ETHICS OF GOVERNMENT USE OF DATA COLLECTED VIA INTELLIGENT TRANSPORTATION SYSTEMS

June, 2012

This document is a product of the Center for Automotive Research under a *State Planning and Research Grant* administered by the *Michigan Department of Transportation*.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The convergence of sensing, wireless telecommunications, and multi-media platforms have provided new opportunities for the development of a fully connected transportation system. Intelligent transportation systems (ITS) can provide real-time information related to traffic, travel time, travel behavior, and transportation asset management and performance. In addition to providing benefits to individual travelers, improvements in ITS-based data collection can help increase the overall efficiency of the transportation network and allow public transportation agencies to improve the management of their systems. While the deployment of ITS and connected vehicle applications can improve transportation system efficiency, safety, and traveler convenience, they also introduce ethical concerns and raise questions about tracking and privacy. As a prerequisite to deployment of ITS technologies, issues regarding the privacy and ownership of collected data will have to be addressed to the satisfaction of all parties, including government agencies, manufacturers and, most importantly, citizens.

The Michigan Department of Transportation (MDOT) is a recognized leader in ITS and connected vehicle technology. In this role, MDOT has identified the protection of citizen privacy in the collection, management, and use of ITS data as a high priority for both its own and the national ITS and connected vehicle programs. Therefore, MDOT asked the Center for Automotive Research (CAR) to examine the ethical issues surrounding ITS applications and legal ramifications of the State of Michigan's collection and use of data from such systems. This report catalogs the range of issues related to government involvement with ITS applications and data.

Appropriate governing mechanisms are needed to provide a balance between the interests of members of the public, government agencies, and businesses. The United States lacks an overarching information privacy law governing government agencies and private businesses. While there are federal and state laws that regulate the collection and management of personal information within government agencies, as well as laws that regulate consumer data use in specific industries, such regulation is a patchwork of legal provisions that has largely been left to individual states and the court system. While individuals widely cite the Fourth Amendment as providing a right to privacy, its implications for ITS and connected vehicle deployment are less than clear. Although historical court cases that have set precedents for the interpretation of the law, contemporary rulings are not always consistent and evolving technology could prompt changes in legal interpretations. Much of the state and national experience with ITS and connected vehicle technologies involves voluntary and private sector applications that have relied on voluntary self-regulation and the use of contracts.

This report provides specific recommendations on the ethical collection, management, and use of ITS data. Proposed recommendations prompted by the findings of this study include:

- Identify ITS data needs and select data collection techniques accordingly
- Determine participants' requirements and options for anonymity
- Balance the tradeoff between privacy and quality of ITS data through advanced data architecture
- Make participation voluntary for appropriate applications (such as connected vehicles, mileage-based user fees, and electronic tolling)
- Use market incentives to promote adoption where appropriate (such as in-vehicle technologies and early deployment of mileage-based user fees)
- Resolve equity issues using subsidies for installation of in-vehicle technology
- Coordinate outreach and education programs to enhance understanding of and support for various ITS applications
- Determine the governance and ownership of data collected using ITS applications

- Create public-private partnerships to collect, manage, and disseminate data collected using ITS applications
- Develop effective information technology strategies to mitigate risks associated with data security, privacy, and data sharing
- Integrate ITS data collection and information sharing policies into existing data management strategies

The privacy implications of ITS technologies are becoming a bigger concern for many transportation organizations and further assessment of privacy protection mechanisms is needed for both public and private sectors. Federal and state privacy laws lag behind ever advancing ITS technologies, but privacy laws are likely to evolve in response to these innovative technologies.

LESSONS FOR MICHIGAN

Although MDOT has already deployed many ITS applications and successfully dealt with associated legal and ethical issues, additional applications that are in varying stages of deployment and research also could be considered for deployment. New ITS applications will be increasingly advanced and data driven, thereby making it more important to mitigate risks associated with the new systems. MDOT should consider the recommendations contained in this report, as well as those outlined in other ITS principles documents referenced in this work. These recommendations and basic principles will help MDOT design systems, policies, and operating procedures that protect Michigan citizens and limit exposure to legal uncertainties, while at the same allowing the agency to manage and operate the state's transportation network effectively using ITS and to maintain its position as a national leader in the ITS field.

LESSONS FOR THE BROADER ITS COMMUNITY

Beyond Michigan and MDOT, the content of this paper is broadly applicable to other state DOTs as well as other government agencies, companies, and other organizations involved with ITS and connected vehicle technologies. A better understanding of the issues related to the deployment of such technologies could lead to more productive partnerships and broader deployment of ITS and connected vehicles across the nation.

I. INTRODUCTION

High quality transportation datasets on performance of the transportation system are essential to support public policy and investment decisions facing state departments of transportation. Traditionally, transportation professionals have relied on two data collection methods. One method is the use of travel surveys to analyze trip characteristics, such as start and end times, duration, distance, origin, destination, purpose, and mode. Another method is field- or infrastructure-based data collection using fixed detectors built in the pavement or radars and cameras along the road, to provide data on traffic volume, flow, and speed. The cost of deployment, communication, maintenance, and operation for field data collection is often very high.

The convergence of sensing, wireless telecommunications, including Global Positioning System (GPS) enabled mobile phones, and multimedia platforms have provided new opportunities for transportation solutions as well as alternative data collection methods. Some have suggested that the advancements in ITS and vehicle tracking technologies are possible replacements for traditional data collection methods, as they are able to provide information related to traffic, travel time, travel behavior, and transportation asset management and performance (Lwin and Murayama, 2011).

According to the United States Department of Transportation (USDOT) Research and Innovative Technology Administration (RITA), the location-based service (LBS) and real-time traveler information market has expanded greatly across the various modes of surface transportation in recent years (2010). In addition to the benefits it provides to travelers individually, real-time information helps to increase the overall efficiency of the transportation network and allows public transportation agencies to improve the management of their systems. Commercial vehicle probe data has also been widely used by private entities in order to enhance system-wide operations and develop advanced fleet management systems. One common data platform uses cell phone signal data to provide location, movement, and real-time traffic information. LBSs have enjoyed rapid increases in usage by transit providers. For example, real-time digital bus arrival information is now available to millions of Londoners via the Internet, smartphones or text messages. Two-way feedback between riders and providers by using riders' GPS enabled mobile phone location data is the key to supporting such services.

While ITS applications have positive effects on transportation system efficiency, safety, and traveler convenience, they also introduce ethical concerns and raise questions about tracking and privacy. Before successful deployment of ITS technologies can commence, issues of privacy and ownership of collected data will have to be addressed to the satisfaction of all parties – government agencies, citizens, and manufacturers. MDOT, a recognized leader in ITS and connected vehicle technology, has identified that protecting the privacy of citizens regarding the collection and distribution of ITS data is a high priority.

The purpose of this study is to examine the ethics of use of data collected via ITS and the legal ramifications of the State of Michigan's collection and use of data on vehicular movements. This study will serve both to catalog the range of issues related to government use of ITS data and to provide specific recommendations on how such data should be used, with attention given to how different types of data might ethically be used in different ways depending on key distinguishing features of the data (e.g., does it uniquely identify individual drivers or vehicles, does it reveal individual behavior, etc.).

The rest of the paper is structured as follows. Section II provides an overview of related literature; Section III and IV describes federal and state privacy laws, and the Freedom of Information Act (FOIA), respectively; Section V covers existing USDOT and MDOT ITS privacy policies; Section VI discusses the connection between ITS applications and locational privacy; and Section VII provides the list of recommendations. A list of

abbreviations used in this paper can be found in Appendix A.

II. RELATED LITERATURE

The privacy concerns in the realms of ITS and GPS tracking technology have increasingly become a hot research topic in recent years. This section summarizes major research findings on location privacy, level of privacy, and relation between privacy and ITS technologies.

LOCATION PRIVACY CLASSIFICATION AND RELATED CONCEPTS

According to Iqbal (2009), a traveler's location privacy is defined as, "the interest that a 'motorist' has in sustaining a 'personal locational space' free from interference by other motorists, telematics providers and other organizations." There are three different types of information: personal information (e.g., identity, gender, address, date of birth etc.), personal identifiable information (e.g., email address, phone number, credit card number, driver's license number, vehicle registration plate number, Media Access Control (MAC) and Internet Protocol (IP) address, etc.), and derived sensitive personal information based on location data (e.g., political opinions, religious beliefs, or race/ethnicity). It is recognized that blurred boundaries exist in this attempted classification.

Andersen and Kjærgaard (2011) classified the types of Location Based Service (LBS) into four categories: point-of-interest, social networking, collaborative sensing, and route tracing. There are five high-level location privacy methods, including anonymization, classical security, spatial obfuscation, temporal obfuscation, and protocol. It was found that insufficient work has been done in route tracing. It is, therefore, suggested that a new overall method should be proposed to solve the problem of location privacy in route tracing.

- Some other concepts related to legal aspects of location privacy include:
- Objective Expectation of Privacy - A reasonable expectation of privacy in a certain location or situation generally recognized as private by society.
- Subjective Expectation of Privacy – An individual's opinion that a certain location or situation is private; this varies from individual to individ-

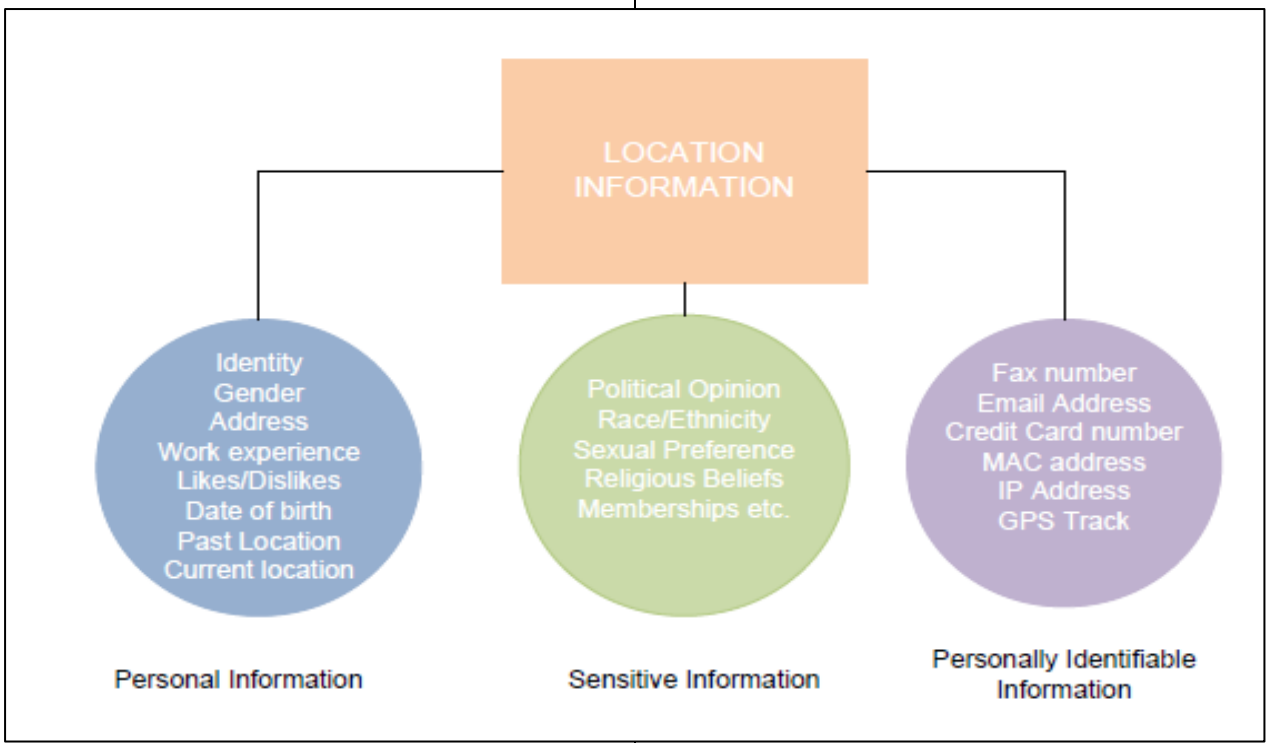

Figure 1: An Illustration of the Types of Location Information
Source: Muhammad Usman Iqbal. Location Privacy in Automotive Telematics. The University of New South Wales. 2009

ual.

- Probable Cause – A reasonable belief that a person has committed a crime. This is the standard by which an officer can make an arrest, conduct a personal or property search, or obtain a warrant for arrest with respect to criminal charges.
- Reasonable Suspicion – A legal standard that implies a person in the same circumstances could reasonably believe another person has been, or is about to be engaged in criminal activity. This legal standard that is not as high as probable cause, but allows an officer to detain an individual.

LEVEL OF PRIVACY

In modern society it is virtually impossible to preserve the absolute privacy of individuals traveling on today's transportation systems. However, it is desirable to give travelers a range of options to protect their identity. The level of privacy required by an individual will depend on personal preferences and specific situations. This range of acceptable levels of privacy can be reflected in following six exposure levels (Plotnikov, 2012):

- No ability to detect or track vehicles or individuals
- Low ability to detect or track vehicles or individuals - Manual data extraction from selective single location, single source records (e.g., recorded video)
- Medium ability to detect or track vehicles or individuals - Automatic data extraction from single location, single-source records
- High ability to detect or track vehicles or individuals - Automatic data extraction from multiple location, single-source data records
- Very High ability to detect or track vehicles or individuals - Automatic data extraction from multiple location, multiple-source data records (e.g. video and toll transponder)
- Full ability to detect or track vehicles and individuals inside and out of the vehicle - Automatic data extraction from continuous multiple-source data records (e.g. GPS, cellular transmitter, and live high definition (HD) video)

A more in-depth discussion on ITS technologies and their impacts on locational privacy are presented in Section VI.

ITS AND LOCATION PRIVACY

As mentioned earlier, ITS provides significant benefits to end users but often creates new ethics and policy dilemmas due to the increased use of sensing, tracking, and real-time behavior evaluation. Many ITS applications require collection and use of location data, status of vehicles, and personal information in the process of operating the devices or systems (e.g. electronic tolling and user-based insurance). In the case of connected vehicle technologies, the information is aggregated and likely shared with other vehicles and the infrastructure by using Dedicated Short Range Communication (DSRC), cellular communication, satellite communication, WiFi, Bluetooth or radio-frequency identification (RFID). Protecting personal privacy should be a central consideration in decisions about how information is collected, archived, and distributed (Briggs and Walton 2000).

The protection of information privacy often requires the balancing of interests between privacy protection and other affected legal interests, such as FOIA. In some cases, the lines of responsibility are also blurred due to the potential for active safety systems, such as automated decision making, warnings, and vehicle control. In addition, because many different entities will be manufacturing and using the ITS equipment for a wide range of applications, it is important to use universal design approaches when resolving ethical and policy concerns (Steinfeld, 2010).

