourced to another agency.

Most toll systems, whether publicly or privately operated, work in the same way. All LPR components are in communication with and controlled by a computer called the "lane controller." Its database, through which a list a toll tags is maintained, is used to validate LPR reads and charge the customer's account. The information from each lane controller is passed on to a plaza host computer. Each plaza host computer is in constant communication with the central computer in a "back office" center that manages the accounts, enrolls customers and issues tags, processes the violations, handles all inquiries, and serves as the facility management center. Most toll road operators contract the back-office activities managed to third party vendors. The protection of PII by such vendors is typically covered by state statutes pertaining to data privacy. Because states vary in their requirements, as noted earlier in this report, the measures taken also vary by state. For example, Washington has very strict statutes designed to maintain user privacy, and vendors are required to adhere to the same data privacy standards as are imposed on banking institutions. In other states, there are no specific privacy laws. In these cases, customer privacy protections are typically explicitly written into the business agreements, along with any limited permitted uses of that data. Business rules vary greatly with regard to data retention and access practices, as noted below.

Data Storage and Retention

Data storage practices varied across agencies and use cases. The most consistent practice involved tolling, where agencies tended to keep data for long periods of time. One agency said they maintained data "as long as necessary" to complete the toll transaction, but the data would be destroyed once a charge was enforced. The maximum length of time this particular agency could keep the data was 30 days, although this period was limited to seven days for reads associated with a preexisting account. Several agencies deferred to state laws and maintained the information accordingly: one toll authority kept the data for as long as 4.5 years (but discards once the toll was paid), and another held the data for 7 years.

LPR used for enforcement had different practices, which again varied by agency. One DOT used LPR in real time, and data storage was limited to very short term due to storage capacity limitations. A local toll provider also stated that their law enforcement system does not store toll data beyond the initial read; the data was deleted after it was read.

Another state DOT using LPR for tolling and travel time analysis said they discard data immediately after it is collected for any travel time analysis, but store the toll read information for one year, and even could reuse the data. The agency stated that they might need to reference the data again in the future for billing disputes.

Data Security and Access

Several of the toll agencies pointed to state laws or industry standards guiding how they store and secure data. One DOT, for example, stores data according to state law, which requires data not be:

- Open to the public,
- Sold or used for sales, marketing, or solicitation purposes,
- Disclosed to any other entity except as may be necessary for the identification of violators or to a vehicle owner or operator as part of a challenge to the imposition of a civil penalty, or
- Used in a court in a pending action or proceeding.

The state DOT also mentioned that its system is access controlled to the relevant employees only, and they review and audit access records to ensure inappropriate individuals are not accessing data. Similarly, a local toll authority said they follow state statute requiring them to store the data for 4.5 years. It keeps toll information on separate, access-controlled networks where only the individuals responsible for operating and managing the system are granted access. Another local toll provider also mentioned that its system saves the information inside a CSV file, which includes the initial plate read image, the OCR transcription, and other details associated with the occurrence. All data is controlled and limited to relevant persons, per the Payment Card Industry (PCI) Data Security Standards (PCI 2016). The third local toll provider mentioned its automated system determines when a toll has been paid and deletes the appropriate file from its database. The database is also access controlled to the appropriate staff. A DOT stated that its system is sufficiently automated so employees do not have access to the original files, and never directly interact with the data.

Data Sharing

Four of the five agencies interviewed reported that they did not share tolling data outside of their organization. If the agencies receive a subpoena or other court order, they are legally bound to comply and provide the information, but many emphasized that short of this, they would not share data. The agencies with partnerships with local law enforcement agencies mentioned that there was no cross-sharing of data with the agencies.

The one agency that did report data sharing, did so under a contractual arrangement. The original agency operated toll roads and bridges for other local transportation agencies, and would share data about transactions on these facilities with the road or bridge owners. The original agency was the larger operator in the area, and operated a regional data center processing and handling customer accounts. This agency also emphasized that they only provided data to law enforcement under court order, per state law.

Technical Issues

The interviewees all extolled the ease of use, high level of automation, and simplicity of the tolling LPR systems. Some interviewees mentioned that despite the systems being easy to use, there were still occasional errors that required a human to review and confirm or correct the computer's interpretation of the license plate. One local agency stated that systems integration had been one of the largest challenges: older equipment, for example, took low quality images,

but the newer system required higher quality. Higher quality images requires upgraded networks cables and other related infrastructure. The organization was considering upgrading to wireless as a means of addressing the bandwidth constraints.

Privacy Issues

Both the state DOTs and local toll providers mentioned few privacy problems relating to LPR and tolling. Some agencies reported that individuals had requested information about themselves or others, which the agencies' were not legally permitted to supply. The agencies reporting this explained that laws in their states restrict their ability to provide information to the public, with one agency explaining that they could not provide information without a judge's order.

> *From a toll collection standpoint, we have statutes that make the data confidential information… This is not an internal policy… there is a statute relating to distributing information that governs this. Everyone knows, you don't give it [information] out. If you came in and asked for a plate, we would deny you. We have to comply with state law.*

The agencies reported that they were unaware of any occasions where data were used for data mining activities, with the exception of using the data internally to improve processes. For example, one state DOT and one toll agency said they used the data for quality control in analyzing and optimizing the LPR read accuracy. Another agency reported that the process was so highly automated that the automation, in combination with state statutes making the data confidential, had helped reduce any privacy issues.

Awareness and Knowledge of Applicable Laws and Regulations

The agencies frequently reported that state law or industry standards were often the guidelines they followed relating to protecting privacy. As referenced above, PCI standards and data storage or access laws influenced how toll providers and state DOTs handled their data. When discussing potential privacy-threatening situations, like requests for information or data, both state DOTs and local toll operators would cite state statutes that made the data confidential and not subject to open records request.

Due to the highly-automated nature of LPR systems and the state statutes restricting divulging information, the agencies did not report manpower or other resource constraints restricting their ability to properly address privacy.

Internal Policies

Agencies were asked about both specific training and internal procedures or guidelines for storing and handling LPR data. When asked if they had specific training policies on data privacy, two local tolling agencies said no, but they follow state laws; both DOTs reported that they were unsure; and the final local agency reported they did, but were ultimately unable to locate a copy of the policy.

When asked about specific policies governing how long data could be stored, two agencies referenced state laws governing how long data must be stored. One of the local toll agencies referenced PCI standards requiring data be held for seven years, one DOT reported that they store tolling data for 30 days at the roadside level, the image of the transaction for one year at the back office, and the other related transactional details for five years. A local agency

reported that they are using a current system that stores three images for an undisclosed time period, but the new system stores data according to the status of the transaction: if an invoice is closed out, the system deletes the information automatically, but it will store the transactional information until the transaction is settled.

Summary of Tolling and Enforcement Use Case

State and local transportation agencies commonly use LPR systems for toll collection and enforcement because it reduces man-hours and saves agencies money. Open road tolling is current state-of-the-practice. They reported few technical issues with the equipment, characterizing it as well-developed technology. The agencies reported they often follow state laws when determining how long to preserve data, although the length of time data could be maintained varied widely based on state law. Other agencies mentioned their adherence to PCI standards as helping ensure data privacy and security protections. Agencies often referenced an organizational culture and ubiquitous knowledge of the issues pertaining to data privacy protections.

