The Implications of Current and Emerging Privacy Law for ITS

Final Report

Prepared by:

Frank Douma
Jordan Deckenbach

Hubert H. Humphrey Institute of Public Affairs
University of Minnesota

CTS 08-26

Technical Report Documentation Page

1. Report No.	2.	3. Recipients Accession No.	
CTS 08-26			
4. Title and Subtitle The Implications of Current and Emerging Privacy Law for ITS		5. Report Date December 2008 6.	
7. Author(s) Frank Douma, Jordan Deckenbach		8. Performing Organization Report No.	
9. Performing Organization Name and Address State and Local Policy Program Hubert H. Humphrey Institute of Public Affairs University of Minnesota 301 19th Avenue South Minneapolis, Minnesota 55455		10. Project/Task/Work Unit No. CTS Project # 2008010 11. Contract (C) or Grant (G) No.	
12. Sponsoring Organization Name and Address Intelligent Transportation Systems Institute Center for Transportation Studies University of Minnesota 511 Washington Avenue SE, Suite 200 Minneapolis, Minnesota 55455		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code	
15. Supplementary Notes http://www.cts.umn.edu/Publications/ResearchReports/			
16. Abstract (Limit: 200 words) As Intelligent Transportation Systems (ITS) incorporate data-gathering and compiling systems into the transportation infrastructure, questions about privacy implications stemming from the potential misallocation or abuse of collected data have started to arise. The United States has no comprehensive national regulatory structure for privacy, leaving answers to these privacy questions to be found through a consideration of variety of sources of federal and state privacy law. In this paper, the authors examine a number of the areas where privacy law could impact ITS projects. To address these concerns, developers and planners of ITS technologies have to navigate a myriad of legal considerations and consequences that correspond with the ways in which they utilize the technologies and the information they collect. In an attempt to assist in that endeavor, the final part of this paper suggests tools for ITS developers and planners that explain the level of restrictions that correspond with different kinds of information being collected.			
17. Document Analysis/Descriptors ITS, Privacy, VII, automatic enforcement, vicarious criminal liability, vehicle data recorders, photo enforcement		18. Availability Statement No restrictions. Document available from: National Technical Information Services, Springfield, Virginia 22161	
19. Security Class (this report) Unclassified	20. Security Class (this page) Unclassified	21. No. of Pages 42	22. Price

The Implications of Current and Emerging Privacy Law for ITS[1]

Final Report

Prepared by

Frank Douma
Jordan Deckenbach

State and Local Policy Program
Hubert H. Humphrey Institute of Public Affairs
University of Minnesota

December 2008

Published by

Intelligent Transportation Systems Institute
Center for Transportation Studies
University of Minnesota
200 Transportation and Safety Building
511 Washington Ave. S.E.
Minneapolis, MN 55455

---

[1] A version of this article first appeared in the University of Illinois Journal of Law, Technology & Policy in Fall 2009 (Frank Douma and Jordan Deckenbach, *The Challenge of ITS for the Law of Privacy*, 2009 U.ILL.J.L.TECH. & POL'Y 295 (2009))

Acknowledgements

We would like to extend thanks to Steve Frooman, whose assistance in the early stages of this research set the foundation of this current work, the ITS Institute at the Center for Transportation Studies at the University of Minnesota for funding this project, and to Max Donath of the ITS Institute for bringing this topic to our attention. Financial support was provided by the United States Department of Transportation Research and Innovative Technologies Administration (RITA). Finally, this paper could never have been written without the input of Professor Stephen Simon of the University of Minnesota Law School, who provided valuable advice about the current state of privacy law, indispensible assistance in developing the privacy taxonomy and timely, on-point recommendations of multiple sources.

Table of Contents

List of Tables

List of Figures

Executive Summary

As Intelligent Transportation Systems (ITS) incorporate data-gathering and compiling systems into the transportation infrastructure, questions about privacy implications stemming from the potential misallocation or abuse of collected data have started to arise. Currently, the United States has no comprehensive national regulatory structure for privacy, leaving answers to ITS privacy questions to be found through a consideration of a variety of sources of federal and state privacy law.