In a connected vehicle study using probe vehicles that was conducted by Hoh et al (2006), the authors found that driver privacy could be compromised because the location and identification data transmitted from their vehicles could be intercepted and used to track individual vehicles or identify drivers' homes. The authors suggest to protect against these privacy and security threats that authentication and data analysis be handled by separate entities and that the connected vehicle architecture integrate encryption, tamper-proof

hardware, and data sanitization techniques to ensure data integrity. The authors also suggest using data suppression techniques, such as reducing sampling frequency. The researchers also claim that even anonymous data collection does not solve this privacy problem, since users can be identified through data mining techniques (so-called inference attacks).

Similarly, Duri et al. (2002, 2004) recommend a framework that relies on defense-in-depth, data aggregation near the source, and user defined privacy policies to provide data protection. The phrase "defense-in-depth" means that each layer of hardware and software provides its own security functions. Data aggregation near the source implies that rather than having the vehicle transmit large quantities of raw data, the computing system within the vehicle can serve to aggregate the data before sending it on to service providers. User-defined policies allow for specific data handling preferences for each user, these preferences, together with solution provider policies, will form virtual contracts between users and solutions providers.

Raya and Hubaux (2005) emphasize vehicle communication systems using DSRC and describe various threats to vehicle networks. These specific attacks include providing bogus information to other drivers, cheating with positioning information to avoid liability, identifying and tracking of other vehicles, using denial of service attacks to bring down the network, and masquerading as another vehicle. To protect against these attacks, the authors propose security requirements including: vehicle authentication, verification of data consistency, availability, non-repudiation, privacy, and real-time constraints.

Some researchers argue that individual privacy is threatened not by the collection of public location information but by the centralization of aggregated information, and by the combination of location information with other personal information. In these cases, informed consent ought to be necessary to balance the privacy rights of individuals against the freedom rights of businesses and the security rights of communities (Wang and Loui, 2009).

In general ITS applications, there is no need to identify a particular vehicle since the aggregate information is sufficient to perform ITS services. However, recent developments in transport technology, with the agenda of enforcement, policing, road safety, national security and road pricing, are systematically requiring the road-users' identity, either with the help of contracts such as electronic toll collection (ETC) systems, or through visual interfaces such as Automatic Number Plate Recognition (ANPR) which extracts the license plate details from a photo electronically (Iqbl, 2009).

Continuing developments in the fields of transportation technology and privacy law present an abundance of opportunities for conflict. From the legal perspective, advocates of comprehensive privacy law struggle to update existing law at a pace that keeps up with innovative advancements in technology. Privacy issues related to electronic communications are often the primary concern for transportation organizations. It is suggested that ITS planners and developers take steps toward reconciling the legal and political privacy issues presented from the beginning of the design phase of a project through its implementation, and consider the policy impacts of those decisions and the effect on current public perception (Douma and Aue, 2011).

Douma and Deckenbach (2009) examined a number of areas where privacy law could impact ITS projects and technologies. They concluded that the United States currently has no comprehensive national regulatory structure for privacy, leaving answers to these privacy concerns to be found through a consideration of a variety of sources of federal and state privacy law.

The following sections (III, IV, and V) provide an overview of federal and state privacy laws and legislation, the federal and state FOIAs, and existing USDOT and State of Michigan privacy policies.

III. FEDERAL AND STATE PRIVACY LAWS AND LEGISLATION

In the United States there is no overarching information privacy law to govern both government agencies and private businesses. There are federal and state laws that regulate the collection and management of personal information within government agencies as well as laws that regulate consumer data use in specific industries such as telecommunications, cable television, and banking. Largely private sector information privacy protection is provided through voluntary self-regulation and use of contracts. The issue of data protection is a patchwork of legal provisions that has largely been left to individual states and the court system. Some companies have instituted their own privacy policies and many belong to associations with stringent rules governing privacy (Economist 1999).

Because of the concerns identified in previous sections and the tensions between various groups, it is necessary to use mechanisms, either legal or institutional, to provide balance between public, government, and commercial interests. This section discusses some of these mechanisms as they apply to connected vehicles and ITS applications broadly. The first subsection outlines federal and state legislation relating to electronic privacy, which is followed by a discussion of the Fourth Amendment and its implications. This discussion is followed by an overview of historical and ongoing court cases that have set precedents for the interpretation of the law. The section closes with a brief examination of voluntary mechanisms used by private interests to self-regulate ITS applications.

FOURTH AMENDMENT

The right to privacy is not expressly guaranteed in the U.S. Constitution, but through numerous court opinions regarding the Fourth Amendment, it has been upheld as a Constitutional right. The basis for much of privacy law is the Fourth Amendment of the U.S. Constitution which reads:

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

The Fourth Amendment protects citizens from unreasonable search and seizure by government officials without due process. A search is constituted by the infringement of an individual's expectation of privacy by a governmental official. The limitations on searches and seizures particularly affects law enforcement agents, though government employees involved with civil suits may also be affected by these limitations. The Fourth Amendment does not apply to the actions of private individuals.

A seizure is constituted by interference with an individual's property by a governmental official. An individual can be considered seized when physical force is used to restrain the individual, or if a reasonable person in the same or a similar situation would not feel free to leave the situation (Cornell 2011). In order to invoke Fourth Amendment protections, an individual must have a legitimate expectation of privacy. A legitimate expectation must be both subjectively and objectively reasonable, meaning that the individual must, given the circumstances, actually expect privacy and a reasonable person in the same or a similar situation would also expect privacy.

Despite being written over 200 years ago, the Fourth Amendment has been applied to modern technologies and thus protections exist for searches and seizures conducted with the use of electronic devices. The electronic searches and seizures have received significant attention from the courts in recent years. These cases have covered the use of new technologies such as electronic beepers, GPS, cellular phone data, and other surveillance technologies, used to track the movement of individuals.

FEDERAL AND STATE LAWS RELATING TO ELECTRONIC PRIVACY

Privacy law, especially since the 1980s, is largely a response to technological changes in electronic

information technology such as computers, networks, and digital information products. A common theme is protection against unauthorized use of the collected information and government access to private records. In federal laws that are relevant to ITS applications, there is precedent for protecting privacy above and beyond protections offered by the Fourth Amendment (Jacobson 2007). Some of these relevant laws include the Privacy Act (1974), Electronic Communications Privacy Act (1986), and Drivers Privacy Protection Act (1994).

The Privacy Act established requirements for federal agencies relating to the collection, maintenance, use, and dissemination of personally identifiable information about individuals. It requires government agencies to disclose the purpose for collecting information, routine uses that may be made of the data collected, and consequences for failing to provide requested information. The act also requires agencies to establish appropriate administrative, technical, and physical security measures to protect the privacy of the individuals on whom it has collected information. The Electronic Communications Privacy Act (ECPA) created government restrictions on monitoring transmissions of electronic data by computer. The act also places restrictions on government access to stored communications and tracing of telephone communications. The Drivers Privacy Protection Act (DPCA) prohibits the disclosure of personal information gathered by state Departments of Motor Vehicles (DMV). The act also outlines permissible uses of personal driver information.

The Communications Act of 1934 established the Federal Communications Commission (FCC). The act was amended by the Telecommunications Act of 1996 and requires the telecommunications companies to "protect the confidentiality of proprietary information of, and relating to... customers" as well as "customer proprietary network information." As of 2012, the FCC is researching privacy and data security practices relating to private information stored on customers' mobile communications devices and how existing privacy and security requirements apply to that information (Tatel 2012). A regulatory decision resulting from FCC's inquiry could affect connected vehicle service providers in that it may require certain data protections, or may limit what data can be collected and stored using On-Board Equipment (OBE).

Other laws such as the Communications Assistance for Law Enforcement Act (CALEA) and the Patriot Act have changed how law enforcement officials can monitor individuals. While CALEA enhances the ability of law enforcement to monitor individuals by requiring equipment manufacturers and electronic service providers to include monitoring abilities in product and service design, it also enhances privacy of electronic communications and places restrictions on obtaining tracking information. The Patriot Act amends the ECPA and allows greater access to electronic data by federal agencies. The Patriot Act may allow mobile phone tracking and conflicts with some circuit court rulings prohibiting such tracking.

There are not many state laws that address connected vehicle technology implementation specifically, though some common types of state laws could have an impact on connected vehicle systems. For instance, fair information practices statutes restrict the type of personal information that state government agencies can collect, maintain, and disclose. These types of laws also frequently allow individuals to access and correct information about them held by state agencies. Stored wire communications statutes and wiretap statutes restrict state agency access to stored and transmitted information. States also have common law remedies which allow individuals to seek redress for invasion of privacy and public disclosure of private information.

COURT CASES INVOLVING PRIVACY AND GOVERNMENT TRACKING

This section discusses court cases involving the use of location tracking electronic devices and the protection of privacy. The cases reviewed for this paper include selected Supreme Court, federal, and state cases regarding the use of technology in surveillance and tracking by law enforcement. The case law surrounding this subject is relatively

clear for simple devices such as beepers for tracking over short periods of time, but is less clear with respect to more sophisticated technologies that can provide highly detailed information, especially when used over longer periods of time. In depth discussions of the court cases referenced in this discussion can be seen in Appendix B.

In general, the courts have ruled that individuals have a decreased expectation of privacy while driving in public and hence have allowed the manual or electronic surveillance and tracking of vehicles on public streets. Some state courts, however, have ruled to require greater restrictions on law enforcement personnel using electronic tracking devices on vehicles (Briggs and Walton 2000). Because cellular and GPS tracking technology can be used to obtain detailed information and present significantly greater capabilities than beeper technology, some argue that it should require higher legal standards. Many of the cases involving these newer technologies have referenced cases that involved beepers, with decisions being based off of beeper jurisprudence (Stephens 2008). In the past few years, courts have come to recognize how powerful these technologies are, and though the case law is at times contradictory, are commonly requiring a warrant to use GPS and cellphone tracking.

Figure 2 below outlines selected major Supreme Court cases relating to privacy law. In Katz v. United States, the Court clarified that intrusion with technology is considered a search. Years later in United States v. Knotts the Court decided that electronic beepers could be used for tracking from a short distance without a warrant. One year later in United States v. Karo, the Court ruled that while using a beeper on public roads was legal without a warrant, tracking an individual inside a residence with a beeper without a warrant was a violation of the Fourth Amendment because it violated expectation of privacy. In the United States v. Kyllo, the Court similarly ruled that using a thermal imaging device to monitor heat radiation from a residence was a search and required a warrant (many states have adopted thermal imaging as a high-occupancy-vehicle lane enforcement tool to help determine vehicle occupancy). The Antoine Jones case, detailed below, has led many groups to push for national legislation regulating the use of GPS and cellphone tracking by law enforcement. Absent legislation, the Jones case, which received a ruling from the Supreme Court in January 2012, could serve to further clarify the legal requirements for using these types of tracking technologies.

ANTOINE JONES GPS TRACKING CASE

Over the course of a month, law enforcement officials used a GPS tracking device on a vehicle owned by Antoine Jones to collect evidence connecting Jones to illegal drug distribution (MTTLR 2011). The evidence was used in a D.C. federal district court to convict Jones and he was sentenced to life in prison. A federal appeals court later overturned the conviction on the grounds that the FBI and local police did not have a valid search warrant to collect travel information from Jones' car (Courier 2011). The investigators continued to use the GPS device to track the vehicle long after the warrant used to place the device expired and used tracking information from outside the warrant's jurisdiction to convict Jones (Gatto 2011). The appeals court accepted the precedent set by United States v.

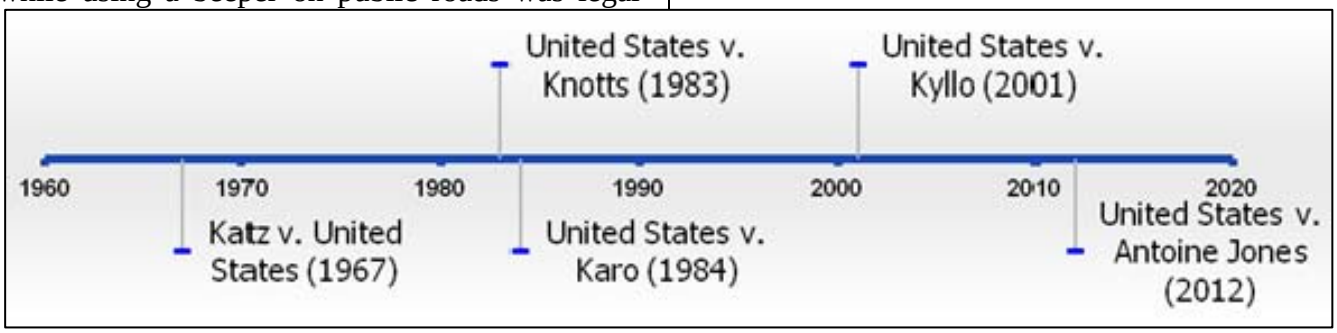

Figure 2: Relevant Selected Supreme Court Interpretations of Privacy Law
Source: Center for Automotive Research

Knotts (1983) which concluded that warrantless tracking for a single trip did not constitute a search, but concluded that using the GPS device to collect data over an extended period was an unreasonable search because it revealed private information through patterns of behavior, and individuals have a reasonable expectation of privacy in the sum total of their movements over long periods. The court decision does not preclude the use of GPS tracking devices, but instead requires a warrant to use such a device for continuous monitoring over a prolonged period of time (Durkee 2010).

In November 2011, the Supreme Court heard oral arguments on the case. The Supreme Court ruled on the Jones case in January 2012. Some had speculated that the decision could have a broad impact on investigative techniques and technologies used by the police, as well as societal expectations of privacy (MTTLR 2011). However, the Court ruled unanimously that the police erred by not obtaining an extended search warrant before attaching a tracking device to Jones's car and the majority opinion did not address future Fourth Amendment cases, where the police may not need to physically trespass in using electronic surveillance technologies. As a result of the ruling, the FBI would have been forced to turn off 3,000 GPS devices; however, because the FBI was able to get warrants for, 2,750 of the devices, over 90 percent of the 3,000 are still in operation. In those cases where the FBI cannot get warrants for GPS monitoring, they are still able to deploy teams of six to eight officers to track suspects the old fashioned way (Johnson 2012).

For now, discretion as to how long tracking devices can be used before requiring a warrant is up to future court cases, though the issue could be taken up by legislators, as it has been in several states, including California, Pennsylvania, Florida, Utah, Minnesota, Oklahoma, and South Carolina (Durkee 2010). In addition, there have been calls to create legislation governing the warrant requirements for using GPS tracking devices such as in the white paper issued by the Constitution Project in September 2011, which advocated for national legislation on this issue (Constitution Project 2011). Legislation known as the Geolocation Privacy and Surveillance Act (GPS Act) was introduced to the in June 2011 and is awaiting consideration before committee in both the House and Senate (GPS.gov).