TRAVEL BEHAVIOR ANALYSIS

Travel behavior is the study of how people or goods move from point A to point B. Travel behavior studies collect data on where, why, how, and when travel is done. Travel behavior studies are an important tool for state, regional, and local transportation planning and policy making because data collected are used as inputs to travel demand forecasts. Interviews with two state DOTs, two MPOs, and three consultants provided information on travel behavior analytic uses of LPR, benefits and challenges associated with LPR use, and procedures and policies implemented that impact the privacy risk associated with the use of LPR data.

History and Current Context

Historically, the collection of travel behavior data from various populations of interest (e.g., households, employees and customers of commercial establishments, commercial vehicle operators, and visitors) was labor intensive. Teams of field researchers stopped drivers along roadsides, boarded buses and trains, or visited people in their homes or commercial establishments to ask questions about origins, destinations, purposes, modes, and times of travel. Technology improvements led to more cost- and time-effective data collection by automating certain tasks that were once conducted manually. As noted in the report introduction, beginning in the mid-1990s, LPR began to be used for travel behavior surveys that involved identifying a subset of vehicles using a particular transportation facility to gather information on occupants' origins and destinations as well as other information about the trip for which the facility is being used. Since that time, LPR has been commonly used to conduct external station surveys (although it has been applied in one-off studies of vehicles using a particular facility or parked at specific location of interest). External station surveys involve identifying a subset of vehicles using a particular transportation facility to gather information on occupants' origins and destinations as well as other information about the trip for which the facility is being used. LPR technology was typically applied to replace roadside intercept survey methods. Such intercept interviews with sampled vehicle drivers were conducted at interchanges on or near freeway exit ramps and on the shoulders of the freeway main lanes (Hard et al., 2006). Commercial vehicle drivers could also be intercepted and interviewed at rest areas, weigh stations, and truck stops. While quite common in the 1970s–1990s, safety and congestion concerns prompted states to

discontinue roadside interview surveys and to employ alternative methods such as LPR, which could identify vehicles and through a license plate match, identified registered owners who could be sent a questionnaire through the mail.

External station surveys are a significant component of the suite of travel behavior surveys (i.e., household travel survey, commercial vehicle survey, workplace survey, transit-onboard survey) used for travel demand forecasting. External related travel can have a significant impact on modeled vehicle miles traveled (VMT). External station surveys are used to determine the number of vehicle trips that originate outside the urban area and continue through the urban area without stopping (external-external trips), as well as trips that originate inside the urban area but depart the urban area and trips that begin outside the urban area but travel to a destination inside the urban area (external-internal trips). There are generally two types of LPR-based techniques that are used: license plate match and a license plate match with a mail-out/mail-back survey.

The license plate match involves capture of the license plates of vehicles with time stamp at two or more survey locations and then matching them to identify vehicle movements between the different locations (e.g., external-external, external-internal). The match method does not involve the capture of any PII (e.g., name and address of registered owner, specific origin and destination information, trip purpose). Only anonymous information is needed to perform the license matching: license plate number, state of registration, time of day when plate was recorded, and direction of travel; however for the matching to be most effective all of the survey locations should be recorded on the same day. This means placing the LPR cameras at a significant number of locations, which can be extremely costly. As one of the consultants mentioned, LPR video cameras were deployed at less than half of desired locations in an external station survey for the Omaha/Council Bluffs metropolitan area due to cost implications. The sample of captured video license data was used to estimate resident/non-resident apportionment at the non-video sites.[8] Another consultant said that even though equipment costs have come down with technology advancements, the high cost of data collection does dissuade some public agencies from employing this method. Even so, his firm conducts about 6–12 license plate matching surveys per year.

The license plate match with mail-out/mail-back method was a common application for LPR use in external surveys. Hard and his colleagues found the method used in 17 of 29 origin-destination type travel surveys implemented in the late 1990s to early 2000s (Hard et al., 2006). The survey method is executed in two parts. The first part is the same as the match method above. The second part includes querying the captured license plates against state motor vehicle records to obtain the address of vehicle registrants. In most cases, the license data was transmitted to the state DMV and then returned by the DMV with the needed address information attached. Then the vehicle owner would be mailed a survey questionnaire to be returned by mail.

The questionnaire typically contained items on trip origin, destination, vehicle occupancy, trip purpose, and other trip details. The survey also typically contained introductory language such as: *Your vehicle [with license plate number] was observed traveling on [specific*

[8] It should be noted that the original survey design for Omaha/Council Bluffs was a license plate match with mail-out/mail-back survey, but the state division of motor vehicles stated that matching to their state motor vehicle records to identify the vehicle owner would not be permitted. The DMV did agree to match to obtain the zip code of the owner and this was used to determine resident/non-resident status.

roadway] on a [specific date] at a [specific time]. If this was your vehicle, the "x" agency would like to ask you some important questions about your trip. The language, although required to verify that the correct vehicle owner was responding to the survey, sometimes raised concerns about government surveillance or tracing among members of the traveling public. While imposing greater privacy risks, this method collects more detailed information as data inputs for VMT forecasting.

In the past 10 years, both consultants and transportation agencies confirmed that the use of video mail-out/mail-back surveys has declined due many reasons including privacy, data collection cost, and cost/benefit due to low survey response rates. Privacy concerns have been expressed by the general public and politicians on the use of public records to obtain the identity of a vehicle owner traveling on a particular roadway. For instance, TxDOT drastically curtailed its use of video capture methods as parts of its statewide survey program in the 2005–2006 timeframe. License plate matching can be used as long as no state motor vehicle databases are queried and persons contacted. In 2016, because of privacy concerns, lawyers for Arizona DOT ruled out use of LPR as one of several technologies to be evaluated for collecting long-distance travel data. Cost concerns pertain to not only equipment costs but also labor costs: cameras typically have to be manned.

The low survey response rates were caused by three factors. First, some license plates are not read or recorded properly, and cannot be matched. Second, out-of-state plates require special consideration, because it is often uneconomical to send small groups of license plate data to several outside states. Third, many people do not respond to the mailing, because they may not wish to participate, or they may not have been driving the vehicle when the license plate was recorded.

The practice of how to conduct external surveys is also in a state of transition. Many external studies across the country have begun using newer technologies such as cellular data mining, Bluetooth, and GPS (primarily for freight) (Farnsworth and Hard, 2013). An MPO source mentioned that crowdsourcing of travel survey data on roadway links has not yet raised alarms of protecting privacy, as individual IDs are typically not included and the origins and destinations are not. Currently, his MPO does not use LPR for any data collection to determine travel patterns.

Information on LPR System

The use of LPR for travel behavior surveys was typically implemented by consultants (i.e., traffic data collection firms or professional transportation planning/engineering firms) who supplied both the equipment and the labor for data collection as well as the personnel for data processing and analysis. We could not find any information on agencies who owned LPR equipment for this purpose.

Data Storage and Retention

There are potentially two types of databases involved in these surveys. First, there is the database of captured license plates that also contains a survey location code, state of registration, day and time stamp, and direction of travel. If this is a license plate matching-only survey, this is the only database required. After license plates have been matched and proportions of external-external or internal-external trips have been computed, the common practice is to destroy or delete all license plate records – even though there is no PII associated. According to consultants, the typical practice is to keep the data for about 6 months to a year.

If this is license plate match with mail-out/mail back questionnaire, then the database of captured license plates is sent to the appropriate DMV for the purpose of obtaining the name of the individual (or corporation) the vehicle was registered to, street address, city, state, and zip code. The returned information is used to mail the registered owner a questionnaire. Once the questionnaires have been mailed, the license plate records are typically destroyed or deleted. An anonymous sample identification number is used to manage the mail-out and to track the mail-back

The second type of database is the database of survey data elements. This database is typically provided to the transportation agency sponsor. Data are anonymized with the sample identification number used as the data management controller. Consultants typically would retain the data for about 6 months to a year following the completion of the study; although some sponsor contracts might specify longer. Length of data retention is dependent upon the sponsors' policies, which vary from agency to agency. However, since travel surveys are expensive to conduct, they are typically executed about once every 7 to 10 year. This can place a burden on the agency having to retain the data for many years.