The federal government has established a foundation for privacy protections through Supreme Court rulings and regulations aimed at stopping cases of abuse of privacy. Outside of these rulings and regulations, the federal government has deferred to the states in establishing privacy regulations. This results in a fractured approach to regulating ITS data and information utilization as different state courts and legislatures apply different levels of privacy restrictions.

Federal case law has developed protections based on the reasonableness of citizens' privacy expectations. The courts have found reasonable privacy expectations exist in an individual's home; however, no reasonable privacy expectation exists when an individual is driving a car since the activity is occurring in a public place. However, evolving technologies and their ability to record information not observable by the public at large have pushed the court to begin expanding privacy protections beyond the home. Though driving activities are unprotected now, the federal courts could find the invasiveness of developing ITS technologies violates the citizens' reasonable expectation of privacy even though the activity is taking place in public.

On a state level, privacy protections greatly vary. State laws, courts and constitutions all provide their own level of privacy protections, leaving ITS developers and planners with a complicated national legal landscape in which to navigate. State courts use privacy regulations enunciated by the federal government as a floor and have built upon them, expanding the realm of privacy beyond the home in numerous states. State legislatures have also begun to respond to ITS technologies being implemented in their jurisdictions through creating ownership statutes over the information being collected, as well as expanding previous state data protection acts to ITS information collected in their state. Inconsistencies in state privacy laws may result in developers having to take a state by state approach in considering the design of information sharing and collection systems to satisfy numerous levels of regulation in different states. The burdens and inefficiencies of such an approach is not attractive, yet the alternative of only developing technologies and systems that meet the standards of all 50 states is equally unattractive as it would be at the expense of innovative and beneficial technology designs that would be allowed in some jurisdictions. Tort law has also become an arena where ITS collected information can run into legal obstacles as mismanagement or misuse of personal information that results in harm to citizens can have civil legal consequences.

There are number of other legal principles and doctrines which are likely to impact how the law affects the use of ITS technologies. The third party doctrine dictates that information willingly shared with a third party carries no privacy protections and the government has free access to it. Under this doctrine, information collected by private ITS companies could be made known to the government investigators or other government departments without any warrant. Information

gathered by private ITS companies would be vulnerable to court and law enforcement demands for information on ITS customers in civil and criminal cases, putting a chilling effect on drivers' desire to utilize and benefit from ITS systems.

Legal issues also arise for ITS technologies when they are used in law enforcement efforts. Automatic enforcement technologies fine owners of vehicles for traffic violations committed in their vehicle through vicarious liability. Whether the owner is being charged with a civil penalty or criminal penalty affects the constitutionality of these technologies, as some courts have found criminal charges based on identification of the offending vehicle's owner, as opposed to the actual driver, violates due process protections.

As ITS developers and planners look to create technologies and systems that benefit roadways without tripping legal restrictions, specific consideration needs to be given to a number of choices. The first choice deals with the type of information to be collected. Collecting anonymous information about drivers is less likely to trigger legal restrictions than the collection of personally identifiable information. How ITS administrators collect consent is also a choice that must be considered. When roadway users voluntarily consent to having information collected about them, legal restrictions and privacy expectations are limited. However, when ITS administrators need information from all roadways users, implied consent is granted through the law, leaving legal restrictions and privacy expectations largely intact. Finally, ITS developers and planners need to choose whether private or public entities will be responsible for maintaining ITS systems. Private companies currently face less regulation over the management of their databases when compared to government collected data. However, potential for abuse of information by private companies may result in consumers looking to government intervention in how ITS information is managed and stored, creating burdensome oversight for ITS systems.