RECENT DEVELOPMENTS IN GPS AND CELLPHONE TRACKING

Cell phone tracking has become a regular feature in criminal investigations. Police can obtain either retrospective data kept by mobile providers for billing or detailed prospective data revealing the minute-by-minute location of a mobile device (McCullagh 2010). In the past few years, there have been several rulings on the use of satellites and cellphones to track criminal suspects.

Many of the recent court cases have reached somewhat conflicting conclusions on GPS and cellphone tracking issues. For instance, on August 22, 2011, New York U.S. District Court Judge Nicholas G. Garaufis ruled that police need a warrant to track an individual using cellular-tower triangulation (Nojeim 2011). However, on October 3, 2011 Chief Judge Royce Lamberth of U.S. District Court for the District of Columbia ruled that police did not need a warrant to use cellphone tracking, noting that, "…a reasonable cellular phone customer presumably realizes that his calls are all transmitted by nearby cell-site towers, and that cellular phone companies have access to and likely store data regarding the cell-site towers used to place a customer's calls… An individual's decision to place a cellular phone call and thus provide information regarding his location to the phone company thus defeats an individual's privacy interest in that information" (Lamberth 2011). On Nov. 11, 2011, Texas U.S. District Court Judge Lynn N. Hughes ruled that a warrant was necessary to force cellular telephone services to share data that reveal location (Angwin 2011). In May 2012, a federal judge ruled vital evidence inadmissible in a drug crime because it was gathered during a traffic stop made possible by warrantless GPS tracking (Associated Press 2012). Later in May 2012, Federal prosecutors argued in a case before the Ninth U.S. Circuit Court of Appeals that the government has the right to place GPS tracking devices on cars with-

out a warrant, even despite the Supreme Court's Antoine Jones case ruling. The prosecutors pointed out that the court did not specifically state that a warrant would be required in other situations (Angwin and Bravin 2012). At the same time, the Justice Department has advised agents to obtain warrants for new or ongoing investigations, suggesting that there is still much uncertainty relating to the use of vehicle tracking technology for criminal investigations.

In addition to criminal investigations, electronic surveillance technologies are now available to private citizens. Some companies offer tracking applications for phones that allow an individual to monitor both the location and communication of a smartphone. While the Biddle v. State case determined that a citizen using GPS tracking on another individual's vehicle violated state law, there is no consistency between state laws. In fact, in July 2011, a New Jersey appellate court ruled that GPS tracking can be used by private citizens to track their spouses (Gatto 2011).

IV. THE FREEDOM OF INFORMATION ACT

Federal and state Freedom of Information Act (FOIA) laws require government agencies to disclose records in their possession upon request. These laws protect the public's right to know and enhance government transparency and accountability. This section discusses the impact of federal and Michigan FOIA laws on privacy of data collected through ITS.

FEDERAL FREEDOM OF INFORMATION ACT

The FOIA was enacted in 1966 to allow members of the public to obtain records from agencies in the federal government. The FOIA allows any person (U.S. citizens, foreign nationals, organizations, associations, and universities) to file a request. The FOIA was amended in 1974 to improve agency compliance and again in 1996 to improve access to electronic information (GWU 2012). Recent national legislation affecting the FOIA includes the Openness Promotes Effectiveness in our National (OPEN) Government Act of 2007 and the OPEN FOIA Act of 2009 (DOJ 2012).

Federal case law has established that drivers do not have a reasonable expectation of privacy while traveling. Because of this, it should be expected that an agency maintaining a database containing data collected through the use of ITS applications may be required to disclose portions of that database. In the interests of individual privacy, said database system should be designed in a manner that anticipates and resolves problems of access that could result from FOIA requests (Pethtel et al. 2011).

It is not uncommon for organizations involved with the generation of data through ITS applications to receive data requests from private or public entities. In one study, survey responses indicated that FOIA requests specifically were not uncommon. Several respondents reported reacting to requests for data in the form of court orders or other form of request from public entities, and some respondents even honored requests from private entities (Pethtel et al. 2011). In several states where Electronic Toll Collection systems exist, data collected by these systems has been subpoenaed by criminal as well as civil courts (Newmarker 2007).

The federal FOIA addresses access to data from federal agencies; however, if Michigan's connected vehicle system were managed by MDOT, the data would not necessarily be covered under the federal FOIA. To obtain data from MDOT, a requester would have to make a request under Michigan's FOIA, which is outlined in the following section.

MICHIGAN FREEDOM OF INFORMATION ACT

Like the federal FOIA, the State of Michigan has its own Freedom of Information Act which was passed in 1977 and amended in 1996. The basic intent of Michigan's FOIA is to set requirements for the disclosure of public records by all public bodies in the state. Public bodies include state agencies, county and other local governments, school boards, other boards, departments, commissions, councils, and public colleges and universities. Public bodies do not include the governor or lieutenant governor, their executive office, and their employees or private non-profit corporations (Schuette 2010).

Public records covered under the Michigan FOIA include any writing that is prepared by, owned by, used by, in the possession of, or retained by a public body in the performance of an official function. Records in all formats are subject to the Michigan FOIA, including material that has been handwritten, typed, printed, photographed, photocopied, or documented with other means of recording or retaining meaningful content (software is exempt). In general, all records are open to disclosure except those which have specifically received exceptions. Among the types of public records that are exempt from disclosure are several that may be relevant for connected vehicle data, including:

- Records revealing specific personal information about an individual if the release would constitute a clearly unwarranted invasion of that individual's privacy;

- A public record or information which is furnished by the public body originally compiling, preparing, or receiving the record or information to a public officer or public body in connection with the performance of the duties of that public officer or public body, if the consideration originally giving rise to the exempt nature of the public record remains applicable;
- Records specifically exempted from disclosure by another statute; and
- Records of a public body's security measures (Schuette 2010).

Because the detailed data collected as part of a deployed connected vehicle system would have the potential of revealing specific personal information about an individual and constitute an unwarranted invasion of privacy, the data would be exempt from disclosure under the Michigan FOIA. In addition, if detailed data were collected by MDOT and given to another agency, the data would still be exempt from disclosure because the consideration originally giving rise to the exemption of the public record would remain applicable. However, less detailed data would not necessarily be exempt from disclosure requirements as it might not reveal personal information about individuals.

The Michigan FOIA also allows records to be exempt from disclosure if another law states this exemption. This rule would allow the Michigan legislature to pass additional protections specifying which types of data collected by a connected vehicle system are exempt from disclosure. With legislative clarification, connected vehicle data could be better protected from disclosure, creating greater certainty and public acceptance of connected vehicle systems.

In addition, the exemption to software and security measures is important to maintaining the security of connected vehicle data systems. Security of data is a major concern for both the connected vehicle system managers and the general public. Because the software and security measures taken to prevent unauthorized access or tampering with connected vehicle data are protected from disclosure under the Michigan FOIA, maintaining data security is more tenable.

COURT OPINIONS ON MICHIGAN'S FOIA

Michigan courts have rendered decisions which interpret the language of Michigan's FOIA. These rulings are the law of the state unless changed by a higher court or by the Michigan legislature. The rulings also provide insight as to how the Michigan FOIA has been enforced over the years.

In Mullin v Detroit Police Department (1984), the court provided for privacy protection in the context of Michigan drivers when it ruled that, "a computer tape containing personal information on persons involved in traffic accidents" should be exempted for the Michigan FOIA, because "disclosure of the tape would have been a clearly unwarranted invasion of privacy." On the other hand, the court interpretation of Herald Co. v Ann Arbor Public Schools (1997) noted that, "exempt material must be segregated from non-exempt material to the extent practicable," which could mean that some data from connected vehicles could be subject to disclosure as long as it can be cleaned so as not to disclose private information.

According to the courts, "information is considered personal if it concerns a particular person and his intimate affairs, interests or activities" (Herald Co. v Ann Arbor Public Schools 1997). Because detailed data collected through connected vehicles could be used to identify individuals and intimate details about their lives through driving patterns, it is likely that the data would be considered personal information. In addition, in Swickard v Wayne County Medical Examiner (1991) the court stated that determining whether a disclosure of requested information would constitute an invasion of privacy that the court should look to "common law and constitutional law" as well as "customs, mores, or ordinary views of the community." Given the inconsistent rulings on vehicle tracking throughout the nation, however, it is possible that legislative action will need to be taken to clarify what types of data collected from connected vehicle systems should be considered private for the purposes of the Michigan FOIA.

V. ITS PRIVACY POLICIES

FEDERAL ITS PRIVACY POLICIES

The federal government has not adopted one set of privacy policies specifically for ITS applications. However, among federal agencies, there has been significant work that considers the issue of privacy. Both the Federal Highway Administration (FHWA) and the National Highway Transportation Safety Administration (NHTSA) have authored reports on connected vehicle technology that outline design goals related to privacy (Andrews and Cops 2009, Volpe 2008). The goals are listed in the table below.

While FHWA and NHTSA reports list goals for connected vehicle systems, they do not reference formal laws or regulations guiding the design of connected vehicles. In fact, except for the Federal Trade Commission's "Fair Information Practice Principles," there is only limited guidance on privacy issues from the federal government with respect to transportation issues, and none with respect to ITS applications (Fries et al. 2010).

MDOT ITS PRIVACY POLICY

In the Michigan Department of Transportation's strategic and business plan for deploying connected vehicles, it was stated that, "…it will be critical to ensure information security and exchange of data will support acceptable standards of user privacy" (Underwood et al. 2008). While the document itself does not specify privacy standards, it does suggest that implementation will require addressing issues related to driver privacy. MDOT has identified driver privacy as a

Table 1: ITS Privacy Goals

Organization	Privacy Goals
Federal Highway Administration (FHWA)	• System provides effective safeguards to avoid use of privately collected data to be used to track a vehicle or to identify an individual vehicle as violating a traffic law • Cannot track an individual vehicle over any road segment longer than 2 km • Cannot identify any individual vehicle as violating a traffic law through publicly collected data • Cannot identify a vehicle or a vehicle occupant or owner from messages sent to, or through, the infrastructure • System's ability to protect consumer privacy can be clearly communicated to the public
National Highway Transportation Safety Administration (NHTSA)	• Physical protection of the transponder device, its antenna, and its wiring to resist damage, either accidental or intentional • Security against intentional tampering or jamming • Security against counterfeiting, identity theft, or other criminal intrusion or illegal transponder activities • Security against system circumvention by individuals or by underground manufacturers • Privacy-protection features and software protocols to prevent unauthorized access to vehicle or driver data • Devices to detect and reveal transponder negligence, fraud, or cheating by a driver or vehicle owner.

Source: Andrews and Cops 2009, Volpe 2008

crucial issue and that public acceptance hinges on the adequate protection of civil liberties, but has yet to craft its own privacy policy for data collected through connected vehicle technology.

VOLUNTARY PRIVACY PRINCIPLES

While there are few existing laws and policies governing privacy in the design of ITS applications, there are several existing guidelines that can be used to create privacy policies for users of connected vehicle systems. The most well-known example is the Intelligent Transportation Systems of America "Fair Information and Privacy Principles" (ITSA 2001), though these principles are voluntary and do not reflect legal or regulatory standards. Another source for guidance is the "Vehicle-Infrastructure Integration Privacy Policies Framework" (Jacobson 2007). These documents, copies of which can be found in Appendix C and D, outline basic principles that should be used to govern the design of connected vehicle systems. They can be used as a starting point for the development of policies addressing regulation on privacy. In general the documents seek to provide privacy protection for drivers and the principles are designed to be flexible so they will remain relevant despite technological, social, and cultural change. The documents suggest limitations on the acquisition, use, distribution, and retention of data collected using connected vehicle technology. They suggest security and disclosure procedures and also discuss issues relating to traffic enforcement and public disclosure through the FOIA process.

VI. ITS APPLICATIONS, DATA COLLECTION TECHNIQUES AND PRIVACY CONCERNS

Privacy implications of ITS technologies are closely related to the types of applications (e.g., safety, operations, and maintenance), the selected data collection techniques, and purpose for information collection. Given the wide range of intelligent transportation systems, it is difficult to organize ITS applications into one standard list, especially when many applications can serve multiple functions or purposes. According to ITS America (2011) and Information Technology & Innovation Foundation (ITIF 2010), the service areas of ITS can be grouped into following eight broad areas:

- Advanced Traveler Information System (ATIS)
- Advanced Transportation Management Systems (ATMS)
- ITS-Enabled Transportation Pricing Systems
- Advanced Public Transportation Systems (APTS)
- Vehicle-to-Infrastructure Integration (VII) and Vehicle-to-Vehicle Integration (V2V)
- Commercial Vehicle Operations
- Emergency Management
- Maintenance and Construction Management

While this list is not inclusive of all possible ITS categories, it includes the most prominent ones. Table 2 provides examples of specific applications under each of these ITS categories. It can be seen that the driving forces behind many ITS initiatives are safety and mobility. Most of the applications do not need to specifically identify the travel patterns of a vehicle or individual driver. Therefore, data needs for these applications may not require any personal information or identification.

On the other hand, ITS or connected vehicle technologies are increasingly used in some emerging areas, such as user-based insurance, road pricing, and vehicle-miles traveled (VMT) fees. These applications normally require the collection of personal information, such as name, address, driver license number, other personal identifiers, as well as increased accuracy of location data in real-time. The uses of such information could pose a threat to the privacy of individuals. The levels of privacy invasion generally depend on what data collection technique is used, what information is collected, how it is stored, and how it is used, as illustrated in Table 3. These privacy concerns become even more complicated because data may be collected and used by a wide variety of organizations such as telecommunications companies, insurance agencies, government agencies, and private data collection and management firms.

Table 2 and Table 3 on the following pages contain a broad range of ITS applications and data collection techniques. These applications and techniques include those currently used or planned for use by MDOT, as well as those that could potentially be used by MDOT, even though they are not currently being considered.