Data Storage and Access

Data are typically housed and secured on the server of the survey consultant until the data are delivered to the survey sponsor as a final deliverable. In the past there have been concerns about data security, such as whether data is weakly encrypted without following accepted standards or even encrypted at all. Fortunately, data management and control policies at transportation agencies have improved in the recent decades as data security and cybersecurity concerns become critical issues. A potential solution for data security is to house travel survey datasets at The National Renewable Energy Laboratory, which operates the Transportation Secure Data Center. This repository provides free access to detailed transportation data from a variety of travel surveys and studies while preserving the privacy of survey participants. Some sponsors have chosen to store their datasets long-term at the repository.

Data Sharing

To the knowledge of persons contacted for this case study, data are not shared with agencies outside of the sponsors. Law enforcement agencies may be contacted to inform them of LPR data collection in their jurisdictions but not to share any of the information. Our sources also said that law enforcement agencies have not requested access to travel survey data. One person postulated that it was because law enforcement is interested in real-time data, not data that takes time to be processed, cleaned, and reduced.

Technical Issues

Depending on the conditions, the LPR systems could correctly detect approximately 70–90 percent license plate matches. Weather conditions could be a significant factor in both accuracy and detection rates. Plate type is also a contributing factor. For example, Tennessee has over 140 different styles of vanity plates, and there are not unique numbers assigned to each type of plate. In some travel behavior applications, surveyors would manually use voice recorders along with LPR to both verbally record and photograph license plates at the same time. But problems with diction and with accurately seeing the license plate limited the voice recording strategy. Also problematic images have to be manually inspected to improve accuracy. For these

technical reasons as well as cost and privacy, LPR use for travel behavior analysis has been somewhat supplanted by other technologies.

Privacy Issues

Privacy risks are present when captured license plates are queried against motor vehicle records to obtain ownership and address information. The public becomes aware when a person receives a survey questionnaire in the mail. A small, but vocal, proportion express alarm to the survey sponsor or to elected offices about the way in which their license plate numbers were captured without their knowledge or consent. Public education or awareness campaigns prior to the survey execution tend to mitigate the concerns.

Privacy risks are lowered if the query is done by the state's motor vehicle registration office and the vehicle owners are not contacted. This was the approach used in the Omaha/Council Bluffs survey, in which the plates were queried only to identify zip codes (residency) of travelers along several major freeway corridors coming into and out of the area.

Awareness and Knowledge of Applicable Laws and Regulations

Most consultants were aware of applicable laws and regulations governing use of the data. Transportation agency staff was less aware of laws and regulations but were strongly aware of their agency's policy permitting use of LPR for license plate matching or for matching against state motor vehicle records. Agencies' concerns were based primarily on perceived public perceptions. Agencies expected the consultants to properly use and address privacy issues in data collection and database preparation.

Internal Policies

Most consultants who conduct travel survey data collection have policies on protection of respondent's personal information, destruction of records, and release of information. Many state and local transportation agencies are beginning to put such policies in place.

Summary of Travel Behavior Analysis Use Case

Travel behavior is a vital tool for state and local transportation planning and policy making. Studying how goods and people move from A to B provides the information required to make informed planning and policy decisions about how to allocate scarce transportation resources. LPR use for travel behavior analysis has been somewhat supplanted by other technologies – like Bluetooth and GPS – for technical, economic and privacy reasons. Securing data for the long time periods needed for travel behavior purposes can present challenges, although some entities have outsourced secure data storage to third parties. The interviews indicated inconsistent knowledge of laws and regulations, although organizations were familiar with internal data privacy protection policies.

CONCLUSIONS FROM CASE STUDIES

The issues involved in the application of LPR to the transportation uses, depend to a large degree on whether or not the application pertains to the routine collection of data. For instance, tolling, access control, and commercial vehicle screening are routine and ongoing uses of the LPR systems. Case study informants mentioned that the LPR equipment is typically their own, and that they are well-versed in its operation. These agencies have well-defined data storage,

retention, security, and access practices. Even though the practices vary by agency, state law often prescribes the specific practices. While well-aware of the privacy risks, the agencies mentioned few privacy problems. There is no indication that LPR would be supplanted by other technologies in the near-term for these transportation uses.

Other cases such as travel time estimation or use for travel behavior analysis have more isolated instances of privacy concerns. The LPR equipment is typically owned by consultants or vendors who would be under-contract to the transportation agency. While the consultants typically have well-defined policies for data privacy protection, the public agencies are less knowledgeable. In the case of travel time estimation, LPR has been largely supplanted by newer technologies that are less expensive and easier to apply, such a Bluetooth, cellular, and GPS. In the area of travel behavior studies, LPR has continued to be used for license plate matching studies, while its use for license plate matching with mail-out/mail-back is almost non-existent. The latter use entails contact with a respondent and informing him/her of the license plate capture and the match to personal information. This situation raises concerns about government tracking of personal mobility. With such public concerns, survey sponsors have tended to back off of the use. Newer technologies such as cellular data mining, Bluetooth, and GPS are being used more frequently.

In all cases, cost- and time-savings are the primary influences on the application of the technology. Accuracy could be negatively affected by weather, lighting, and other conditions; although accuracy of the reads has improved over the past two decades. Also in all cases, data sharing is not a common practice. Sharing with law enforcement is only done when the agency was under a legal requirement to do so.

CHAPTER 5: BEST PRACTICES IN PRIVACY PROTECTION

In the U.S., there is no single comprehensive national law that regulates the collection and use of personal information. Privacy protection is set by a patchwork of federal and state laws. As for LPR, while no state bans LPR use outright, several states heavily restrict its use. To guide transportation agencies in balancing between beneficial uses of LPR data and the protection of individual privacy, the research team has identified best practices when using these devices in a transportation context. These best practices should be understood as the minimum aspirations for an agency's policies, procedures, and controls. Due to the unique requirements of individual agencies and their differing geographies, uses, and experiences, no one set of best practices will be applicable to all organizations.

The review covered best practices and recommendations for protecting privacy put forth from the federal government, interest groups, and international organizations, including:

- The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Digital Global Economy" (White House 2012);
- NIST, "Guide to Protecting the Confidentiality of Personally Identifiable Information" (NIST 2010);
- Organization for Economic Co-operation and Development (OECD), "The OECD Privacy Framework" (OECD 2013).
- The International Association of Chiefs of Police (IACP) "Privacy Impact Assessment Report for the Utilization of License Plate Readers" (IACP 2009).

LPR systems are commonly used by law enforcement agencies, and as such, much of the literature surrounding their use focuses on law enforcement purposes. As a result of the dearth of transportation-focused literature to review, the research team turned to law enforcement recommendations, documents, and best practices, applying these from the broader perspective of data privacy as noted in the above bullets.

The team reviewed these best practices and recommendations to identify those that would applicable to privacy risks associated with LPR use. The list presented in Table 8 represents the research team's synthesis of best practices. The team also analyzed the interviews to identify and reinforce best practices. The case studies provide a source of anecdotes to illustrate how agencies operationalize these best principles and practices specific to LPR.