The fragmented nature of privacy protections in the United States is likely to create obstacles for the implementation of ITS technology networks that cross jurisdictional lines. The numerous functions of ITS technologies trigger their own unique set of privacy concerns and legal restrictions on a state, federal and local level. Consequently, developers and planners looking to utilize ITS technologies are forced to navigate a myriad of legal considerations and consequences that correspond with the ways in which they utilize the technologies and the information they collect. In an attempt to assist in that endeavor, the final part of this paper looks to establish tools for ITS developers and planners that explain the level of restrictions that correspond with different kinds of information being collected.

Chapter 1
Introduction

Imagine in the not so distant future, an individual is running late to a family gathering in a vehicle equipped with Intelligent Transportation Systems (ITS) technologies. While Global Positioning System (GPS) technologies assist the driver in navigating his way on unfamiliar roads, instantly updated ITS traffic monitoring technologies inform the driver of potential traffic delays ahead and suggest alternative routes. The driver safely arrives at his destination with time to spare thanks to the assistance of these ITS technologies. However, as the driver shuts off his vehicle, he is informed by an on-screen display that he is being fined for $315.00 worth of traffic infractions which were recorded and reported to local law enforcement agencies by his vehicles ITS technologies. The infractions include speeding, improper lane change and failure to come to a complete stop at a crosswalk, all offenses registered by the very technologies that assisted him in his travels.

Though the realization of this hypothetical probably will never come to complete fruition, current ITS developments and initiatives are advancing technologies which make such monitoring and enforcement a real possibility. For example, the U.S. Department of Transportation's Vehicle Infrastructure Integration (VII) initiative is currently working with federal, state and local governments, as well as the automobile industry, in developing an information infrastructure on American roadways through a web of in-vehicle information sharing technologies which communicate with other vehicles and roadside monitoring equipment. The U.S. Department of Transportation is working to connect the data flows from these technologies with the information being gathered by electronic toll collectors and emergency vehicle notification systems under the National ITS Architecture project. The national integration of administrative systems for automatic enforcement technologies used in monitoring commercial trucking has resulted in lowered costs for both enforcement and compliance, while also creating more efficient travel in the commercial trucking industry. It is not difficult to imagine that the potential for safer, cheaper and more efficient law enforcement through integration of information systems would be attractive to law enforcement agencies who could push for the incorporation of speed cameras, red-light cameras and congestion pricing cordon zone enforcement mechanisms into the national ITS architecture. Many of these technologies collect identifiable vehicle information which can be utilized in monitoring an individual's driving behavior and enforcing traffic regulations. It is important to note that all of these emerging vehicle technologies track and gather vehicle data. They do not identify the driver. For many purposes the driver is assumed to be the registered owner of the vehicle. Yet technology exists and continues to emerge that can and will identify the driver. Those emerging technologies raise very significant privacy issues.

The types of vehicle information collected by these systems include trip routes, frequency of use and compliance with traffic laws. As new technologies continue to improve traffic flow and safety, they also require increasingly enhanced abilities to capture and utilize data. Yet, this capability to gather, store, and transmit data about a transportation network user carries implications for the privacy of vehicle owners, drivers, and potentially passengers. Questions of how the technologies interact with public perceptions and expectations of privacy, as well as the

current legal framework established to protect privacy, are important to determining the ways in which ITS will be allowed to operate in the future. By taking into account the legal principles governing information practices in the United State, ITS developers and planners will be in the best position to predict and mitigate potential limitations to ITS technologies resulting from the emergence of legal privacy regimes responding to the modern transportation networks' alterations to the physical reality of privacy on the road. A thorough accounting of privacy law in the U.S. will also inform ITS planners and developers in their efforts to alleviate citizens' privacy concerns through technology design and the adoption of privacy protection principles.

This paper describes the legal systems that define "privacy" in the United States and considers how these regulations and legal definitions are likely to impact the development and utilization of ITS technologies. An understanding of how federal and state privacy legal regimes have effected the management of other information systems and data practices will help ITS developers and planner navigate the current legal landscape, as well as serve as a basis for new legal and technology solutions that could accommodate emerging innovations in ITS. After an overview of the implications of both state and federal privacy law on ITS technologies, a toolbox is presented which explains the different choices ITS planners and developers face in creating and utilizing ITS technologies, as well as the corresponding legal consequences of those choices.