Table 2: ITS Categories and Applications

ITS Category	Examples of Specific ITS Applications	Applicable in Michigan
1. Advanced Traveler Information Systems (ATIS)	• Real-time Traffic Information Provision	Yes
	• Route Guidance/Navigation Systems	Yes
	• Parking Information	Yes
	• Roadside Weather Information Systems	Yes
2. Advanced Transportation Management Systems (ATMS)	• Traffic Operations Centers (TOCs)	Yes
	• Adaptive Traffic Signal Control	Yes
	• Dynamic Message Signs (or "Variable" Message Signs)	Yes
	• Ramp Metering	No
3. ITS-Enabled Border Crossing Program	• Advanced Traveler Information System	Yes
	• Variable Toll Pricing	No
	• Electronic Screening System for Trucks and Buses	Yes
4. Advanced Public Transportation Systems (APTS)	• Real-time Status Information for Public Transit System	Yes
	• Automatic Vehicle Location (AVL)	Yes
	• Electronic Fare Payment (for example, Smart Cards)	Yes
5. Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) Integrations	• Cooperative Intersection Collision Avoidance System (CICAS)	Yes
	• Infrastructure Monitoring and Data Management	Yes
	• Data Use Analysis Processing Project (DUAP)	Yes
	• Signal Phase and Timing Communication System	Yes
	• Vehicle-based Information and Data Acquisition System (VIDAS)	Yes
	• Slippery Road Detection and Evaluation	Yes
	• Intelligent Speed Adaptation (ISA)	Yes
6. Commercial Vehicle Operations	• Driver Communication Systems	Yes
	• Vehicle Monitoring and Safety Management Systems	Yes
	• Cargo Management Systems	Yes
	• Driver Credentialing Systems	Yes
7. Emergency Management	• Emergency Routing Equipment Systems	Yes
	• Roadway Service Patrols	Yes
	• Wide-Area Alert Systems	Yes
8. Maintenance and Construction Management	• Vehicle and Equipment Tracking Systems	Yes
	• Fixed and Vehicle-based Sensors/Probe Monitoring	Yes
	• Work Zone Management	Yes
9. ITS-Enabled Transportation Pricing	• Electronic Toll Collection	No
	• Congestion Pricing/Electronic Road Pricing	No
	• Fee-Based Express (HOT) Lanes	No
	• Vehicle Miles Traveled (VMT) Usage Fees	No
	• Variable Parking Fees	No

Table 3: ITS Data Collection Techniques and Locational Privacy

Data Collection Techniques	Functionality of Data Collected	Vehicle Information and Identification	Driver and Occupant Information and Identification	Privacy Expectation and Legal Protection	
					Applicable in Michigan
Loop Detectors	Volume, Vehicle Class, Speed, Estimated Travel Time, and Incident Detection	No Individual Vehicle Information Obtained	None	None	Yes
Video Image Detectors	Vehicle Class, Estimated Speed, Volume, and Incident Detection	Individual Vehicle Information Likely Obtained	None	Medium	Yes
Infrared and Thermal IR Cameras	Occupant Observation	Vehicle Identification Likely Obtained	None	Medium	No
Toll Transponder	Origins and Destinations, Volume, and Average Speed	Vehicle Identification Obtained	Possible through Vehicle Registration System	Medium	No
License Plate Reader	Origins and Destinations, Average Speed and Travel Time	Vehicle Identification Obtained	Possible through Vehicle Registration System	Medium	No
GPS-enabled Mobile Phones or Probe Vehicles	Real-time Vehicle Location, Travel Paths, Speed, Origins and Destinations	Vehicle Identification Likely Obtained	Possible through Vehicle Registration System and Telecommunication Records	High	Yes

Adapted from: Frank Douma and Sarah Aue. ITS and Locational Privacy: Suggestions for Peaceful Coexistence. Center for Transportation Studies, University of Minnesota. October 2011.

VII. RECOMMENDATIONS

As discussed in previous sections, privacy implications of the ITS program and connected vehicle data collection are becoming a bigger concern for many transportation organizations. However, further assessment of privacy protection mechanisms is needed for both public and private sectors, mainly because existing federal and state privacy laws are not keeping up with innovative advancements in ITS technologies. In addition to keeping an eye on developing technologies, state agencies and transportation professionals should stay aware of legal developments in the United States since privacy laws are likely undergoing significant changes in response to the innovative advancements in technologies. Our recommendations for Michigan's ITS planners and developers are as follows:

IDENTIFY ITS DATA NEEDS AND SELECT DATA COLLECTION TECHNIQUES ACCORDINGLY

The first step for transportation professionals and ITS planners is to determine the type of information that needs to be collected. As suggested by many researchers, the best option is to only collect the data needed for the task and to use anonymous information whenever possible. This will result in fewer legal liabilities and requirements while maintaining the anonymity of vehicles, drivers, and passengers. Anonymous information carries no personally identifiable information, such as full name, address, telephone number, and driver's license number, but can still provide good data on traffic, vehicular movements, and people's travel patterns. Anonymous information is valuable and often sufficient for most mobility, safety, and operations-related ITS applications and general transportation planning purposes.

When personally identifiable information is needed (e.g., electronic toll collection, GPS-enabled insurance, and vehicle mileage fees), the consent from an individual is required before being participating in these programs. Examples of information that needs to be conveyed to the willing participants usually include:

- What information is being collected
- How the information will be used
- Who can access personally identifiable information
- The legal consequences for giving consent
- The privacy safeguards that will be put in place over the collected information
- How false information can be corrected
- How long the information will be kept
- Choices to remain anonymous or "opt-out"

When using informed consent mechanism, liability over ITS information practices can be waived and limited, allowing ITS managers to use the personal information towards ITS goals without fear of legal liability (Douma and Aue, 2011).

DETERMINE PARTICIPATIONS REQUIREMENTS AND OPTIONS FOR ANONYMITY

The privacy implications of ITS and connected vehicle technology are determined significantly by the participation options of the system. There are two major design approaches related to user participation: anonymity by design and anonymity by policy. These two approaches have been frequently used in ITS and connected vehicle privacy discussions (RITA ITS Joint Program Office, 2009).

"Anonymity by design" means that multiple technical controls are built into the system to ensure that, to the maximum extent possible, a vehicle's or person's identity cannot be determined based on ITS data exchanges, or based on what was captured in one system's log file. This approach provides the maximum anonymity consistent with the privacy policy framework, but could be too sophisticated to implement and expensive.

An alternative approach is "anonymity by policy," which allows the use of commercial wireless network and focus more on protecting the content being moved on a network and on securing access to the network itself, rather than on providing anonymity. This approach requires relaxed privacy requirements, but can provide more needed information such as individual vehicle probe data,

traffic management, traveler information, and other ITS applications. While personally identifiable information is collected, it is stripped off at the earliest opportunity. The drawback of this approach is that anonymity is not guaranteed.

BALANCE THE TRADEOFF BETWEEN PRIVACY AND QUALITY OF ITS DATA THROUGH ADVANCED DATA ARCHITECTURE

Many factors will affect the quality and integrity of ITS data, such as data sampling rate, network coverage, and impacts of privacy rules. Poor data quality will certainly become a significant issue. Many ITS practitioners suggested using advanced data suppression techniques and system design architecture, such as separating communication and traffic servers, encryption, and using virtual-trip-lines (VTL) to balance the tradeoff between privacy and quality of ITS information.

Figure 3 illustrates the entities and cryptographic schemes involved in transmitting a data sample from a vehicle (Hoh et al. 2006). The communication server (CS) maintains network connections and authenticates users but doesn't access location and speed data. The traffic server (TS) receives anonymous data from the CS, decrypts and sanitizes it, and conducts tasks such as producing real-time congestion maps. Because these functions share only well-defined messages, only anonymous position information is available at the traffic-monitoring service. As such, the proposed architecture can meet privacy and data integrity requirements.

Another useful technique is encryption, which is the conversion of data into a form that cannot be easily understood by unauthorized people. The privacy of individuals can be maintained using business processes and software that encrypts the data (e.g., toll tags) at the source of data collection. The encrypted IDs are anonymous and are retained for a limited time period, such as twenty-four hours in many cases, and then discarded. No historical database of the encrypted IDs is maintained beyond that time period.

Hoh etc. (2008) also suggested a traffic monitoring system based on the VTL concept, which uses virtual geographic line segments deployed across roadways in the transportation network, triggering phones to collect and transmit data to the system. The VTL paradigm achieves strong anonymity, through a system design that separates identity- and location-related processing, so that no single entity has access to both location and identity information. Virtual trip lines can be easily omitted around particularly sensitive locations. Virtual trip lines also allow the application of temporal cloaking techniques to ensure anonymity properties of the stored dataset, without having

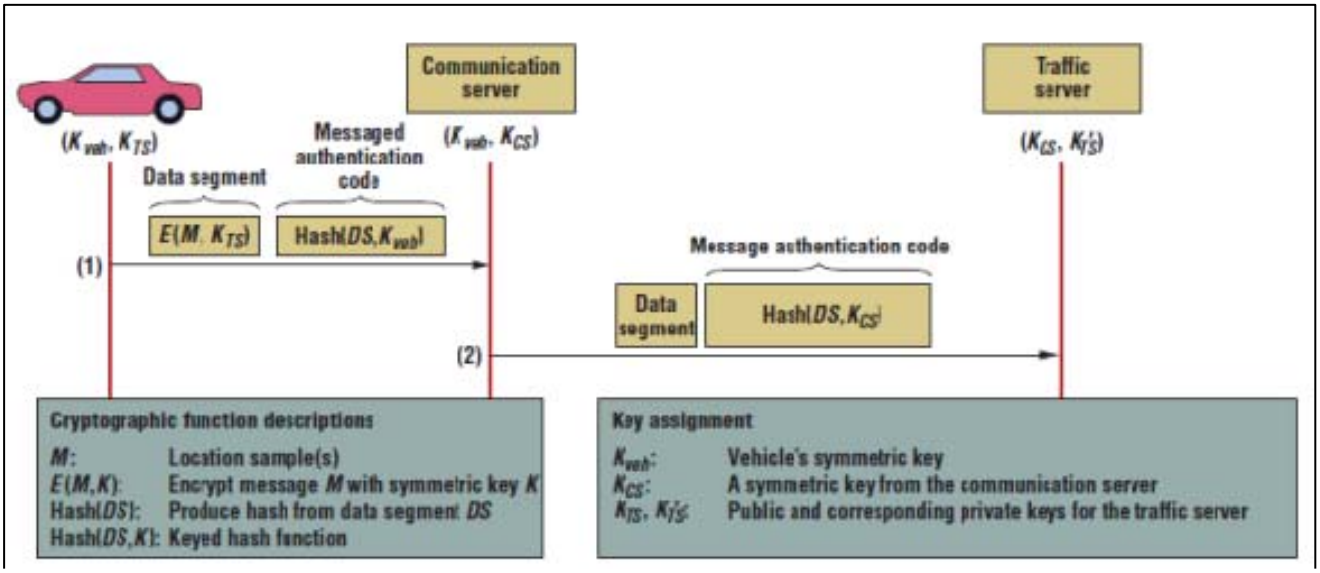

Figure 3: Traffic Monitoring Architecture to Ensure Data Integrity and Anonymous Data Collection
Source: Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Enhancing Security and Privacy in Traffic-Monitoring Systems. PERVASIVE Computing. 1536-1268/2006s

access to the actual location records of phones (Hoh et al, 2008).

MAKE PARTICIPATION VOLUNTARY

The design of ITS and connected vehicle technology policies can play a significant role in addressing public concerns about the technology and its applications. In addition to specifying how data can be collected, managed, and used, policy can be used to determine the nature of implementation, for instance, whether adoption is mandatory or voluntary. In the former case, universal participation would be required and all new vehicles will be required to feature operational OBE. Making participation voluntary may reduce the number of users initially, but it could help make the deployment of connected vehicle technology publically acceptable and politically viable (Briggs and Walton 2000). Under a voluntary or "opt-out" system, drivers with privacy concerns can hold off on adopting the technology, while others who value the benefits of the system and have little concern can be early adopters. As the penetration rate of connected vehicle technology increases, many drivers who were initially hesitant about the technology may decide to adopt it in their vehicles. Beyond connected vehicle technology, voluntary participation could be used for other ITS applications such as mileage-based user fees, electronic verification, or electronic toll collection. Obviously voluntary participation would not be applicable for numerous ITS applications such as traffic cameras, license plate recognition, and variable message signs.

USE MARKET INCENTIVES FOR TO PROMOTE ADOPTION

Significant benefits, convenience, and low cost often trump privacy and other public concerns with respect to consumer adoption of new technologies (Persad et al. 2007). Examples of already deployed ITS technologies such as electronic toll collection have demonstrated that consumers react to incentives. The convenience and sometimes lower costs of electronic toll collection has spurred its adoption among commuters who regularly use toll roads and the potential for saving on insurance costs has attracted drivers to the idea allowing insurance companies to monitor aspects of their driving habits. Similarly, if connected vehicle technology can be offered for a relatively inexpensive cost and can offer ways for users to save time and money, it will gain widespread acceptance and adoption. If initial deployment needs an impetus, policymakers can offer additional incentives (these could be a variety of things including tax exemptions, rebates, reductions in registration or title fees, or special privileges such as priority parking spaces or high-occupancy lane access) to early adopters to spur purchases of the technology. Once there are many users on the road, connected vehicle technology will benefit from networking effects, increasing the value of the technology to consumers and spurring further adoption. Again, beyond connected vehicle and electronic toll collection applications, market incentives could be used for other ITS applications requiring in-vehicle technology such as mileage-based user fees or electronic verification.

RESOLVE EQUITY ISSUES USING SUBSIDIES FOR INSTALLATION

Deployment of connected vehicle systems could possibly create equity issues among rural drivers, low-income drivers, and other groups who may feel that investment is not occurring in their communities or for whom the benefits of such a system may not be accessible. The notion of equity suggests that no individual or group should be disproportionately harmed or systematically excluded from the benefits brought about through public investments. Segments of society which may disproportionately receive benefits or experience costs associated with decisions may include groups associated with particular income levels, geographic locations, minority statuses, and other social categories. Low-income drivers may not be able to afford new vehicles equipped with connected vehicle technology and installation costs for retrofitting a vehicle with aftermarket equipment may be prohibitively high for these drivers. Providing subsidies to these low-income vehicle owners could address the dual goals of driving adoption of connected vehicle technology and mitigating equity issues.

COORDINATE OUTREACH AND EDUCATION PROGRAMS

The rationale for instituting a connected vehicle system still needs to be established with the general public. Educational initiatives and other forms of outreach (such as focus groups, demonstrations, pilot programs, and media events) that increase familiarity with connected vehicles and effectively communicate the benefits and convenience that can be accrued through the use of connected vehicle technologies will be crucial for gaining public support for system deployment. These programs allow experts to demonstrate to the public that a connected vehicle system is a logical, sustainable solution and that the costs of the system are far outweighed by the benefits. Focus group research has shown that drivers would be more accepting of new programs if the reason for the change is clearly explained (Baker and Goodin 2011). Public acceptance may hinge on drivers understanding specifically why data is being collected, feeling that only necessary data is being collected, and perceiving benefits to data collection. If these criteria are not met, the public may not support the use of connected vehicle technology (Briggs and Walton 2000).