Table 8. Privacy Protection Principles for LPRs

Principle	Description
Transparency & Openness	Individuals should be able to acquire information about the collection, storage, or use of personal information.
Purpose Specification	Agencies should clearly and specifically state why they are collecting information. Any changes to the purpose should be clearly stated.
Data Minimization, Retention, & Use Limitation	Agencies should only collect the information that is both directly relevant and necessary to meet their objectives. Agencies should only retain information as long as is necessary to meet their objectives.
Data Quality & Accuracy	Agencies should strive to ensure data is accurate and high quality. Incorrect information can negatively harm individuals. Regular audits can help ensure the data are accurate.
Accountability	Agencies are responsible for complying with data privacy rules.
Security	Agencies must protect personal data with reasonable security measures to prevent loss, unauthorized access, or disclosure.

The following subsections describe these principles in detail, and provide illustrative anecdotes drawn from the interviews about their application for LPR. Each section also includes a brief checklist agencies can use to determine if each principle could apply to their LPR data collection activities. When reviewing, if one or more of the questions apply to an agency, the principle may apply to their operation. It is important to note that these items are best practices, and are meant as a guiding framework. The use cases for LPR data collection are broad and diverse, and some aspects of the principles may apply to certain uses, but not others. Agencies also can use the checklist to help inform their procedures with regards to each principle.

TRANSPARENCY AND OPENNESS

Transparency and openness are key principles. Agencies should notify individuals in their jurisdictions about the types of information they collect, including passive data collected using technologies such as LPR. Agencies should also explain how they collect the information, how it is used, disseminated, shared and protected. This principle encourages agencies to use plain language to explain their data practices, which helps individuals understand how their information is being used, and the risks these uses may create.

This principle is particularly significant if the information in question is personally identifiable. PII includes any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records. A single piece of data can be PII, provided it can be used to distinguish or trace an individual’s identity, such as a social security number. Likewise, merging multiple pieces of individually-innocuous data can become PII, even when the individual pieces are not (e.g, combining date of birth plus a personal address).

LPR data in isolation may not meet this standard, but when aggregated across multiple sources or matched with information from other databases, LPR can meet the standard of personally identifiable. Explaining how data is collected and used can help individuals understand why their information is needed, and this transparency and openness can help

legitimize these uses in the public's mind. It may serve to mitigate public perceptions of government surveillance or tracking of personal mobility.

There is no one-size-fits-all approach to providing notices of data collection activities. An important aspect of this principle is that the communication should be clear and understandable, and devoid of legal jargon. Agencies often use their public-facing website to explain the rationale and process of data collection. Publically displaying a project website on a variable messaging sign, sending notices to an affected community, or using an existing online customer account portal are all potential options for informing the public. For example, tolling agencies often use their customer account portals or user agreements to communicate about data collection and use.

In addition, notices need not be provided in every instance of collection where privacy has been addressed by prior or preexisting notices; however, notices need specifically deal with the issue of obtaining consent and explicitly state how the agency will consider that consent was obtained. For example, the following are four common methods used to obtain consent. The method for obtaining consent should be customized to fit the needs of the data collection context, while considering the severity of the privacy risks, as well as the data collection location and the agency's access to the individuals.

- Explicit consent —an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of personal information.
- Implicit consent — an individual's consent is implied by his/ her behavior relative to the data collection activity.
- Opt-out consent —an individual is given the option to decline consent
- Opt-in consent – an individual is provided a check-box which, if filled in by the user, indicates consent.

The method for obtaining consent should be customized to fit the needs of the data collection context, while considering the severity of the privacy risks, as well as the data collection location and the agency's access to the individuals.

In a passive data collection situation as is often the case with LPR, individuals may not be aware that their behavior is being observed and recorded, and obtaining permission typically is not possible. In this situation, the agency should take all steps necessary to protect the privacy and security of that information as required by state law and professional practice. If PII cannot be de-identified, the agency should delete the personal data or seek informed consent from the individual for any further use.

Principle Checklist:

1. Is your agency collecting information on individuals with its use of LPR?
2. Is the information considered PII: does it contain information that identifies an individual, or is the information linked with other information that can identify an individual?
3. Does your agency communicate to individuals in your jurisdiction about all data collection activities involving LPR systems?
4. Does your agency consider the manner in which consent has been obtained: opt-out, opt-in, implied, informed, or explicit? Do public notices communicate the method?

Answering these questions can help your agency understand if the principle of transparency applies to your data collection activity, and identify possible actions or tools to aid implementation. If answers to these any of these questions are "yes", then the principle of transparency and openness could apply to the data collection activity.

PURPOSE SPECIFICATION

This principle builds upon the transparency principle. Agencies should clearly and specifically state why they are collecting information, and under what authority they are gathering the information, when providing notices of LPR-related data collection activities. This purpose specification should be clearly articulated in writing in advance of starting a specific LPR data collection activity. Identifying the "purpose" creates a guiding framework for balancing data needs and privacy, and the documentation can be helpful for those who must answer the public's or media's questions about privacy risk. If the agency adopts new purposes, or changes the original purpose(s) for collection, these should be documented and clearly communicated to their constituencies as well. This information should be available to consumers at the time of data collection and throughout any continued uses.

As an example drawn from the commercial vehicle screening case study, when a camera was installed on a roadway for commercial vehicle screening, the DOT informed the public that its purpose was only to gather information on commercial vehicle activity. The DOT launched a public awareness campaign to inform the public that they were not looking at personal vehicles, enforcement of speed limits, or even the drivers of commercial vehicles. In the commercial screening case studies from this research, several DOTs set up a system where they immediately discarded the data they did not need (e.g., Class 1-3 vehicles since the DOT was looking only at Class 4 and above). By understanding the purpose of the data use, the DOT has avoided holding data that could be a privacy risk.

Privacy notices should be reviewed on a regular basis to ensure that the type of data collected and the intended uses have not changed. The actual data collection practices and technologies being used should be consistent with the commitments made to individuals in the jurisdiction and comply with evolving regulatory requirements. The privacy notices should also state any data sharing that will be done with third parties. This principle can apply to collecting identifying or non-identifying data, but is perhaps most critical when agencies collect sensitive and PII data.

During case study interviews, agencies noted that while they would occasionally receive requests for data, they would not share the information. Their purpose in using the data was very narrow, and they would not grant other entities access, unless they were legally compelled through subpoena or other court order. Some organizations inform the public about their data

collection activities, and the purposes behind such activities through existing customer portals or public-facing websites.

Principle Checklist:

1. Does your agency have a clear specific purposes for the data it is collecting?
2. Does your agency staff and the affected public understand the purpose or purposes for which LPR data are collected and maintained?
3. Does your agency typically limit the collection of personal data to only those items that are necessary to the research purpose, and ensure they are not used in any manner incompatible with these purposes?
4. Does your agency regularly audit the purposes for which LPR data are used?

Answering these questions can help your agency understand if the principle of purpose specification applies to your data collection activity, and identify possible actions or tools to aid implementation. If answers to any of these questions are "yes," then the principle of purpose specification could apply to the data collection activity.

DATA MINIMIZATION, RETENTION, AND USE LIMITATION

This principle requires agencies only collect information that is both directly relevant and necessary to meet their objectives. The agency should retain the information only as long as is necessary to meet its objectives. In addition, any personally identifiable or sensitive information should not be disclosed or shared, unless such uses are consistent with the purposes explicitly specified. Minimizing the amount of PII collected with LPR systems and the length of time it is stored can also reduce the severity of a data breach or other unintended data action, should one occur.