Chapter 2
Background on Privacy

While slow to adopt federal privacy protections, the United States federal government has readily adopted technological advancements towards an improved infrastructure in record keeping, trade flow, security measures, criminal investigations, and transportation. These advances in essences create what privacy experts call a "digital dossier" which is "an ever-growing series of records…about almost every facet of a person's life" (6). These digital dossiers affects the daily lives of many individuals through influencing what financial institutes do business with them, what employers might hire them, and how law enforcement investigates potential crimes relating to them. Information gathered by ITS technologies is likely to contribute to these digital dossiers through reflecting an individual's travel patterns which can show where that individual works, sleeps, worships and recreates with others.

The legal concept of privacy in the United States is an evolving one. Solove, in noting the importance of articulating "what privacy means" before discussing the issues raised by a particular action or policy, advocates that the term needs to be used as "shorthand umbrella term for a related web of things" (1). While Solove has developed a useful taxonomy (2), we find it a bit more useful to start from a policy-based perspective, where analysis has defined this "web" as protecting five aspects of life. These five aspects are spatial, which distinguishes geographically between private and non-private places; behavioral, which grants privacy to certain actions; decisional, which protects personal decisions from monitoring or influence; bodily, which gives privacy to a person's body; and informational, which consists of protection both from data collection and of collected data (3). ITS programs create a set of surveillance and data-compilation concerns that primarily implicate the behavioral and informational aspects of privacy (3).

Privacy must also be addressed with an eye to why privacy matters, lest a privacy right get violated due to a failure to recognize that an action even implicates privacy concerns (1). Privacy can be treated as an individual's human right, as a political value placing a check on powerful entities, and as prerequisite for trust between actors (3). Moreover, violations of privacy can cause a variety of harms: "dignitary harms" like "reputational injury… [,]incivility, lack of respect, or causing emotional angst"; "enhancement of the risk that a harm will occur" such as increasing a person's "risk of that person being victimized by identity theft or fraud"; and altering the balance of power in society with a "chilling effect" on private behavior (2).

Chapter 3
Established U.S. Privacy Laws

The legal landscape for privacy in the United States is not easily navigated. As the US does not have comprehensive privacy legislation, unlike many other countries (3), regulation of privacy issues has several legal bases. These legal bases of U.S. privacy law are rooted in state and federal constitutional, statutory and tort law. The following is an examination of these privacy laws and how they relate to one another, as well as their potential to impact the use of ITS technologies. The current lack of federal statutes regulating the rapidly developing innovations in communication technology, surveillance methods and data collection process has left American citizens vulnerable to the utilization of growing amounts of collected personal information by both government and private actors in ways which are likely to infringe upon expectations of personal privacy, specifically when the utilization of personal information results in the curbing of societal privileges.

Relationship between Federal and State Privacy Protections

The right to privacy is not expressly protected in the United States Constitution; however American jurists have used a number of Constitutional Amendments and federal laws to create a network of legal protections for citizens from state and private intrusions upon personal privacy. U.S. Federal Courts have set a floor of limited protections for privacy rights that are found to be "fundamental" or "implicit in the concept of ordered liberty" (4). These fundamental privacy rights can be further broken into protecting two different types of interests, "the individual interest in avoiding disclosure of private matters, and another is the interest in independence in making certain kinds of important decisions"(5). The former interest is in informational privacy, whereas the latter interest is in decisional privacy. Both interests work to address overarching concerns of personal autonomy and avoidance of unnecessary intrusion in to citizens' personal lives by the government.

The United States Congress has supplemented informational privacy protections through placing regulations (limitations concerning access and use) over government and private data pertaining to areas of a citizen's life that might not be considered fundamental by the courts, such as employment, finances, health care, education and general consumption information. The pace at which federal law is extending these additional protections is slow, reactionary and narrowly tailored to specific misuses of information which have warranted Congressional attention. Another reason for the lack of an overarching federal privacy legal regulation is the federal government's traditional deference to individual states in the matter of determining their own privacy regimes.