DETERMINE GOVERNANCE AND OWNERSHIP OF DATA

There has been significant discussion as to whether ITS data ought to be collected and managed by public or private organizations. It is unclear whether the public or private sector is more capable of protecting proprietary data. The argument could be made that private sector organizations would be ethically safer options because federal and state FOIA requirements would pose privacy issues, and there are questions of whether publicly held data could be more easily used by law enforcement personnel for issuing citations if the data were held by a public organization. On the other hand, public ownership and management of data could be more consistent with the use of ITS data to provide public benefits, and there is concern that the profit-driven private sector may sell data that would not be released by the public sector. When considering the advantages and drawbacks of involving the public and private sector in the collection and management of ITS data, perhaps the most important predictor of how the data will be treated is not whether the organization is public or private, but rather its goals and operating characteristics (Briggs and Walton 2000).

Many of the above weaknesses of public and private ownership of data have caveats or can be remedied. While it is unclear whether connected vehicle data held by public entities would be publicly accessible under FOIA, public agencies can take actions to protect the data by requesting rulings from their attorneys general determining whether the data are exempt under current law or by seeking new exemptions from legislatures. In addition, it is unlikely that connected vehicle data would be used for traffic enforcement purposes as none of the public ITS agencies currently allow data to be accessed for these purposes (data that has been used by law enforcement has been for purposes such as apprehending serious criminals and accident investigations, uses which have not faced public opposition). Given that a privately managed connected vehicle system will require the use of contracts guaranteeing privacy protections and disclosing the potential uses of data, improperly releasing personal data would undermine the trustworthiness of the organization and discourage adoption of connected vehicle technologies. Thus, a private organization will likely have little incentive or legal ability to use personal data against the wishes of its customers (Briggs and Walton 2000).

CREATE PUBLIC-PRIVATE PARTNERSHIPS TO COLLECT, MANAGE, AND DISSEMINATE DATA

The public cost of deploying a connected vehicle system could be prohibitively high; however, by creating partnerships between public and private entities, some of the deployment costs could be covered by private sector partners who would benefit/profit from deployment. In addition to decreasing the public share of deployment costs, public-private partnerships to manage connected vehicle systems could be beneficial in many other ways, such as improving trust in the system, strengthening privacy protections, and efficiently disseminating data to stakeholders.

Public acceptance will hinge on drivers trusting the institutional setup for collection, management, and security of data from a connected vehicle system. Public-private partnerships can be used in the institutional design of a legitimate connected vehicle system that separates functions to protect privacy while ensuring that various stakeholders have access to data that can be used to generate public and private benefits. Institutional separation could be used to generate trust and support; for instance, if the activities of tracking and identifying vehicles are divided between two different organizations, it poses less of a threat to potential privacy invasion than if the same organization was involved with both tracking and identifying the vehicles (Briggs and Walton 2000).

The data collected through connected vehicles and other ITS applications could potentially be useful for purposes not related to the drivers themselves. For instance, the data could be used by state departments of transportation or other road managers for analyzing road use patterns and planning maintenance and improvements (transportation asset management). Data could also be useful to other users such as university researchers, economic developers, and businesses. By including many of these stakeholders in public-private partnerships, issues with accessibility and privacy concerns can be effectively resolved in a flexible and cooperative manner.

Licensing agreements could allow organizations access to data under controlled conditions and for legitimate purposes. Sharing could be done through the data collecting agency itself, or may involve a third party which would gather data, remove any individually identifiable information, and make it available to interested organizations. Such work is already being done with certain data sets with organizations such as Smart Route Systems, ETAK, and the Texas Transportation Institute (Briggs and Walton 2000).

DEVELOP EFFECTIVE INFORMATION TECHNOLOGY STRATEGIES

The use of information technology (IT) tools, methods, and practices are becoming increasingly important among transportation agencies. Any issues associated with IT risks must be addressed to reduce their negative impacts on data security, privacy, and data sharing.

Generally speaking, IT issues will affect all major tasks of transportation data management and ITS programs, including:

- Data collection
- Data archiving/storage
- Data processing
- Data analysis
- Reporting/dissemination
- Data sharing
- Data access

Taking effective preventative measures to ensure against the possibility of information privacy infringement will have significant impacts on the success of IT risk management. Outsourcing data management and IT operations to a third party are often used by public and private sectors in order to reduce internal privacy liability. In dealing with service suppliers, privacy-related risk management practices could become even more important, particularly when service suppliers are handling personal information on your behalf. It is important to assess the security policies and procedures related to personal information, system security, and experiences before a service provider is selected.

INTEGRATE ITS DATA COLLECTION AND INFORMATION SHARING POLICIES INTO EXISTING DATA MANAGEMENT STRATEGIES

In the course of developing the Transportation Management System (TMS), MDOT has already undertaken significant efforts to develop comprehensive data integration strategies, including data gathering, storage, and dissemination. The process consisted of identifying which data were needed; developing data definitions; and determining who was responsible for the data. To date, MDOT has reduced approximately 20,000 files to five major databases (MDOT, 2009).

Similar to TMS efforts, the Michigan Department of Technology, Management & Budget (DTMB) recently developed a transportation data stewardship enhancement plan and statewide GIS busi-

ness plan. These policy guidelines, together with TMS and other MDOT data systems, will provide a solid foundation for developing integrated ITS data collection and information sharing policies in Michigan - in particular in the areas of which agencies could be legally allowed to use the data, the level of detail to which agencies could reasonably have access, how long the agencies could have access to the data, and for what purposes the agencies could use the data. More detailed analysis and policy suggestions will be presented in the follow on report, "Analysis of Management Procedures for Data Collected via ITS."

VIII. CONCLUSIONS

Deployment of intelligent transportation systems and connected vehicle applications will result in benefits for drivers and public transportation agencies through improvements to transportation system efficiency, safety, and traveler convenience. Despite these benefits, there are several ethical and legal concerns that must be addressed to the satisfaction of all parties before successful deployment can take place, particularly the development of fully connected transportation system. This study provides specific recommendations regarding to these ethical and legal concerns relating to the collection, management, and use of ITS and connected vehicle data.

Privacy implications of connected vehicle technologies are becoming a bigger concern for many transportation organizations and further assessment of privacy protection mechanisms is needed for both public and private sector applications. As a recognized leader in ITS and connected vehicle technology, MDOT has identified the protection of citizen privacy in the collection, management, and use of transportation data as a high priority. Specifically, the recommendations proposed in this study address several of the ethical issues surrounding ITS technologies and connected vehicle applications.

LESSONS FOR MICHIGAN

Michigan has a long history of being in the vanguard of automotive technology. MDOT has already deployed many ITS applications and successfully dealt with associated legal and ethical issues. Many additional applications are in varying stages of deployment and research, and in coming years, other applications not even being considered yet may become commonplace in Michigan. As new ITS applications become increasingly advanced and data driven, effectively mitigating risks associated with data security, privacy, use, sharing, and other issues will become more involved. MDOT has already shown foresight by considering the legal and ethical issues associated with ITS and connected vehicles and by commissioning this study to further explore these issues. As new technologies mature and ready for deployment on roads, MDOT should maintain a precautionary attitude and consider the recommendations contained in this report as well as the ITS principles which have been published by other organizations in order to design systems, policies, and operating procedures that advance the state of technology on Michigan's roads while protecting its citizens and limiting the agency's exposure to legal uncertainties.

LESSONS FOR THE BROADER ITS COMMUNITY

Though this study was conducted with a focus on Michigan and MDOT, the content of this paper is broadly applicable to other state DOTs as well as other government agencies, companies, universities, and non-profit organizations involved with ITS and connected vehicle technologies. A better understanding of the legal and ethical considerations needed to deploy such technologies could lead to more productive partnerships. As these partnerships develop and various organizations gain experience with specific ITS applications, that experience and the systems and operating procedures developed can be shared with other organizations to help spread ITS applications broadly across the nation.

REFERENCES

Andersen, M.S. and Kjærgaard, M.B. (2011). Towards a New Classification of Location Privacy Methods in Pervasive Computing. Aarhus University. <https://pure.au.dk/portal/files/42117951/andersen2011.pdf>

Andrews, Scott and Cops, Michael. (2009). "Final Report: Vehicle Infrastructure Integration Proof of Concept Executive Summary – Vehicle." The VII Consortium. Produced for Research and Innovative Technology Administration, U.S. Department of Transportation. <http://ntl.bts.gov/lib/31000/31000/31079/14443_files/14443.pdf >.

Angwin, Julia. (2011). "Judge Declares Law Governing Warrantless Cellphone Tracking Unconstitutional." Wall Street Journal. November 16, 2011. <http://blogs.wsj.com/digits/2011/11/16/judge-declares-law-governing-warrantless-cellphone-tracking-unconstitutional/>.

Angwin, Julia and Jess Bravin. (2012). "U.S. Argues to Preserve GPS Tracking." Wall Street Journal. May 31, 2012. <http://online.wsj.com/article/SB10001424052702303552104577438570632493222.html?mod=googlenews_wsj>.

Associated Press. (2011). "Federal judge: GPS use illegal in Chicago-Kentucky drug bust." Chicago Tribune. May 23, 2012. <http://www.chicagotribune.com/news/local/breaking/chi-federal-judge-gps-use-illegal-in-chicagokentucky-drug-bust-20120523,0,2138257.story>.

Baker, Richard and Ginger Goodin. (2011). "Exploratory Study: Vehicle Mileage Fees in Texas." Texas Transportation Institute, Texas A&M University System. Produced for the Texas Department of Transportation. January 2011. <http://tti.tamu.edu/documents/0-6660-1.pdf>.

Barrett, James E. (1978). "580 F. 2d 1382 - United States v. Shovea." United States Court of Appeals, Tenth Circuit. July 27, 1978. <http://openjurist.org/580/f2d/1382/united-states-v-shovea>.

Boyd, Danah. (2010). "The Future of Privacy: How Privacy Norms Can Inform Regulation." 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem, Israel. October 29, 2010.

Briggs, Valerie A. and Walton, C. Michael. (2000). "The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data." Center for Transportation Research, University of Texas at Austin. May 2000. <http://swutc.tamu.edu/publications/technicalreports/472840-00075-1.pdf>.

Campbell, Levin H. (1977). "562 F. 2d 106 - United States v. H Moore." United States Court of Appeals, First Circuit. September 9, 1977. <http://openjurist.org/562/f2d/106/united-states-v-h-moore>.

Constitution Project. (2011). "Liberty and Security Committee Statement on Location Tracking: A Report by the Constitution Project's Liberty And Security Committee." The Constitution Project. September 21, 2011. <http://www.constitutionproject.org/pdf/LocationTrackingReport.pdf>.

Cornell. (2011). "Fourth Amendment: An Overview." Legal Information Institute, Cornell University Law School. Website. Accessed December 21, 2011. <http://www.law.cornell.edu/wex/Fourth_amendment>.

Courier. (2011). "Judge Should Approve Police GPS Tracking." The Courier. November 28, 2011. <http://www.thecourier.com/opinion/editoral/2011/Nov/28/ar_ed_112811.asp?d=112811,2011,Nov,28&c=e_0>.

DOJ. (2012). "FOIA Resources" U.S. Department of Justice. Accessed February 16, 2012. <http://www.justice.gov/oip/foia-resources.html>.

Douma, Frank, and Jordan Deckenbach (2009). The Challenge of ITS for the Law of Privacy. JOURNAL OF LAW, TECHNOLOGY & POLICY. Vol. 2009 No. 2.

Douma, Frank, and Sarah Aue (2011). ITS and Locational Privacy: Suggestions for Peaceful Coexistence. Center for Transportation Studies, University of Minnesota. October 2011.

Durkee, Musetta. (2010). "Privacy Expectations in the Use of GPS Tracking Devices: United States v. Maynard." BOLT, Berkeley Technology Law Journal. November 4, 2010. <http://btlj.org/2010/11/04/privacy-expectations-in-the-use-of-gps-tracking-devices-united-states-v-maynard/>.

Economist. (1999). "Data Dogfights." The Economist. January 7, 1999. <http://www.economist.com/node/181224>.

Fries, Ryan N.; Mashrur Chowdhury; and Mostafa Reisi Gahrooei. (2010). "Maintaining Privacy While Advancing Intelligent Transportation Systems-An Analysis." Transportation Research Board 2011 Annual Meeting. January 23-27, 2011. <http://www.siue.edu/~rfries/2011-TRB-Privacy%20with%20ITS.pdf>.

Gatto, Katie. (2011). "Is It Legal for Your Cellphone to Track You?" MSNBC. November 21, 2011. <http://www.msnbc.msn.com/id/45394735/ns/technology_and_science-security/>.

GPS.gov. (2011). "Geolocation Privacy and Surveillance Act." GPS.gov. Website. November 7, 2011. <http://www.gps.gov/policy/legislation/gps-act/>.

Gregory, Nina. (2012). "New Ways To Think About Online Privacy." National Public Radio. February 29, 2012. <http://www.npr.org/blogs/alltechconsidered/2012/02/29/147669008/new-ways-to-think-about-online-privacy>.

GWU. (2012). "FOIA Basics." The National Security Archive, George Washington University. Accessed February 16, 2012. <http://www.gwu.edu/~nsarchiv/nsa/foia/guide.html>.

Hoh, Baik, Marco Gruteser, Hui Xiong, and Ansaf Alrabady (2006). Enhancing Security and Privacy in Traffic-Monitoring Systems. PERVASIVE Computing. 1536-1268/2006s

Hoh, Baik et al (2008). Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring. MobiSys'08, June 17–20, 2008, Breckenridge, Colorado, USA.

Iqbal, Muhammad Usman (2009). LOCATION PRIVACY IN AUTOMOTIVE TELEMATICS. The University of New South Wales. 25 August 2009

ITSA. (2001). "Fair Information and Privacy Principles." Intelligent Transportation Society of America.

Jacobson, Leslie. (2007). "Vehicle Infrastructure Integration Privacy Policies Framework Version 1.0.2." Prepared for the Institutional Issues Subcommittee of the National VII Coalition. February 16, 2007. <http://www.nevadadot.com/uploadedFiles/NDOT/Micro-Sites/VMTFeeNV/NS_privacy-policy.pdf>.

Johnson, Bobbie. (2010). "Privacy no longer a social norm, says Facebook founder." The Guardian. January 10, 2010. <http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy>.

Johnson, Carrie. (2012). "FBI Still Struggling with Supreme Court's GPS Ruling." National Public Radio. March 21, 2012. <http://www.npr.org/2012/03/21/149011887/fbi-still-struggling-with-supreme-courts-gps-ruling>.

Lamberth, Royce C. (2011). "In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number XXX." United States District Court for the District of Columbia. October 12, 2011. <http://legaltimes.typepad.com/files/lamberth_ruling.pdf>.