Transportation agencies often talk about collecting data once and using it many times; sometimes for some future unknown purpose. While this is efficient from a data acquisition perspective, it often means that agencies may collect more data elements than they might need for a specific purpose and keep it on hand longer than is necessary. This principle reminds agencies of the potential harm that could arise from collecting superfluous data, or retaining PII longer than necessary. To do so would be an unfair and deceptive practice. If an agency collects more than necessary, this could lead others to believe the agency will use it in ways that have not been communicated, putting privacy at risk.

During interviews, agencies often mentioned their focus on several aspects of this principle. Agencies, for example, often would point to their efforts to limit the amount of data they collect, how long they keep it, and only collecting the data they need. In commercial screening, agencies would only collect data from the heavy goods or commercial vehicles that were within their purview; other vehicles were automatically dropped from collection.

Another example was when an agency set its LPR system to only collect the last three digits of a license plate; for its purposes, this was all the information needed. Limiting collection to only the necessary information enabled the agency to reduce privacy risks.
Finally, some agencies reported that they would not share information with outside entities unless legally compelled through a subpoena.

Principle Checklist:

1. Does your agency collect information on individuals: sensitive, PII, or otherwise?
2. Is your agency clear about the specific LPR data to be collected and the databases to which it might be linked?
3. Could individuals be harmed if the information collected by your agency is not properly protected from loss?
4. Does your state government mandate how long information can be stored?
5. Does your agency have procedures to separately store or remove identifiers from data records once they are no longer needed?
6. Does your agency have contracts in place to ensure that subcontractors provide an appropriate level of protection?

Answering these questions can help your agency understand if the principle of data minimization, retention, and use limitation applies to your data collection activity, and identify possible actions or tools to aid implementation. If answers to any of these questions are "yes", then the principle of data minimization, retention and use limitation could apply to the data collection activity.

DATA QUALITY AND ACCURACY

Agencies should work to ensure the data they collect and use are accurate and of high quality. Explicit quality checks should be performed. In addition, agencies should allow individuals the opportunity to correct any information about themselves that may be incorrect if data are used in an ongoing manner, such as for tolling or commercial vehicle screening. This principle is closely linked with the principles requiring accountability and openness.

Inaccurate data can harm individuals, by – for example – erroneously billing an individual, which could occur in a tolling context. If a vehicle is sold, and the new vehicle owner incurs tolls, those charges could be sent to the original owner if a connected database is not updated to reflect the new owner. In travel behavior surveys with a mail-out/mail-back option, the erroneous identification of a vehicle being sited on a particular road at a particular time can result in embarrassing or more-threatening situations. Taking steps to ensure databases with personal information are up-to-date and high quality can reduce the likelihood of these or similar incidents. Allowing individuals to verify their personal information, and request it be corrected if inaccurate, provides a form of redress and can minimize harms from inaccurate data.

Some agencies mentioned that data accuracy can be a concern with LPR systems. Certain lighting conditions, like those that commonly occur during dawn and dusk periods, can reduce the accuracy of plate reads. These agencies mentioned that their LPR systems worked on a probabilistic basis: if the computer did not meet a certain confidence threshold when attempting to read a plate, a human would manually review what the computer saw and interpreted. This sort of human intervention was more expensive, but helped to ensure the quality and accuracy of their data systems. This step reduces the likelihood an individual will be harmed by low-quality or inaccurate data.

Principle Checklist:

1. Does your agency collect information on individuals: sensitive, PII, or otherwise?
2. Does your agency routinely collect and use LPR data pertaining to the same individuals?
3. If the data your agency has collected is incorrect or inaccurate, is there potential to harm individuals?
4. Does your agency have procedures for handling access requests from individuals? Do these include procedures for responding to requests in a reasonable period of time?

Answering these questions can help your agency understand if the principle of data quality and accuracy applies to your data collection activity, and identify possible actions or tools to aid implementation. If answers to any of these questions are "yes," then the principle of data quality and accuracy could apply to the data collection activity.

ACCOUNTABILITY

The principle of accountability requires that agencies be responsible for ensuring they comply with data privacy principles. Written rules and procedures should define internal policies governing the use and disclosure of personal data, including data collected via LPR systems. Internal policies should be consistent with local privacy and data protection laws, and should be reviewed periodically to keep up with evolving regulations. Agencies should also hold their employees accountable for upholding the privacy principles.

An agency is accountable when there is an entity responsible for checking to see if they comply with the rules; this is often a third party auditor or can even be a law enforcement agency. During the interviews, some agencies referenced third parties that would audit their records to ensure they were in compliance. One agency mentioned that they had to report their LPR use to a state legislative oversight body, for example. Several agencies were required to adhere to certain principles, like destroying data after a given time period, under a state law. Such legal requirements, coupled with regular reporting or auditing, can also create accountability in the system.

Tolling agencies also, for example, would commonly point to the PCI Security Standards that create a variety of requirements on an entity collecting payment through credit cards. The PCI Data Security Standards are a set of requirements instituted and regulated by the PCI Security Standards Council. The Security Standards Council is a consortium of major card brands including VISA, MasterCard, American Express, DiscoverCard, and JCB International Credit Card Company. All organizations that process, store, or transmit payment card data must comply with PCI security requirements or be fined and/or risk losing their ability to process credit card payments. According to the PCI SCC website, penalties are not openly discussed nor widely publicized. These standards provide an additional level of accountability: if an agency does not comply with these standards, it can lose its ability to process credit card payments.

Principle Checklist:

1. Does your organization collect information on individuals: sensitive, PII, or otherwise?
2. Does your agency have defined internal policies governing the collection of data and the use and disclosure of personal information?
3. Are your agency staff aware of those rules and trained in how to implement the procedures?

Answering these questions can help your agency understand if the principle of accountability applies to your data collection activity, and identify possible actions or tools to aid implementation. If answers to any of these questions are "yes," then the principle of accountability could apply to the data collection activity.

SECURITY

The security principle requires that agencies must protect personal data with reasonable measures to prevent loss, unauthorized access, or disclosure. Determining which security measures are reasonable will vary depending on the data collection methods, data types, and other variables. Agencies should assess their specific situation, and conduct security and privacy assessments to determine which practices are reasonable and appropriate. The use of appropriate security safeguards to provide necessary privacy protection includes:

- Physical measures: restricting access to LPR hardware and software systems
- Technological tools: passwords, encryption, firewalls
- Organizational controls: limiting access, staff training, agreements with subcontractors and consultants.

The security policy should also include a procedure for dealing with a potential data breach in which personal data are disclosed. Individuals whose data have been disclosed must be notified if the disclosure exposes them to some risk and steps should be taken to protect against that risk. The International Organization for Standardization (ISO) 27001 is a recognized information security standard upon which a thorough security policy can be based. It comprises information security standards published jointly by ISO and the International Electrotechnical Commission and provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series). It is applicable to organizations of all and sizes and encourages them to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.

During the interviews, agencies commonly mentioned a variety of security measures to protect sensitive or personal data. Perhaps the most common method was the use of role and credential-based security. This practice entails agencies granting access to sensitive data only to members of the staff that need the access, and restricting this access through computerized credentials. For example, an individual that needs access to sensitive information would be granted rights through his or her computer log-in information, while individuals whose jobs did

not require it would not be granted such access. The application of technological controls, like encryption, was a much less typical practice.

Principle Checklist:

1. Does your agency collect information that should not be released publically, like PII or sensitive information?
2. Does your agency have security protocols in place for each data set that protect against loss or unauthorized access?
3. Will individuals be harmed if information collected by your agency is not properly protected from loss?
4. If a data breach occurs, does your agency have procedures in place for timely notification of affected individuals relating to a potential data breach?