Where the federal law has failed to be proactive in providing privacy protections and limitations on how personal information is used, states have begun to establish increased levels of protection through local legislation and the expansion of privacy rights through court rulings and state constitutions. This is in line with the US Supreme Court's finding that "the protection of a person's general right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States" (7).

Though wary to embrace large privacy protection schemes which would regulate personal information and data collected in a variety of ways, the federal government continues to embrace and implement new ITS technologies. Initiatives such as the previously mentioned VII are working to establish a nation wide network of integrated ITS programs towards the coordination of a unified federal intelligent transportation system. Though some of these systems seek to only utilize anonymous vehicle information, the VII program also looks to integrate personally identifiable information from information service providers into the transportation information flow. By design these systems will increase the amount of stored driver and trip information which will require accompanying privacy protections and regulation. State legislators and courts are now beginning to respond with limitations and protections for their own citizens' information in addition to the federal regulations and court rulings on privacy, creating another layer of complicated privacy protections in numerous state jurisdictions for ITS developers and planners to consider. Before these state laws are considered, an analysis of current federal state law is needed.

Chapter 4
Federal Privacy Laws

Federal Constitutional Protections of Privacy

The fundamental source of legal protection and redress for privacy violations by state actors is constitutional interpretation. Here, there are two routes by which the U.S. Constitution provides protection for privacy. One is interpretation of the Fourth Amendment, 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" (4) to include protection for situations in which "a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'" (7). Though apparently protective of behavioral privacy, case history from the Supreme Court of the United States incorporates an element of spatial privacy to it, continuing to use locational factors in determining whether an expectation of privacy has been demonstrated and whether or not that expectation is reasonable (8, 9). Because the Fourth Amendment addresses searches, seizures, and the issue of warrants, its case law and interpretation comes predominantly out of criminal cases. Key cases have addressed the constitutionality of police use of vehicle tracking technologies, advanced camera technologies, and third-party access to confidential information. The legal doctrines espoused in those cases will be translated to ITS later in this paper.

The second constitutional pathway to privacy protection is that a right to privacy is an obvious and essential component of the rights and liberty protected by the 9th and 14th amendments to the U.S. Constitution. However, this source of protection for privacy has been limited to "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education" (10). Privacy protections stemming from these amendments may be applicable to the privacy concerns raised by ITS as the U.S. Supreme Court has acknowledged "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files" and that "the right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures" which is based in these constitutional provisions (5).

The aforementioned routes by which constitutional amendments serve as a source of legal protection for privacy both stem from interpretation of the United States Constitution. While the U.S. Constitution's provisions are applicable to state and local governments due to incorporation via Section 1 of the 14th Amendment, they provide only a minimal protection to privacy outside of criminal investigation.

Building (Home) vs. Vehicle (Car)

The spatial aspect of privacy has always been that aspect of privacy most strongly protected in U.S. law. Prior to 1967, the Fourth Amendment had been assumed to apply only to government violations of privacy in a constitutionally protected zone, particularly a person's house. However, in Katz v. United States, the Supreme Court "recognized that the Fourth Amendment

protects people – and not simply 'areas' – against unreasonable searches and seizures" (7). Thus, in the pre-Katz regime, protection from governmental intrusion of one's privacy was unlikely to be granted outside a protected area.

However, even with a new privacy paradigm under Katz, spatial considerations are still taken into account when determining the "reasonableness" of a privacy expectation. For an example, the courts have found that there is a greater privacy expectation inside a home than inside a vehicle. The court found that a "reasonable expectation of privacy" did not exist for anything put into "plain view" and hence, no constitutional protection is offered as "no intention to keep [it private] has been exhibited" (7). In 1983, the Supreme Court explicitly ruled in United States v. Knotts that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" (11).

Likewise, vehicles are unlikely locations to benefit from the protections afforded to privacy in the form of privacy torts. While the tort of intrusion allows a private cause of action for physically violating a person's spatial privacy or, in a sufficiently egregious matter, their behavioral or informational privacy, "on the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of his privacy to do no more than follow him about" (12).