Lwin, K.K. and Y. Murayama (2011). Web-Based GIS System for Real-Time Field Data Collection Using Personal Mobile Phone. Journal of

Geographic Information System, 2011, 3, 382-389.

Madsen, Barbara. (2003). "State v. Jackson" Supreme Court of Washington. September 11, 2003. <http://caselaw.findlaw.com/wa-supreme-court/1346233.html>.

McCullagh, Declan. (2010) "Feds Push for Tracking Cell Phones." CNET News. February 11, 2010. <http://news.cnet.com/8301-13578_3-10451518-38.html>.

MDOT (2009). Transportation Asset Management Data Collection. <http://www.michigan.gov/documents/collection_16542_7.pdf>

MTTLR. (2011). "United States v. Antoine Jones: GPS Tracking, Privacy Expectations, and Public Places." Michigan Telecommunications and Technology Law Review. October 1, 2011. <http://www.mttlrblog.org/2011/10/01/united-states-v-antoine-jones-gps-tracking-privacy-expectations-and-public-places/>.

Newmarker, Chris. (2007). "E-ZPass records out cheaters in divorce court: E-toll devices used to prove cheaters 'took the off-ramp to adultery.'" Associated Press. August 10, 2007. <http://www.msnbc.msn.com/id/20216302/>.

Nojeim, Greg. (2011). "Court Rules that Warrant Is Required for Stored Cell Site Location Information." Center for Democracy & Technology. September 12, 2011. <http://www.cdt.org/blogs/greg-nojeim/129court-rules-warrant-required-stored-cell-site-location-information>.

Persad, Khali; C. Michael Walton; and Shahriyar Hussain. (2007). "Electronic Vehicle Identification: Industry Standards, Performance, and Privacy Issues." Center for Transportation Research, University of Texas at Austin. Performed for Texas Department of Transportation. January 2007. <http://www.utexas.edu/research/ctr/pdf_reports/0_5217_P2.pdf>.

Pethtel, Ray D.; James D. Phillips, and Gene Hetherington. (2011). "A Policy Review of the Impact Existing Privacy Principles Have on Current and Emerging Transportation Safety Technology." National Surface Transportation Safety Center for Excellence, Virginia Tech Transportation Institute. May 12, 2011. <http://scholar.lib.vt.edu/VTTI/reports/PrivacyFinalReport_05122011.pdf >.

Phillips, Harry. (1980). "628 F. 2d 938 - United States v. Bailey." United States Court of Appeals, Sixth Circuit. July 31, 1980. <http://openjurist.org/628/f2d/938/united-states-v-bailey>.

Plotnikov, M., et al. Evaluating the Impacts of Placing Tolls on Interstate Highways. University of Massachusetts – Amherst. TRB 2012 Annual Meeting.

Rehnquist, William. (1983). "460 U.S. 276 - United States v. Knotts." Supreme Court of the United States. March 2, 1983. < http://openjurist.org/460/us/276/united-states-v-knotts>.

Riley, Dorothy C. (1991). "Swickard v Wayne County Medical Examiner." Michigan Supreme Court. September 19, 1991. <http://www.leagle.com/xmlResult.aspx?xmldoc=1991974438Mich536_1953.xml&docbase=CSLWAR2-1986-2006>.

Robinson, R. (1984). "Mullin v Detroit Police Department" Michigan Court of Appeals. March 20, 1984. <http://174.123.24.242/leagle/xmlResult.aspx?xmldoc=1984179133MichApp46_1174.xml&docbase=CSLWAR1-1950-1985>.

Scalia, Antonin. (2001). "533 U.S. 27 - Danny Lee Kyllo v. United States." Supreme Court of the United States. June 11, 2001. <http://openjurist.org/533/us/27/danny-lee-kyllo-v-united-states>.

Schuette, Bill. (2012). "Freedom of Information & Open Meetings Acts." State of Michigan Attourney General Bill Schutte. Website. Accessed February 2012. <http://www.michigan.gov/ag/0,4534,7-164-20988_18160---,00.html>.

Steinfeld, Aaron (2010). Ethics and Policy Implications for Inclusive Intelligent Transportation

Systems. Carnegie Mellon University. <http://www.cs.cmu.edu/~astein/pub/Steinfeld_IQS10.pdf>

Stephens, Catherine A. (2008). "Caution! Government Intrusion May Be Closer than It Appears: The Seventh Circuit Considers GPS Devices under the Fourth Amendment." Seventh Circuit Review. Volume 3(2): 617-657. <http://www.kentlaw.edu/7cr/v3-2/stephens.pdf>.

Stewart, Potter. (1981). "389 U.S. 347 - Katz v. United States." Supreme Court of the United States. December 18, 1967. <http://openjurist.org/389/us/347/katz-v-united-states>.

Tatel, Jennifer. (2012). "Privacy and Security of Information Stored on Mobile Communications Devices." Federal Communications Commission. Federal Register. Volume 77, Number 114. June 13, 2012.

Underwood, Steven E.; Cook, Steven J.; and Tansil, William H. (2008). "Line of Business Strategy for Vehicle-Infrastructure Integration, Part I: Strategic and Business Plan, Vision of Partnership and National Leadership." Michigan Department of Transportation. June 30, 2008. <http://www.michigan.gov/documents/mdot/MDOT_Michigan_DOT_VII_Strategic_and_Business_Plan_Executive_Summary_269460_7.pdf>.

USDOT Research and Innovative Technology Administration (2010). Real-Time Traveler Information Market Assessment White Paper. February 2010.

Volpe. (2008). "Technology Applications for Traffic Safety Programs: A Primer." Volpe National Transportation Systems Center, Research and Innovative Technology Administration, U.S. Department of Transportation. Produced for National Highway Transportation Safety Administration. <http://www.nhtsa.gov/DOT/NHTSA/Traffic%20Injury%20Control/Articles/Associated%20Files/811040.pdf>.

Wahls, Myron H. (1997). "Herald Co. v Ann Arbor Public Schools" Court of Appeals of Michigan. September 11, 1997. <http://scholar.google.com/scholar_case?case=15044337490468776327>.

Wang, Jessa Liying, and Michael C. Loui (2009). Privacy and Ethical Issues in Location-Based Tracking Systems. 2009 IEEE.

White, Byron. (1984). "468 U.S. 705 - United States v. Karo." Supreme Court of the United States. July 3, 1984. <http://openjurist.org/468/us/705/united-states-v-karo>.

Witham, William L. (2006). "Biddle v. State" Superior Court of Delaware. February 14, 2006. <http://courts.delaware.gov/OPINIONS/download.ASPx?ID=75110>.

APPENDIX A. ABBREVIATIONS

ANPR – Automatic Number Plate Recognition

APTS – Advanced Public Transportation Systems

ATIS – Advanced Traveler Information System

ATMS – Advanced Transportation Management Systems

CAR – Center for Automotive Research

CS – Communication Server

DSRC – Dedicated Short Range Communication

DTMB – Michigan Department of Technology, Management & Budget

ETC – Electronic Toll Collection

FHWA – Federal Highway Administration

FOIA – Freedom of Information Act

GPS – Global Positioning System

IT – Information Technology

ITIF – Information Technology & Innovation Foundation

ITS – Intelligent Transportation Systems

ITSA – Intelligent Transportation Society of America

LBS – Location-Based Service

MDOT – Michigan Department of Transportation

NHTSA – National Highway Transportation Safety Administration

RFID – Radio-Frequency Identification

RITA – Research and Innovative Technology Administration

TMS – Transportation Management System

TS – Traffic Server

USDOT – United States Department of Transportation

V2I – Vehicle-to-Infrastructure

V2V – Vehicle-to-Vehicle

VII – Vehicle-Infrastructure Integration

VTL – Virtual-Trip-Lines

APPENDIX B. RELEVANT COURT CASES

SELECTED SUPREME COURT INTERPRETATIONS OF PRIVACY LAW

Katz V. United States (1967): This Supreme Court case clarified the nature of the "right to privacy" and the legal definition of a "search." The ruling reinterpreted the unreasonable search and seizure clause of the Fourth Amendment to include immaterial intrusion with technology as a search. The case also extended Fourth Amendment protection to all areas where a person has a "reasonable expectation of privacy" (Stewart 1967).

United States v. Knotts (1983): This Supreme Court case clarified privacy protections with respect to electronic surveillance devices. The specific device in question was a beeper that could be tracked from a short distance. The ruling indicated that such devices did not invade a legitimate expectation of privacy, and were therefore allowed, without a warrant, under the Fourth Amendment (Rehnquist 1983).

United States v. Karo (1984): This Supreme Court case further clarified privacy protections with respect to electronic surveillance devices. The specific device in question was a beeper that had been hidden in a can of ether. The ruling in this case was that the device constituted an unlawful search because it was done without a warrant and the beeper was used to monitor an individual within a private residence. The difference between Knotts and Karo cases is that while in the Knotts case, the information the police obtained could have been obtained by following the defendant on a public street, in the Karo case, the information the police obtained could not have been obtained without entering the defendant's home and therefore was considered an unreasonable search under the Fourth Amendment (White 1984).

United States v. Kyllo (2001): This Supreme Court case clarified privacy protections with respect to electronic surveillance devices. The specific device in question was a thermal imaging device which was used from a public vantage point to monitor the radiation of heat from a home. The Court ruled that using such a device was a "search" within the meaning of the Fourth Amendment, and therefore required a warrant. Similar to the Karo case, the police would not have been able to obtain the information without entering the defendant's home, so the Court considered the scan to be an unreasonable search under the Fourth Amendment (Scalia 2001).

SELECTED FEDERAL AND STATE COURT INTERPRETATIONS OF PRIVACY LAWS

United States v. Moore (1977): This district court case concluded that evidence obtained by using beepers to track movement violated the Fourth Amendment. The court found that a beeper "transforms the vehicle, unknown to its owner, into a messenger." The court required the establishment of probable cause before attaching a beeper. In the case of Moore, the court agreed that probable cause was satisfied, and that the use of the beepers was not an unreasonable search under the Fourth Amendment (Campbell 1977).

United States v. Shovea (1978): This U.S. appeals court case concluded that evidence obtained by using a beeper to track the vehicle of a suspected drug manufacturer did not constitute a violation of fourth amendment rights. The court noted that "The search of a motor vehicle, especially its exterior, is less intrusive and implicates a lesser expectation of privacy than otherwise applies under the general warrant requirement." The court also stated that "If there is probable cause, an automobile, because of its mobility, may be searched without a warrant in circumstances that would not justify a warrantless search of a house or office." Thus, the ruling allowed for a tracking device to be used without a warrant (Barrett 1978).

United States v. Bailey (1980): This U.S. appeals court case concluded that monitoring using a beeper constituted a search. Though in this particular case, the beeper device was installed in a drum of chemicals while it was still in possession of government agents and a warrant was obtained before the beeper was installed. Despite this, the

court ruled that the monitoring was a violation of Fourth Amendment rights because the defendant had a subjective expectation of privacy as shown by his attempt to keep chemicals in private areas and out of public view (Phillips 1980).

State v. Jackson (Washington State, 2003): This Supreme Court case clarified the need for a warrant when installing GPS tracking devices on vehicles. An appellate court ruled that warrantless installation of a GPS tracking device did not violate the Washington constitution. On the other hand, the Washington Supreme Court found that a warrant was required for installing GPS tracking devices on vehicles; however, the court still affirmed the defendant's conviction (Madsen 2003).

Biddle v. State (Delaware State, 2006): This Superior Court of Delaware case found the defendant guilty of violating a fellow civilian's right to privacy by attaching a GPS tracking device to a victim's vehicle (Witham 2006). The court explained its reasoning, stating:

It is true that persons have diminished expectations of privacy in automobiles on public roads. These automobiles can be visually tracked by the police, but the police do not have the unfettered right to tamper with a vehicle by surreptitiously attaching a tracking device without either the owner's consent or without a warrant issued by a court. If the police whose duty is to prevent and detect crime have no such right then a private person would have no such right without the permission of the owner of the vehicle. The right to privacy is a fundamental right in a free and civilized society. The increasing use of electronic devices is eroding personal liberty.

APPENDIX C. DRAFT FINAL ITS AMERICA FAIR INFORMATION AND PRIVACY PRINCIPLES

These fair information and privacy principles were prepared in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems. They have been adopted by ITS America in "draft final" form. The Privacy Task Group of the Legal Issues Committee will present these principles for review and comment to organizations and groups interested in privacy and ITS outside of ITS America during 1995. They will then be submitted for final adoption to the ITS America Legal Issues Committee, Coordinating Council, and Board of Directors.

The principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy makers, and the public as they develop fair information and privacy guidelines for specific intelligent transportation projects. Initiators of ITS projects are urged to publish the fair information privacy principles that they intend to follow. Parties to ITS projects are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements.

1. INDIVIDUAL CENTERED. Intelligent Transportation Systems (ITS) must recognize and respect the individual's interests in privacy and information use.

ITS systems create value for both individuals and society as a whole. Central to the ITS vision is the creation of ITS systems that will fulfill our national goals. The primary focus of information use is to improve travelers' safety and security, reduce travel times, enhance individuals' ability to deal with highway disruptions and improve air quality. Traveler information is collected from many sources, some from the infrastructure and some from vehicles, while other information may come from the transactions -- like electronic toll collection -- that involve interaction between the infrastructure and vehicle. That information may have value in both ITS and non-ITS applications. The individual's expectation of privacy must be respected. This requires disclosure and the opportunity for individuals to express choice.

2. VISIBLE. Intelligent transportation information systems will be built in a manner "visible" to individuals.

ITS may create data on individuals. Individuals should have a means of discovering how the data flows operate. "Visible" means to disclose to the public the type of data collected, how it is collected, what its uses are, and how it will be distributed. The concept of visibility is one of central concern to the public, and consequently this principle requires assigning responsibility for disclosure.

3. COMPLY. Intelligent Transportation Systems will comply with state and federal laws governing privacy and information use.

4. SECURE. Intelligent Transportation Systems will be secure.

ITS data bases may contain information on where travelers go, the routes they use, and when they travel, and therefore must be secure. All ITS information systems will make use of data security technology and audit procedures appropriate to the sensitivity of the information.

5. LAW ENFORCEMENT. Intelligent Transportation Systems will have an appropriate role in enhancing travelers' safety and security interests, but absent consent, government authority, or appropriate legal process, information identifying individuals will not be disclosed to law enforcement.

ITS has the potential to make it possible for traffic management agencies to know where individuals travel, what routes they take, and travel duration. Therefore, ITS can increase the efficiency of traffic law enforcement by providing aggregate

information necessary to target resources. States may legislate conditions under which ITS information will be made available. Absent government authority, however, ITS systems should not be used as a surveillance means for enforcing traffic laws. Although individuals are concerned about public safety, persons who voluntarily participate in ITS programs or purchase ITS products have a reasonable expectation that they will not be "ambushed" by information they are providing.