Answering these questions can help your agency understand if the principle of security applies to your data collection activity, and identify possible actions or tools to aid implementation. If answers to any of these questions are "yes," then the principle of security could apply to the data collection activity.

CHAPTER 6: CONCLUSIONS, RECOMMENDATIONS, AND SUGGESTED FUTURE RESEARCH

CONCLUSIONS

This study examined privacy risk in transportation uses of LPR, and potential practices for minimizing that risk. The use of LPR technology for transportation purposes is not new: applications stem from the 1990s as means of more efficient data collection, improved data quality, and reduced costs. LPR, like other new technologies, was viewed as a "technological fix" for the cost and time challenges associated with capturing required information for transportation planning and policy making. However, even at the time, an opposing perspective viewed LPR as a "big brother-like" force with negative implications for individual privacy. Privacy is defined as the capability of individuals to determine for themselves when, how, and to what extent information about them is communicated to others.

Many of the negative perceptions related to LPR use come from its increasing use among law enforcement, and concerns about their purposes and who has access to the collected information. Such concerns have been raised by privacy advocates such as the ACLU, and are tied to governments' ability to track and reconstruct individuals' movements across space and time without their knowledge or consent. A close look at public opinion trends indicated that people are growing more concerned (not less) about government surveillance, security breaches, and individual data privacy. While there could be transference of concerns about law enforcement use of the technology to the transportation context, this study did not reveal this to be a significant issue. This research revealed a decreasing application of LPR for some transportation purposes such as travel behavior, but most often this was because LPR was supplanted by newer technologies, such as Bluetooth, GPS, or cellular data mining.

Privacy Risk and Transportation Uses

Privacy risk is tied to the likelihood of PII disclosure and the magnitude of harm that might result. PII is information that – by itself or in combination with other information – can identify, locate, or distinguish an individual. Examples can include names, addresses, social security numbers, credit card numbers, and precise geographical locational data. Five transportation uses of LPR were identified in this study: travel time estimation, access control, commercial vehicle screening, tolling and payment, and travel behavior analysis. Of these use cases, two were deemed higher risk: tolling payments and travel behavior analysis. Payment uses may link vehicle data from LPR to an individual user account that includes financial information. Financial information contributes to a higher possibility of a problem occurring because of the opportunity for fraud, identity theft or economic loss. However, case study interviews revealed that tolling agencies appeared to have defined policies, practices, and industry standards protecting their customer data.

In contrast, travel behavior analysis involved a high potential for harm because it was the use most likely to incorporate detailed information about the individual and his/her behaviors. The harm increases as individual actions are recorded at multiple locations and times, making it possible for an individual's actions to be tracked. While the consultants who routinely conduct the travel behavior studies have widely implemented data protection policies, the transportation agencies who sponsor them were less knowledgeable of their responsibilities for data protection and security; although awareness is growing. There has been a discontinuance of LPR studies

involving mail-out/mail back surveys. This has been largely due to vocal public concerns that reached the media or public officials.

Commercial vehicle activity, which may be operationally similar to passenger uses, were a lower privacy risk because the industry is highly regulated and, although a driver is a private citizen, the activities of the driver and the vehicle are associated with a commercial operation.

Legal Issues

While privacy risks are a salient concern, legal use of the technology is also a pressing issue. In the U.S., there is no comprehensive national legislation regarding personal data protection generally, or use of LPR systems specifically. While most states have enacted some form of privacy legislation, only 12 states have enacted legislation specifically pertaining to the use of LPR systems. In none of these states is the use of LPR banned or prohibited. However, several states heavily restrict its use. Several states have measures in place that restrict who can use LPRs and for what purposes (e.g., Arkansas and Maine). Most of the state laws cite restrictions on data use and sharing, and place requirements on data destruction. However, indicative of the interstate variance, data destruction requirements range from 14 days to 1095 days. Specific transportation uses are rarely, if ever, mentioned in the legislation.

At the judicial level, the Fourth Amendment has long been considered the most relevant article of the Constitution protecting citizens' privacy. It has at its core the security of one's privacy against arbitrary intrusion by the government. Unfortunately, advances in Fourth Amendment doctrine have fallen behind rapid progress in modern information technologies, such as LPR systems that seem to conflict with individuals' expectations of locational privacy. Recent U.S. Supreme Court decisions on individuals' locational privacy have been conflicting or left key questions unresolved (Gierlack et al., 2014). As this issue is becoming more prominent in the public discourse, the research team holds that it is difficult to predict exactly how the Court will resolve Fourth Amendment issues raised by LPRs in the future.

RECOMMENDATIONS

The implementation of the best practices presented in this report will serve to mitigate privacy risks associated with LPR use. While the practices apply to data privacy protection collected via any means, LPR systems fall into a special category of modern data collection technologies that have the potential to identify unique individuals. Thus, LPR application is likely to receive greater scrutiny in the future – certainly by law enforcement, but likely for other uses as well. The implementation of the practices can serve as insurance against future privacy-related challenges. The team consolidated best available guidance (i.e., White House, NIST, OECD, and IACP) into the following practices:

- **Transparency and openness**: Agencies should notify or otherwise communicate the types of information they collect and how that information is used, disseminated, and shared to individuals within their jurisdictions.
- **Purpose specification**: Agencies should clearly communicate why they are collecting information and under what authority; a change in purpose requires an update of the communication.

- **Data minimization, retention, and use limitation**: Agencies should only collect information that is necessary to meet their specified purpose, retain it for only as long as needed, and restrict its use to only specified purposes.
- **Data quality and accuracy**: Agencies should ensure that data are accurate, of high quality, and – when relevant – enable individuals to review and correct any information.
- **Accountability**: Agencies should define explicit policies and procedures for complying with data protection principles.
- **Security**: Agencies should protect personal data with reasonable measures to prevent loss, unauthorized access or disclosure.

Because of uncertainty in the future legal environment, and in how the public perceives LPR use for transportation purposes, the research team also recommends that agencies monitor evolving state legislation and judicial cases involving data privacy in general, and LPR use specifically as well as public opinion trends in their specific jurisdictions.

FURTHER RESEARCH

There is the need for more transportation-focused empirical research on data privacy. Privacy is a data issue that has grown in importance and complexity over the past decade. The transportation industry has been fortunate – technologies have been developed to capture and store more data and in more detail than ever before, at relatively low cost. Advances in data mining and analytics and the massive increases in computing power and data storage capacity have expanded, by orders of magnitude, the scope of transportation-related information available to businesses, government, and individuals. Transportation agencies have more data and different data. The risks associated with unauthorized collection or misuse of PII have increased.

These issues are not unique, or even new to transportation, having existed more prominently in social media and e-commerce for a much longer period. However, transportation professionals lack an evidence base that focuses on the legal, technical, and societal issues relevant to data privacy and data protection in the transportation context, in which there are both public and private interests in the data. The following are suggested topics for ongoing research.

- Public opinion research is needed that isolates and tracks privacy-related concerns specific to transportation and how those concerns may be affected people's transportation behavior. Tracking would help agencies monitor whether people are more or less concerned about data privacy and security issues and the context for those concerns.
- The focus of this research -- privacy risks of LPR technology -- is just the proverbial "tip of the iceberg" in transportation. LPR systems are being supplanted by newer technologies that are more cost- and time-efficient for many of their transportation uses. The examination of privacy risks of these newer technologies such as Bluetooth, GPS, and cellular data mining would inform agencies use of them. Questions include:
    - Who should own data of use to transportation agencies and what are sharing protocols?
    - How can transportation agencies ensure an adequate level of data literacy for handling new data streams and novel types?