Evolving Surveillance Technologies

Advances in technology require an examination of how they might impact privacy as "new technologies enable, as the old (because of expense) do not, wholesale surveillance" and can result in the government or commercial agencies obtaining information that would otherwise be unavailable without physical intrusion (13). Likewise, "anything visible in a public place may be recorded and given circulation by means of a photograph… since this amounts to nothing more than giving publicity to what is already public and what any one present would be free to see" (12).

The current check on using new technologies is the "generally public use" limitation which states that while there is no legally recognized privacy violation created by "augmenting the sensory faculties bestowed upon [people] at birth with such enhancement as science and technology [affords]," as defined in Knotts, (11) when the "technology in question is not in general public use," a warrant is required (14).

It is not clear how this limitation would apply to ITS, however. The Supreme Court defined this limitation in Kyllo v. United States, where police used heat sensing technology to determine whether the suspect may be growing marijuana inside a home, and, as noted above, there is a spatial distinction in US law between one's home and elsewhere, including one's car, when it comes to privacy expectations. A recent case in the 7th Circuit Court of Appeals indicates that this distinction could be a significant one, as it allowed police to us a GPS device to track the movements of a suspect's car without obtaining a warrant (15). Instead of deciding that the GPS device provided information not generally available, the court reasoned that it was similar to police use of cameras on lampposts, or even simple use of a police car to follow the suspect down the road (15).

The implications for ITS under privacy requirements of the U.S. Constitution are currently small as the U.S. Supreme Court has not found information about an individual's activities in public to be protected. However, it is not unrealistic to expect the Court may determine that a public expectation of a certain level of privacy in their vehicles is reasonable, which creates a potential for the court to extend the protect privacy sphere around the home to individuals in their vehicles. The advancement in the ability of ITS technologies to collect detailed information from drivers and their vehicles may also eventually trigger constitutional limitations as the court has been more proactive in restricting state actions when their enhanced information gathering capabilities are made possible through technologies without which the information could only be gathered through a physical intrusion (15).

Federal Statutory Protections of Privacy

Although there is not a single comprehensive privacy statute or constitutional provision in the United States, statutes have been passed to address specific privacy concerns. In many cases, these have stemmed from public outcry over a revealed gap in privacy laws; accordingly, they address only those specific instances of privacy concerns. For example, Congress passed the Video Voyeurism Prevention Act of 2004 (Public Law108-495), which criminalized taking or distributing some types of photograph without their subject's consent, in order to address the specific privacy issue of surreptitious sexual photography done mostly with cell-phone cameras (9). Likewise, the Driver's Privacy Protection Act of 1994 was passed in response to stalkers' use of driver's license records (1). Worth noting is that when the Supreme Court upheld this law, which protects informational privacy connected to a fundamental aspect of American transportation, as an exercise of Congress's authority to regulate commerce, it did not revisit lower courts' rejection of the alternate claim that the law was an exercise of Congress's 14th Amendment authority to legislatively protect individual rights from state encroachment (16).

The Privacy Act of 1974 may be the most overarching legislation passed by the federal government in relation to how government agencies are required to handle information about citizens. That act mandates that administrative and physical security systems be put in place in order to avoid the unauthorized release of information to third parties (17). Inter agency exchange of information is only allowed under a number of exceptions and upon request individual citizens must be granted a right to access any information being kept by an agency. Under this act, citizens have the right to demand access to records collected by any ITS programs that collect personally identifiable information about them. This could become burdensome to ITS data managers in cases where such records are not easily accessible due to technology design and record maintenance practices. It should also be noted that there has been recent exceptions to this law in the United States in the last ten years. In an effort to strengthening security after the September 11th, 2001 attacks, the Bush Administration exempted the Department of Homeland Security from having to disclose information gathered concerning domestic and international travelers arriving or departing in the United States via aircraft. Depending on future political concerns regarding security, future laws could extend these exceptions to records regarding citizen movements on the road as well in the name of security vigilance.