6. RELEVANT. Intelligent Transportation Systems will only collect personal information that is relevant for ITS purposes.

ITS, respectful of the individual's interest in privacy, will only collect information that contains individual identifiers which are needed for the ITS service functions. Furthermore, ITS information systems will include protocols that call for the purging of individual identifier information that is no longer needed to meet ITS needs.

7. SECONDARY USE. Intelligent Transportation Systems information coupled with appropriate individual privacy protection may be used for non-ITS applications.

American consumers want information used to create economic choice and value, but also want their interest in privacy preserved. ITS information is predictive of the types of goods and services that interest consumers, for example the right location for stores, hospitals, and other facilities. However, that same information might also be used to disadvantage and harm a consumer. Therefore, the following practices should be followed.

- ITS information absent personal identifiers may be used for ITS and other purposes.
- Other unrelated uses of ITS information with personal identifiers may be permissible if individuals receive effective disclosure and have a user friendly means of opting out.
- Data collectors will only provide personal information to private organizations that agree to abide by these privacy principles.

8. FOIA. Federal and State Freedom of Information Act (FOIA) obligations require disclosure of information from government maintained databases. Database arrangements should balance the individual's interest in privacy and the public's right to know.

In determining whether to disclose ITS information, governments should, where possible, balance the individual's right to privacy against the preservation of the basic purpose of the Freedom of Information laws to open agency action to the light of public scrutiny. ITS travelers should be presumed to have reasonable expectations of privacy for personal identifying information. Pursuant to the individual's interest in privacy, the public/private frameworks of organizations collecting data should be structured to resolve problems of access created by FOIA.

APPENDIX D. VEHICLE INFRASTRUCTURE INTEGRATION PRIVACY PRINCIPLES

The purpose of these Vehicle Infrastructure Integration (VII) Privacy Principles is to provide general guidance regarding privacy and personal information used in a National VII Program. The nine VII Privacy Principles are designed to reflect fair information practices that will help ensure that a National VII Program is implemented in a way that is properly respectful of reasonable privacy expectations on the part of personal information subjects. These principles were adapted from the privacy principles published in guidelines adopted by the Organization for Economic Cooperation and Development, as well as the National Information Infrastructure Privacy Principles (1995), and are ultimately based on Fair Information Practices (FIPs) widely used in both the public and private sectors. A National VII Program is in the process of development, with the precise roles of various public and private entities as yet undetermined. As a result, these privacy principles are stated in general terms. They express a commitment to respect the privacy and personal information of individuals who will participate in a National VII Program, if deployed.

The VII Privacy Principles discussed here are not implementation rules specifying rights, responsibilities, and enforcement measures within a National VII Program. The VII Privacy Policies Framework will later include a variety of implementation privacy rules for a National VII Program. These implementation privacy rules will be developed in the future based on these privacy principles and the privacy laws then-applicable to a National VII Program.

1. Principle of Respect for Privacy and Personal Information

Commitment to respect for individual privacy in a National VII Program means that VII-derived personal information should be acquired, retained, disclosed, and used only in ways that protect the privacy of individuals. Personal information users should collect, retain and use only anonymous information whenever possible. Users of VII-derived personal information and VII System administrators are expected to be accountable with regard to the personal information they collect and/or use in a National VII Program.

This first and most general privacy principle recognizes that VII will flourish only if a National VII Program is designed, built and operated so that personal information subjects are respected and privacy is protected. As the fundamental principle regarding privacy and personal information protection in a National VII Program, this principle reflects the realization that privacy and individual control over personal information deserve to be placed first as the most basic of a National VII Program's privacy principles. This principle emphasizes collection and use of anonymous information that is not linkable to any individual whenever possible. VII technology should be designed so that personal information is only collected or used when necessary. In other words, a deployed National VII Program should rely on anonymous information to the greatest degree possible. Accountability for proper treatment of personal information in the operation of a National VII Program will rest with personal information users and VII System administrators. Reflecting commitment to respect for individuals, this basic principle declares that a National VII Program will protect individual privacy and respect an individual's reasonable privacy expectations.

An individual's reasonable privacy expectations are not just an individual's subjective expectations of privacy. Such privacy expectations must also be recognized as reasonable by society. The concept of reasonable expectation of privacy under these VII Privacy Principles is not limited by what counts as a reasonable expectation of privacy under the Fourth Amendment of the United States Constitution. In many instances, society has deemed it reasonable to protect privacy at a level higher than that required by the Fourth Amendment. See, e.g., Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988); Right to Financial Privacy Act, 12 U.S.C. § 3401

(1988); Privacy Act, 5 U.S.C. § 552a (1988); Drivers Privacy Protection Act, 18 U.S.C. §§ 2721-2725; and Federal Communications Law and Regulations protecting wireless communications under 47 U.S.C. § 222. This Principle, and the VII Privacy Principles in general, anticipate that personal information users and VII System administrators in a National VII Program will comply with such existing and future laws and regulations, as well as these privacy principles.

This initial privacy principle is also based on the notion that individual privacy will be best protected when information subjects, information collectors, information administrators, and information users have a shared understanding about how personal information will be acquired, disclosed, and used in a National VII Program.

2. Information Purposes Principle

A personal information user should acquire, use, disclose and retain personal information only for valid purposes, consistent with the goals of a National VII Program, as described in the VII Privacy Limits, below. A personal information user should:

- inform a personal information subject about the purposes for which personal information will be collected, used or disclosed before collecting personal information from that subject so that the personal information subject can decide whether or not to agree to use of their personal information for those purposes;
- use and/or disclose personal information to third parties, only for valid purposes about which the information subject has been informed; and
- retain personal information for only as long as the information serves a valid purpose;
- limit the storage of personal information to a specified duration that should reflect the period of time necessary to fulfill the purpose for which personal information was collected. (See Information Protection and Retention Principle, below.)

Acquisition, use, disclosure and retention of personal information should be restricted to serving valid goals. The Privacy Limits on the Uses of Personal Information that follow these Privacy Principles, discusses some particular types of valid and invalid purposes for which personal information should and should not be collected, used and disclosed within or by the VII System, or by authorized National VII Program users and VII System administrators.

Before personal information is collected, information users should articulate specific, valid purposes for the use of such personal information collection. As reflected in the Notice and Acquisition Principles, below, personal information users should inform personal information subjects about these purposes and describe all intended uses of personal information before collecting personal information from individuals. If personal information will be disclosed to third parties by a personal information user, any such disclosure should be consistent with the purposes about which the information subject has been informed. These personal information purposes will normally be described at the time personal information is collected when the personal information subject is told about the intended uses and disclosures of his or her personal information.

When information about the purpose of a new use or disclosure has not been provided previously, personal information subjects should be informed of the purposes of any further personal information disclosure or use before such a new type of disclosure or use is made. One reason for such additional explanations of new purposes for personal information is to enable the personal information subject, who may have chosen to opt-in to a particular VII application, to reconsider that choice in light of additional disclosures or uses of his or her personal information. Indeed, information subjects should be given the opportunity to make an informed choice about continuing to participate in an application when the application's purposes for collecting personal information have changed. Where only anonymous information, including summarized or aggregated personal information is to be used or disclosed, no further notice should be necessary. Nevertheless, it is good practice to inform personal information subjects about plans for such aggregation

or summarization of personal information when the information is collected.

Encouraging clarity and completeness with regard to valid and announced purposes for collecting personal information from personal information subjects, this principle also fosters several kinds of beneficial privacy practices. Having to explain why personal information is being collected, used or disclosed tends to illuminate and often to eliminate, unnecessary personal information collection. In addition, these announced purposes provide the essential basis for informed consent by the information subject with regard to collection or disclosure of personal information. Moreover, articulation of the purposes for personal information collection provides a restraint against misuse of personal information for other purposes.

From the point of view of individuals who will use VII services and applications, articulated purposes for collecting personal information helps also to foster openness. Articulated purposes also provide assurance that a personal information subject will retain basic choices regarding whether or not to provide personal information.

These purpose requirements are intended to encourage elimination of personal information when there is no longer any valid purpose for keeping it. Retention of personal information after it has served articulated valid purposes that have been explained to the information subjects should be discouraged. (See the Information Protection and Retention Principle, below.)

3. Acquisition Principle

In acquiring personal information, a personal information user should:

- assess the potential impact on the privacy of personal information subjects;
- collect only personal information that is reasonably expected to support current or planned activities; and
- collect personal information consistently with valid purposes for information collection (See Information Purposes Principle, above) and the notices that the personal information user has provided to personal information subjects. (See Notice Principle below.)

Before acquiring personal information, personal information users should assess the potential impact of such information collection on privacy. Personal information collection should be limited to that reasonably expected to support currently planned activities that have been explained in advance to the personal information subjects who will provide personal information. Mere possibility of future use for an undefined potential project would not be a sufficient "planned activity" under this principle.

This Acquisition Principle recognizes that a critical characteristic of privacy is that once privacy is lost, it can rarely be restored. As a result, privacy protection needs to be addressed at the outset, and not merely considered as an afterthought subsequent to personal information acquisition. Under this principle, personal information users and information administrators should explicitly consider impacts on privacy as they design and operate VII networks and applications. Most important, personal information users and information administrators need to take seriously privacy impacts on personal information subjects in deciding whether and how to acquire or use personal information in the first place. It may be that anonymous information is sufficient for identified purposes. In such circumstances, only anonymous data should be acquired or used.

In assessing the privacy consequences of acquiring personal information, personal information users should consider the effects their activities may have on the lives of personal information subjects from whom personal information is acquired. The appropriateness of any particular acquisition or use of personal information will also be affected by other factors, such as public opinion and market forces, as well as the availability of technologies for rendering data anonymous.

Once a personal information user decides to acquire personal information in pursuit of a currently-planned activity, the personal information user should disclose the planned activity in advance to affected personal information subjects so that potential personal information subjects can make

informed choices regarding whether to provide personal information. In all cases, a personal information user should use both technical and administrative means to ensure that only that information reasonably expected to support those activities that have been disclosed in advance, in accordance with the Notice Principle below, are acquired. The purposes of the personal information acquisition should both be explained to information subjects and also be consistent with the Information Purposes Principle above.

Some VII applications will involve transactions that require disclosure of personal information. For example, if an individual chooses to purchase a VII navigation-assistance application, personal information in the form of transactional data will be generated that requires disclosure to predefined third parties in order to complete a financial transaction. Personal information acquired from such transactions should not be used or disclosed for any other purpose that was not defined and disclosed in advance to the personal information subject participating in the application. (See the Information Purposes Principle, above.) Moreover, VII System administrators who have access to or control over transactional processes for transmitting such personal information are also bound by this principle to the extent that such access and control has bearing on privacy protection.

4. Notice Principle

Before a personal information user collects personal information, the information user should provide effective advance notice to each information subject about:

- what personal information is collected;
- why the personal information is collected;
- how the personal information will be used;
- what steps will be taken to protect the confidentiality, integrity, and quality of the personal information;
- any opportunities to remain anonymous;
- the consequences of providing or withholding personal information;
- how long the personal information will be retained, and;
- rights of recourse and redress. (See Accountability Principle, below.)

The Notice Principle insists that appropriate prior notice be given to personal information subjects so that information subjects know in advance about personal information collection and how that personal information will be used. Such knowledge allows personal information subjects to make informed choices about whether, when and how to use VII applications that involve sharing information about themselves.

In the context of some opt-in services, the responsibility for providing notice may devolve upon several different personal information users in cases where multiple users are involved in providing the same opt-in service, depending upon the nature of the contractual agreement(s) that govern service provision. If the third party information user has a direct contractual relationship with the personal information subject, such as a bank that has issued a personal credit card to an information subject, then the responsibility to provide notice according to this principle rests with the third-party personal information user (i.e., bank that issued the credit card), rather than with the entity that originally acquired the personal information (i.e., a service provider). If, on the other hand, the third party information user is a sub-contractor to an entity that has contracted with a personal information subject to acquire personal information in order to provide a service, such as a concierge service provider subcontracted to a vehicle manufacturer to provide services to that manufacturer's customers, then responsibility to provide notice rests with the entity that originally acquires the personal information (i.e., the vehicle manufacturer), rather than with the sub-contracted third-party information user.

Under the Notice Principle, notification about any planned uses of personal information by third parties should be disclosed before that personal information is acquired. (See the Acquisition Principle, discussed above.) To the extent that personal information has been rendered anonymous, such as through aggregation and summarization, no additional notice would be necessary. Since

the information has ceased to be personal information, such use of anonymous information would not require additional notification under this aspect of the Notice Principle. Nevertheless, it is good practice to provide notice to personal information subjects regarding known or expected uses of anonymous information derived from personal information provided by information subjects.

This Notice Principle seeks to assure that personal information subjects are given sufficient advance information to make informed decisions about how their personal information will be used. The importance of providing adequate notice cannot be overstated because the content of the notice substantially determines a person's understanding of, and agreement to, how that individual's personal information will be used in a National VII Program. This understanding, choice and agreement should be respected by all subsequent users of that personal information. Non-personal, anonymous information would, of course, not be so restricted.

This principle specifically applies to personal information in the form of transactional data about individuals generated as by-products of financial transactions. All parties to transactions utilizing personal information derived from or through a National VII Program are expected to abide by this Notice Principle. This Notice Principle applies not only to the party principally transacting with the personal information subject (e.g., in providing a product or service), but also to transaction facilitators such as communication providers and electronic payment brokers who help to consummate financial transactions that make use of a National VII Program. As noted above, the responsibility for providing notice to personal information subjects in cases where opting-into a service requires that personal information be shared among multiple parties may vary, depending upon the nature of the contractual agreement(s) implemented for particular opt-in services.

The Notice Principle suggests some basic elements of adequate notice, but does not prescribe any particular form for that notice. Rather, the Notice Principle sets an objective of ensuring that a personal information subject will have sufficient, understandable information to make an informed decision regarding whether or not to choose a particular application. Ultimately, what counts as adequate, relevant information satisfying the Notice Principle will depend on the circumstances in which the personal information is collected. As a general matter, Notice would be adequate when it provides a personal information subject sufficient information to make informed decisions about whether to agree to use various VII services and applications.

5. Fair Information Use Principle

A personal information user should use personal information about an information subject only in ways that are compatible both with the notice provided by the information user (See Notice Principle above) and with the information subject's reasonable expectations regarding how the personal information will be used.