    - What are the trade-offs in terms of open data / privacy protections that transportation agencies will need to make? And, what are their economic costs?
    - How can transportation agencies responsibly capture, use, and share geo-located personal information?

- In addition, connected transport (and not just DSRC-connected) is an area that may bring extensive risks to privacy, and should be the focus future research on data privacy in transportation. The annual automated vehicle symposium co-sponsored by the Transportation Research Board and the Association for Unmanned Vehicle Systems puts forth research needs statements on this topic. Recent statements have focused on best practices for consumer notices at various levels of automation and during testing, as well as best methods for handing data produced by automated vehicle systems.

REFERENCES

American Civil Liberties Union. July 2013. *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements.* Online. https://www.aclu.org/feature/you-are-being-tracked.

Bertini, R., M. Lasky, and C. Monsere. 2005. "Validating predicted rural corridor travel times from an automated license plate recognition system: Oregon's frontier project." In *Proceedings of the 8th International IEEE Conference on Intelligent Transportation Systems*, pp. 706–711.

Brooks, Sean; Nadeau, Ellen. May 2015. *Privacy Risk Management for Federal Information Systems*. Report #8062. Online. http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.

Burton, P., S. Crosthwaite, A. Simpson, and P. Billington. 2015. The Design and Implementation of a National Real-Time Travel Time on VMS Service. The National Traffic Control Centre, Birmingham, UK.

Calgary Parking Authority. 2016. *ParkPlus System.* Calgary Parking. Online. Accessed August 2016. https://www.calgaryparking.com/parkplus.

Chang, G.L., and K.P. Kang. 2005 *Evaluation of Intelligent Transportation System Deployments for Work Zone Operations*. Maryland State Highway Administration. Report No. MD-05-SP208B4H. Baltimore, Maryland.

Dalgleish, M. and N. Hoose. 2008. *Highway Traffic Monitoring and Data Quality*. Artech House, London, United Kingdom.

Eberline, A. (2008). Cost/Benefit Analysis of Electronic License Plates. Retrieved Jan. 20, 2016, from Arizona Dept. of Transportation: http://ntl.bts.gov/lib/30000/30600/30610/AZ637.pdf

Elizabeth River Crossings. 2015. *Pay by Plate Bill Payment*. ERT Customer Service Center. https://www.driveert.com/pay-by-plate/bill-payment/.

Farnsworth, S., and E. Hard. 2013 Metropolitan Area Planning Agency External Travel Survey: Summary Report, December 2013.

Federal Highway Administration. March 1998. *Travel Time Data Collection Handbook*. Report No. FHWA-PL-98-035. https://www.fhwa.dot.gov/ohim/tvtw/natmec/00020.pdf and https://www.fhwa.dot.gov/ohim/handbook/chap4.pdf

Federal Motor Carrier Safety Administration. August 23, 2016. *Commercial Vehicle Information Systems and Networks (CVISN)*. U.S. Department of Transportation, Online. https://www.fmcsa.dot.gov/information-systems/cvisn/commercial-vehicle-information-

systems-and-networks-cvisn.

Federal Motor Carrier Safety Administration. March 31, 2014. *About Us*. U.S. Department of Transportation. Online. https://www.fmcsa.dot.gov/mission/about-us.

Federal Trade Commission. 2012. *Protecting Consumer Privacy in an Era of Rapid Change*. Accessed on August 10, 2016, Available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Florida DOT. 2016. *All-Electronic Tolling…Paying a Toll*. Florida's Turnpike Enterprise. Online. http://www.floridasturnpike.com/travelerInfo.html.

Gierlack, K., S. Williams, T. Latourrette, J. Anderson, L. Mayer, and J. Zmud. (2014) *License Plate Readers for Law Enforcement: Opportunities and Obstacles.* RAND Corporation, Washington, DC.

Gillula, J., and D. Maas. January 21, 2015. *What You Can Learn from Oakland's Raw LPR Data*. Online. https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

Goldberg, R. (2016) "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities." Accessed on August 10, 2016, Available at https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

Gutierrez-Alm, J. (2015). The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law. Hamline Law Review, 38(1), 127-160. Retrieved February 4, 2016, from http://digitalcommons.hamline.edu/cgi/viewcontent.cgi?article=1054&context=hlr

Hard, E., S. Fransworth, D. Pearson, P. Songchitruksa, D. Spillane, and T. Forrest. (2006) *Evaluation of External Station Survey Methodologies for High Volume Locatio*ns. Report No. FHWA/TX-06/0-4869-1. Study performed in cooperation with the Texas Department of Transportation and the Federal Highway Administration. Access on August 25, 2016, Available at http://d2dtl5nnlpfr0r.cloudfront.net/tti.tamu.edu/documents/0-4869-1.pdf

Hermann, Jourdin (2015) "The Surveillance State: Do License Plate Readers Impinge Upon Americans' Civil Liberties?," Themis: Research Journal of Justice Studies and Forensic Science: Vol. 3: Iss. 1, Article 4. Available at: http://scholarworks.sjsu.edu/themis/vol3/iss1/4

International Association of Chiefs of Police (IACP). September 2009. *Privacy Impact Assessment Report for the Utilization of License Plate Readers*. Online. http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf

ITS International. October 2013. “Bluetooth and Wi-Fi offer new options for travel time measurements.” First published in ITS International September October 2013 as Getting the measure of travel time determination. Online. http://www.itsinternational.com/categories/detection-monitoring-machine-vision/features/bluetooth-and-wi-fi-offer-new-options-for-travel-time-measurements/

Krupa, C., and S. Capecci. June 2009. Truck Size and Weight Enforcement Technologies. FHWA-HOP-09-049. United States Department of Transportation - Federal Highway Administration. Online. http://ops.fhwa.dot.gov/publications/fhwahop09049/sec02.htm

Kumaraguru, P., and L. Cranor. 2005. “Privacy Indexes: A Survey of Westin’s Studies.” CMU-ISRI-5-138. Accessed on August 10, 2016. Available at http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf.

Lee, J. F., and J. Williams. 2014. *New Way to Utilize Remote Sensing Data*. Transportation Research Record: Journal of the Transportation Research Board, Vol. 2460, No. 2460, pp. 15–21.

Liu, T., and M. Haines. 1996. *Travel Time Data Collection Field Tests – Lessons Learned.* FHWA. Report No. DOT-VNTSC-FHWA-96-1. Washington, DC.

Madden, M. Pew Research Center, 2014, “Public Perceptions of Privacy and Security in the Post-Snowden Era.” Accessed on August 29, 2016. Available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Madden, M., and L. Rainie. Pew Research Center, 2015, “Americans’ Attitudes About Privacy, Security and Surveillance.” Accessed on August 10, 2016, Available at http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Merola,L.M., Lum,C., Cave, B., Hibdon, J. (2014) "Community support for license plate recognition", Policing: An International Journal of Police Strategies & Management, Vol. 37 Iss 1 pp. 30 – 51 Permanent link to this document: http://dx.doi.org/10.1108/PIJPSM-07-2012-0064

National Conference on State Legislatures. *Automated License Plate Readers: State Statutes Regulating Their Use*. February 2, 2015. Online. http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx.

National Institute of Standards and Technology (NIST). April 2010. *Guide to Protecting the Confidentiality of Personally Identifiable Information.* Report #800-122. Online. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

NuPark. August 2016. Online. http://www.nupark.com/.