Chapter 5
State Privacy Laws

As previously mentioned, federal law sets the floor of privacy protection upon which states have the ability to build their own privacy regulations. The potential for individual states to apply varying standards on information practices to ITS posses a great challenge for developers looking to provide ITS products that can be applied in a uniform way throughout the country. To help ITS developers and planners better understand the variety of state legal contexts that their technologies are likely to face, an examination of existing state privacy laws is necessary. As a picture of the various approaches to state restrictions and regulation of privacy emerge, developers and planners will be faced with choosing the best strategic legal approach to bringing about a coherent privacy policy in the handling of ITS information gathering and utilization so that the full benefit of the technologies can be realized with as little interference from the state as possible.

State Constitutional Protection of Privacy

Constitutions in ten different states (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington) explicitly recognize a citizen's right to privacy. Other states have derived a right to privacy from the text of their constitutions. The Supremacy Clause of the U.S. Constitution sets a floor, not a ceiling, on the state court's interpretation of citizen privacy rights. Hence, each state court has the capacity to develop their own legal framework for privacy rights based on their state constitutions, even in cases where the language in the state constitution is identical to language in the federal constitution. As the U.S. Supreme Court has been reluctant to expand privacy rights based on the 4th and 14th Amendments over the last couple of decades, states have begun to develop their own enhanced informational privacy rights.

Instances where state courts have expanded the privacy rights of their citizens beyond the protections offered by the federal courts are often in response to the development of new law enforcement procedures or the implementation of new technologies that threaten the state's traditionally recognized sphere of privacy. In State v. Hunt, the New Jersey Supreme Court determined that telephone company's records of long distance phone calls were private information protected by the state constitution, a position opposite to the one taken by the Supreme Court in Smith v. Maryland where they found similar phone company records were not protected by the federal constitution (19, 20). The New Jersey Supreme Court reasoned that "[t]echnological developments have enlarged our conception of what constitutes the home. The telephone has become an essential instrument in carrying on our personal affairs. It has become part and parcel of the home" (19). The New Jersey Supreme Court's willingness to expand what constitutes the home, and hence extend privacy protections beyond what the federal courts identify as the sphere of privacy around the home, carries implications for ITS. It could be argued that technological developments have caused vehicles to become essential instruments in carrying on an individual's personal affairs; hence they too are a natural extension of the home under the New Jersey Constitution. It would then follow that the state government would not be allowed to access privately held ITS records of vehicle information without a warrant or consent

of the driver or owner. The courts could also recognize that an individual's reasonable expectations of being free from intrusive technologies that invade the sphere of the home to collect information could be extended to one's vehicle as well.

Another example of state courts expanding federal protections has occurred in regards to garbage put out on a public street. Where the U.S. Supreme Court decided in California v. Greenwood that the government did not need a warrant to search garbage left on the street curb, some state supreme courts have ruled that such searches violate their state constitution as garbage on the curb is protected as items in the home would be (21). If state supreme courts are willing to extend the privacy protections afforded to the home to the garbage on the street, the potential for the same protections to be expanded to citizens' vehicles on the streets seems possible as well.

The ability of state courts to interpret their state constitutions in a way that expands privacy rights of their citizens beyond those prescribed by federal constitution is likely to result in a variety of different levels of privacy protections a citizen is granted in their vehicle. This would in turn create a variety of limits on how ITS data can be collected, shared and utilized by transportation planners and engineers, depending on what state jurisdiction they are implemented in. Such inconsistencies in state constitutional privacy demands may result in developers having to take a state by state approach in considering the design of information sharing and collection systems in order to satisfy numerous levels of regulation in different states. Such an approach would also require multiple versions of technologies, which would increase ITS development costs and limit the ability of developers to build upon innovations allowed in only some jurisdictions. The burdens and inefficiencies of such an approach is not attractive, yet the alternative of only developing technologies and systems that meet the standards of all fifty states is equally unattractive as it would be at the expense of innovative and beneficial technology designs that would be allowed only in some jurisdictions.