Personal information users should use personal information only in ways that are compatible with the personal information subject's understanding of and agreement to how it will be used. The Fairness Principle recognizes that a personal information subject's reasonable understanding of how personal information will be used, and the scope of the information subject's consent regarding use of personal information, are determined before the personal information is collected. A personal information subject's informed consent is predicated on advance notice of planned uses being provided by a personal information user. Such understanding and consent will depend both on the notice provided by a personal information user (See the Notice Principle, discussed above) and on information available to the individual pursuant to the Openness Principle, below. This Fair Information Use Principle seeks to limit use of personal information in a National VII Program to uses and purposes disclosed to personal information subjects when they consent to collection and use of their personal information.

Some personal information users may seek to use personal information in a manner inconsistent with information about use that was originally

provided when the personal information was collected. In such circumstances, before such changes in the use of personal information can legitimately be made, the information user should first notify affected personal information subjects and obtain their consent to any new use(s) of their information. The nature of the new use(s) will determine whether such consent should be express or implied. In some circumstances, the consequences to an individual may be so significant that the prospective new data use should proceed only if, and after, the personal information subject has expressly agreed to the new use of his or her personal information. In other circumstances where the new use of personal information has minimal consequences for individuals, a notice offering the personal information subject the ability to impliedly consent to a new use of personal information – for example, by continuing to participate in a VII application after the changed use has been described to the information subject – may be appropriate. The opportunity to cease participation in a VII application (i.e., an opt-out choice), may be adequate in some instances of implied consent. Additional uses of anonymous information (in contrast with new uses of personal information) would of course not require such additional notice.

Because all personal information users should abide by the Fair Information Use Principle, both transferors and transferees of personal information derived from or through the VII System are responsible for ensuring that a personal information subject's understanding regarding limits on permitted uses of the personal information is transferred along with the personal information. Since this principle applies not only to primary personal information users, but also to any subsequent users of the personal information, any use of personal information should be compatible with the personal information subject's understanding of the uses to be made of his or her personal information, based in part on the notice provided under the Notice Principle, above. In determining whether a specific new use of personal information is "incompatible" with the information subject's understanding, personal information users should evaluate whether a particular personal information use was expressly disclosed in the original notice about personal information uses and is otherwise consistent with the notice. Uses of personal information beyond these conditions are incompatible with the Fair Information Use Principle.

The Fair Information Use Principle involves balancing. It will not apply uniformly in every setting. An incompatible use is not necessarily an unfair use; in fact, some incompatible uses may be extremely beneficial to the personal information subject and to society. Some incompatible uses may produce great societal benefits and have at most a trivial effect on the personal information subject or on her or his privacy. For example, in conducting a statistical study that examines traffic safety data in order to develop improved countermeasures, in which no individual information subject is identifiable, use of summarized and aggregated information will result in no impact on any personal information subject or his or her privacy. Such anonymous studies can have significant benefits in terms of improved traffic safety systems and policies. Obtaining the consent of each personal information subject to permit further statistical uses of already existing anonymous data would have no impact on any individual's privacy interests. However, personal information users should inform the personal information subject about potential uses even of such personal information that has been rendered anonymous through aggregation and summarization.

6. Information Protection and Retention Principle

Within a National VII Program, the VII System's technical architecture and structure should be designed to implement advanced security and other technologies to protect personal information against improper collection, disclosure or misuse in ways that may affect the privacy interests of personal information subjects..

Personal information users and information administrators should apply administrative, physical and technical controls appropriate to the protection of personal information derived from or ob-

tained through the VII System. Particular attention should be given to:

- maintaining the security of personal information;
- protecting confidentiality of personal information against improper access; and
- assuring the quality and integrity of personal information collected or maintained.

Personal information users and information administrators should only retain personal information that is relevant to a valid purpose and only for as long as, and to the extent that, the information is protected against improper access, disclosure or use. Personal information users and information administrators should have data storage procedures that assure appropriate, secure disposal of personal information:

- when there is no longer a valid purpose for retaining the personal information, or
- when a stated or required time limit on data retention has been reached, or
- when data transmission has been completed within the VII System.

Identifiers, such as data addresses (potentially identifying a data source) captured during transmission or transport of data within the VII System should not be retained longer than is necessary to accomplish the data transport or transmission.

Personal information users and information administrators should use technical, physical and administrative measures to protect the confidentiality and integrity of personal information. The VII System should be designed so as to limit the potential for problems regarding information quality and security. For example, strong encryption of personal information transmitted through the VII System will greatly reduce risk of unauthorized access, as well as disclosure, alteration, or destruction of personal information.

In addition, not retaining personal information any longer than necessary for valid purposes is a particularly important and useful protection for personal information. These retention limitations apply both to administrative controls on personal information users and to VII System administrators in a National VII Program, and include technical VII System controls that automatically delete personal information that may be incidental to accomplishing data transmission with the VII System. For example, MAC addresses should be deleted promptly at the conclusion of a private service transaction requiring communication through more than one consecutive RSU along a particular vehicle's travel route.

Personal information should be retained only to serve explicit purposes that have been disclosed to information subjects. Retention of personal information for extended period or for other potential purposes is inconsistent with this Information Protection and Retention Principle. Personal information users should adopt time-limits on storage of personal information, inform personal information subjects about such time limits, and abide by them in actual operations.

Robust processes must be implemented by National VII Program users and VII System administrators to maintain the privacy and integrity of personal information derived from the National VII Program. In determining what controls are appropriate, personal information users and information administrators should recognize an important obligation to manage personal information in a manner that protects it from inadvertent disclosure, as well as from intentional misuse and abuse. Preparations to react quickly and effectively in the event of a security breach should be evaluated in advance. It is likely to be difficult to keep out unauthorized users, such as a hacker or cracker. Such intruders may either seek access to personal information stored in a personal information user's database or make hard-to-detect changes in such data that would then be relied upon in making critical decisions. As a result, risks of potential security breaches should be analyzed on an ongoing basis, and measures taken to minimize threats. In addition to information security threats posed by unauthorized users (i.e., hackers and crackers), information security and privacy protection may also be threatened by authorized VII System users and information administrators. In general, this type of threat is both

inherently more detrimental and harder to detect than unauthorized breaches. VII System designers and information administrators responsible for technical information security solutions should therefore avoid the temptation to focus on security solutions that aim to "catch" unauthorized users at the necessary expense of increasing exposure to threats from authorized VII System users and administrators.

In protecting personal information, personal information users and information administrators should adopt a multi-faceted approach that includes both technical and administrative controls, as well as physical security. Among important technical controls, personal information users and information administrators should encrypt personal information whenever possible. In addition, administrative controls, such as computerized audit trails, should be implemented to help detect and eliminate any improper access to personal information. Employees with access to personal information should be appropriately trained in proper data handling and management techniques, and be carefully supervised to prevent inadvertent or deliberate lapses. Personal information users should establish policies that clearly forbid the use of personal information acquired for one activity from being used for another, unrelated activity as stated in the Purposes Principle, above. Regular data storage limitations and disposal procedures should similarly restrict how long personal information is retained.

Personal information should be of sufficient quality to be relied upon for purposes that may have consequences for personal information subjects, personal information users or both. This means that personal information should be accurate, timely, relevant and complete for the purposes and uses for which it was collected and about which information subjects have been notified as contemplated in the Notice Principle, above. Maintaining only relevant personal information is particularly important in preventing the pernicious tendency for data acquisition to spawn "mission creep." The fact that personal information collected for one purpose could also be useful in serving other possible purposes does not justify retaining personal information for later uses serving new purposes that have not been explained in advance to personal information subjects. Any such expansion of use would be inconsistent with both the Notice Principle and the Purposes Principle discussed above.

In a National VII Program, both personal information subjects and personal information users, should be able to rely on the integrity of personal information derived from the Program. Thus, personal information users should protect personal information against improper alteration or destruction either by employees of personal information users or by unauthorized intruders into information systems containing personal information derived from the National VII Program. Similarly, VII System administrators should protect personal information against improper alteration or destruction that may result from inadvertent or malicious intervention into data management processes during data transport within the VII System. Advance planning to prevent, detect and eliminate every intrusion or attempted data alteration will be an important responsibility of personal information users and information administrators. Providing information subjects with access to information that is collected and stored about them (See the Participation Principle below) is one effective means to ensure integrity and quality of personal information used in a National VII Program.

7. Openness Principle

Personal information users and information administrators:

- should be informed about privacy issues and the best ways to protect personal information derived from the National VII Program;
- should inform prospective personal information subjects about personal information the personal information user collects through the National VII Program; and
- should explain to personal information subjects protections for personal information derived from National VII Program, and the length of time personal information will be retained by the personal information user.

Personal information subjects should be able to rely on personal information users for adequate information about:

- the nature and extent of personal information collected from them;
- the purposes for which such personal information is collected;
- the uses of personal information made by personal information users;
- the opportunity not to provide personal information;
- the protections for confidentiality, integrity, and quality of personal information;
- the consequences of providing or withholding personal information;
- opportunities to remain anonymous; and
- rights of recourse and redress for misuse of personal information. (See Accountability Principle, below.)

The Openness Principle addresses the need for transparency in a National VII Program. Personal information users, information administrators, and personal information subjects need to be able to make informed decisions regarding what personal information is collected and used, and how it will be protected within the National VII Program. Such transparency with regard to personal information practices helps to reassure personal information subjects that their privacy interests are understood and reasonably protected through the National VII Program design, security, access policies, and other measures. Openness is intended to encourage personal information users and information administrators to adopt coherent privacy protection processes and policies that users have articulated both internally and in communications to personal information subjects who participate in a National VII Program. In doing so, personal information users should seek current, reliable information about potential privacy issues and the best ways to maintain the privacy of personal information.

Traditionally, government has educated the public regarding matters of rights and responsibilities. If a National VII, Program is deployed, government agencies will continue to play a leading educational role. However, as design and implementation participants in a National VII Program, the private sector also has a crucial role in informing information users, information administrators, and personal information subjects about privacy issues. Typical opportunities for education designed to help information subjects understand personal information practices in a National VII Program should involve Internet privacy "help" sites and published privacy compliance guidelines. Comprehensive marketing and publicity campaigns should provide clear explanations by National VII Program information users of how they deal with personal information. The overall goal of the Openness Principle is to assure that personal information users, information administrators, and personal information subjects remain well-informed and up-to-date regarding privacy issues, including effective privacy protection strategies within a National VII Program.

Since all possible privacy consequences of use of personal information in a National VII Program cannot be anticipated, personal information subjects may not initially be aware of how their lives could be affected by personal information collected in such a Program. As a result, it is important that personal information subjects, information administrators, and personal information users continue to engage in a shared understanding of how a National VII Program affects personal information privacy.

A personal information user should inform each personal information subject about all of the ways in which that information subject's personal information is collected and used by the personal information user. Similarly, each personal information subject also has the responsibility to understand the consequences of providing personal information in the course of using VII applications. For example, a VII toll collection authority may ask for personal information prior to permitting a customer to participate in electronic toll payment systems. In such a situation, one use for the personal information is clear – to process toll payments. To the extent that other uses are intended by the toll authority that are not so obvious, such as to generate traffic management data,

those other uses need to be brought to the attention of the information subjects, as well. Similarly, use of information about a toll customer's itinerary to contribute to an anonymous data base for highway planning purposes should be disclosed before the personal information from the toll authority is used for such a purpose. However, additional uses of already anonymous data, that no longer contain personal information, need not be repeatedly explained.

The Openness Principle is intended to make it possible for a personal information subject to actively shape the terms of his or her participation in a National VII Program. In general, when a personal information subject chooses whether and to what degree to participate in a VII application requiring disclosure of personal information to a personal information user, the information subject should take an active role in learning about the terms of such disclosure. Of course, if personal information subjects are to be responsible for their choices, they must be provided sufficient information to make informed decisions, including the potential decision not to participate in a VII application because it requires disclosure and use of personal information. This Openness Principle works in conjunction with the Notice Principle, above, to enable a personal information subject to take responsibility for whether or how his or her personal information will be disclosed and used in a National VII Program. The overall goal of this principle is to make uses of personal information clear so that each information subject has an opportunity to understand and evaluate the benefits and potential risks of choosing among VII applications and services, or of making the choice not to participate in applications that require personal information from them.

8. Participation Principle

In addition to receiving information regarding how personal information is collected and used in a National VII Program, each personal information subject should be expected to protect his or her own privacy. Personal information users should provide each personal information subject opportunities to:

- access personal information about himself or herself;
- correct any inaccurate personal information about the personal information subject;
- object to improper or unfair personal information use; and
- choose to remain anonymous, and not provide personal information.

Personal information subjects should participate in the protection of their own privacy. That means that a personal information subject needs to be given notice of personal information collected from or about him or her (See Notice Principle, above.), as well as access to the information subject's personal information held by a personal information user. A personal information subject should also be able to correct his or her personal information to the extent that it is demonstrated to be inaccurate. A personal information subject should also have the opportunity to object to improper or unfair use of his or her personal information. The nature of the means provided by a personal information user to enable a personal information subject to have access to, and the ability to correct, his or her personal information should depend on various factors, including the seriousness of the consequences to the information subject of continued use of erroneous personal information.

As a general matter, personal information subjects should have the opportunity to avoid personal information collection by remaining anonymous in their uses of a National VII Program. However, as explained in Limit 3, below, in some public-sector regulation and commercial vehicle permitting applications personal information may be required because of legislative or regulatory mandates. As a result, although anonymity is normally appropriate when a vehicle driver or occupant seeks, for example, information about nearby restaurants or parking facilities from a VII service provider, anonymity might not be possible under certain commercial vehicle applications, such as hazardous materials permits, for which personal information is required by law. In other VII services and applications, choice should be

the rule with regard to providing personal information.

9. Accountability Principle

A personal information user should respond to inquiries and complaints about interference with privacy interests or misuse of personal information, including use of personal information in ways that are incompatible with notice provided to information subjects (see Notice Principle, above). If an information subject has a complaint that he or she has been harmed by improper collection, retention, disclosure or use of his or her personal information by a personal information user, the information subject should have appropriate means to raise and resolve the complaint.

Personal information users should provide appropriate means for personal information subjects to raise privacy issues and to make complaints regarding interference with privacy interests. This Accountability Principle contemplates an internal process compatible with the operations of the personal information users. The implementation of privacy officers or boards, as well as other strategies, can be useful ways to carry out such privacy recourse functions. However implemented, an information user should provide an identified person or office that can respond formally and try to resolve privacy problems and complaints by personal information subjects.

This Accountability Principle does not determine whether improper action or harm has occurred in any particular instance or whether any specific form of resolution is required. Complaints from personal information subjects should be taken seriously when they involve claims that harm was suffered because personal information was misused, or was not accurate, timely, relevant, or complete, or was retained for longer than necessary. Providing resolution of complaints in the most timely and cost-effective manner should be the goal.