Oliveira-Neto, F. M., L. D. Han, and M. K. Jeong. 2009. *Tracking Large Trucks in Real Time with License Plate Recognition and Text-Mining Techniques.* No. 2121, pp. 121–127.Transport for London. Congestion Charge. https://tfl.gov.uk/modes/driving/congestion-charge

Oliveira-Neto, F. M., L. D. Han, and M. K. Jeong. 2009. *Tracking Large Trucks in Real Time with License Plate Recognition and Text-Mining Techniques.* No. 2121, pp. 121–127.

Organization for Economic Cooperation and Development (OECD). 2013. *The OECD Privacy Framework*. Online. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Payment Card Industry (PCI) Security Standards Council. August 2016. *PCI Security*. Online. https://www.pcisecuritystandards.org/pci_security/

Rainie, L., and M. Madden. 2016. "American's Privacy Strategies Post-Snowden." Pew Research Center. Accessed on August 18, 2016, Available at http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Roberts, D., and M. Casanova. 2012. *Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement.* US Department of Justice, National Institute of Justice. Washington D.C. Online. http://www.theiacp.org/Portals/0/pdfs/IACP_ALPR_Policy_Operational_Guidance.pdf

Roper, E. September 19, 2014. *City Cameras Track Anyone, Including Minneapolis Mayor Rybak.* Online. http://www.startribune.com/aug-17-2012-city-cameras-track-anyone-even-minneapolis-mayor-rybak/166494646/

Tannery Creek Systems. 2010. *Calgary Parking Authority's ParkPlus with autoChalk awarded the 2009 Institute of Transportation Engineers (ITE) Best Practices Award for its ParkPlus System.* http://tannerycreeksystems.com/wp-content/uploads/2013/11/autoChalk-and-ParkPlus-Win-ITE-Innovation-Award-in-2009-Press-Release.pdf

Texas A&M Audio Visual Surveillance Technology Committee. N.D. *Audio Visual Surveillance Technology Operational Standards*. Online. Accessed August 2016. https://it.tamu.edu/files/AVST_Operational_Standards.pdf

Texas Tech University. 2016. *License Plate Recognition*. Online. Accessed September 2016. http://www.parking.ttu.edu/shared/lpr.

The Commercial Vehicle Information Systems and Networks Program, 2014. U.S. Department of Transportation, Federal Motor Carrier Safety Administration. May 2015. http://ntl.bts.gov/lib/55000/55000/55044/2014_CVISN_Annual_Report_Final_May_18_2015.pdf. Accessed July 25, 2016.

The White House. February 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Digital Global Economy.* Online. https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Transport for London. August 2016. *Congestion Charge.* Online. https://tfl.gov.uk/modes/driving/congestion-charge.

Turner, S., W. Eisele, R. Benz, and D. Holdener. 1998. *Travel Time Data Collection Handbook*. FHWA, Report No. FHWA-PL-98-035. Washington, DC.

U.S. Department of Justice. August 2009. *Project Seahawk*. Online. http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0118/n1-118-09-001_sf115.pdf

United States v. Knotts. 1983. 460 U.S. 276.

University of Kansas. 2016. *License Plate Recognition*. Online. Accessed September 2016. https://parking.ku.edu/license-plate-recognition.

Wang, C.P. and S. Nallamothu. 1997. *Basis of License Plate Recognition and a New Approach*. Congress on Computing in Civil Engineering, Proceedings, pp. 143-152.

Wang, Y., Y. Malinovskiy, Y-J. .Wu, and U. Lee. *Error Modeling and Analysis for Travel Time Data Obtained from Bluetooth MAC Address Matching*. Research sponsored by Washington State Department of Transportation, and Transportation Northwest. Report TNW2001-01. Accessed on August 15, 2016, Online. http://depts.washington.edu/trac/bulkdisk/pdf/782.1.pdf.

Westin, A. 1967. *Privacy and Freedom.* Atheneum Publishing. New York.

Westin, A. 2003. *Bibliography of Surveys of the U.S. Public, 1970-2003*. Accessed on August 11, 2016, Available at http://www.privacyexchange.org/iss/surveys/surveybibliography603.pdf.

Westin, A. 2001. "Opinion surveys: What consumers have to say about information privacy, S.o.C: The House Committee on Energy and Commerce, Trade, and Consumer Protection," http://energycommerce.house.gov/107/hearings/0508200/Hearing209/westin309.htm

Woodson, J.B., P.W. Shuldiner, and S.A. D"Agostino. 1995. *Automated Video-based Survey of Travel Times in HOV vs. General Purpose Lanes*. Report No. WA-RD 399.1. Transformation Systems, Inc., Washington State Department of Transportation, Olympia, Washington.

Zmud, J. and D. Edrington 1999. *Technological Innovation in External Travel Surveys: A Critical Assessment*. Paper presented at the 1999 Application of Transportation Planning Methods, Boston, MA.

Zmud, J., C. Lawson, A. Pisarski. 2014. *Making Trucks Count: Innovative Strategies for Obtaining Comprehensive Truck Activity Data.* NCFRP Report 29. Washington, DC: Transportation Research Board.

APPENDIX: INTERVIEW QUESTIONNAIRE

1. For which of the following purposes has your agency used data collected via LPR technology? Is your agency still using LPR-collected data for [each] purpose? IF NO: Why not?
    a) Travel time estimation
    b) Commercial freight vehicle screening
    c) Payments (toll, parking, etc.)
    d) Travel behavior analysis
    e) Other:
2. When LPR data are collected, are they typically used once and then discarded, or collected and used many times for different purposes? Why or why not?
3. What are main benefits to your agency of using LPR data?
4. What are the main challenges?
5. Does your agency own LPR equipment? IF NO, why not?
6. Does your agency train staff in using LPR data, in terms of proper handling in light of data privacy requirements, etc.? *If written training materials, can you provide to us.*
7. Can you give me an account of the last time LPR was used to collect data for travel time estimation? [Probes]
    a) Time frame (how long ago)
    b) Vehicles and motorists targeted
    c) Were any other state or local transportation agencies involved?
    d) What databases were the license plates matched against?
    e) Were LPR-collected data linked with other data?
    f) What were the main challenges in using LPR for this purpose?
8. In general, what are your agency's procedures or guidelines for storing LPR data, e.g., length of time, location? *If written document, can you provide it to us.*
9. After data are stored, are they sometimes used for general data mining?
10. Are they sometimes linked to other databases for use in separate studies?
11. Are there procedures or guidelines that your agency follows in terms of the linking of your agency's LPR data with other databases? *If written document, can you provide it to us.*

12. Does all staff have access to stored LPR databases or is access controlled in some way?

13. Does your agency have written procedures or guidelines in terms of who can access LPR data? *Can you provide it to us?*

14. Does your agency have access to the LPR databases of other departments or agencies?

15. Under what circumstances has your agency shared data from LPR systems with other agencies for traffic/law enforcement purposes?

16. Has your agency ever been subpoenaed to provide data for traffic or law enforcement purposes? What was the outcome?

17. What safeguards, if any, exist to prevent privacy data "bleed" between your agency and law enforcement agencies?

18. Has your agency run into any specific privacy issues or challenges related to the LPR data?

19. IF YES: How has the department managed these issues?

20. IF NO: What does your department do to ensure that there will be no privacy issues?

21. Has your agency done any specific activities to raise awareness and knowledge among staff of applicable laws and regulations governing use of LPR data?

Are there any other thoughts or comments that you would like to share before we wrap up? That's the end of my questions. Thanks very much for taking part in this discussion today; it was very helpful to us.