State Statutory Protections of Privacy

State legislatures have extended protections over state and privately collected information about citizens in both general and specific ways. General statutes protecting government collected information exist in states like Colorado, Connecticut, Florida, Hawaii, Minnesota, New York and Ohio, where statutes require openness on what kind of information is being collected; avenues of access for citizens to see what information is being collect about them and to make appropriate corrects; limitations on secondary usage of individual information; as well as security requirements for how that information is maintained (22). State regulations on privately collected information are not as overarching, but instead focus on specific kinds of data collection and information. These state laws usually address bank, cable television, employment, insurance, medical and academic records. Further regulations on specific kinds of government records are common in cases of library, driving and criminal records. In the majority of cases, state laws on privacy take a case by case approach in how they regulate the use of personally identifiable information, similar to the piecemeal approach of the federal government.

There are not many state laws specifically addressing privacy rights and transportation technologies. Most laws that have been passed address only specific technologies whose use is either widely unpopular as the public believes there is a potential for abuse of such technologies.

An example of this would be photo radars which use have been banned or limited in at least five different states (California, New Jersey, Oregon, Utah and Wisconsin).

Another example of states responding to developing transpiration technologies is California's "black box" laws which regulate the use and access to information gathered by a vehicle's event data record (23). Insurance companies and manufactures often desire the information in these boxes in order to determine liability in instances of crashes or other instances. The California law dictates the vehicle's owner has complete control of the information which can be kept private from others, unless a court order demands the data be shared. As new ITS technologies begin to become pervasive, tweaking by state legislatures in the absence of federal legislation should be expected by ITS developers and planners.

State Tort Protections of Privacy

State privacy torts have been a fundamental source of privacy protection in the United States. In only a few states have the courts definitively denied the existence of any common-law right of privacy. In the majority of states, privacy torts have been used to provide protections of privacy for citizens while also working to ensure beneficial uses of information can continue. Though there have been no privacy tort cases dealing with ITS technologies as of yet, the pros and cons of relying on privacy torts as opposed to privacy regulations should be considered by developers. Instead of trying to regulate information systems through what can be overbearing and over generalized rules, privacy tort cases gives courts the power to balance the benefits and costs of specific claims, ensuring that the free flow of information for the benefit of society is possible, while bad actors are deterred and punished.

Tort law generally envisions four manners in which a person might accrue liability for violating another person's privacy: intrusion upon solitude, public disclosure of private facts, "false light" publicity, and misappropriation of likeness (12). These largely constitute protection for spatial and informational privacy, with some "virtual" bodily protection in relation to misappropriation of likeness. However, as noted earlier, these do not usually create a cause of action on the public streets. Further, most of these torts rely upon intrusion where the victim had not consented to giving up their privacy. While government has an interest in possibly observing private acts (albeit with a warrant) to protect the public safety, such an action tends to not be in the interest of private industry – or, at least the ITS industry. For example, the VII initiative explicitly stated that it would not use the information collected to support law enforcement (29). Rather, the privacy questions arise in terms of how the private entities gain the consent of those using their technologies; the limits the former are willing to place on the use of the information they collect; and their willingness to conform to those limits.

A potential pit fall of only relying on the common law for establishing privacy standards by which ITS information gathering and utilization is regulated stems from the unpredictability of rulings that might come down under different state courts due to judicial discretion or technical differences in states' legal definitions of the elements of privacy torts. Another potential challenge to relying only on privacy torts is the high barrier of expensive litigation which it would create for consumers in challenging abuses of information. Though the private sector enjoys this buffer which arguably protects them from frivolous claims of abuse, consumer and privacy advocacy groups are likely to demand clear statutory protections which can inform

consumers of their rights and remedies without having to wade into the murky legal world of tort litigation.

Chapter 6
Potential Legal Issues for ITS Information

Personal Information in the Context of the Third Party Doctrine

There is a potential that courts may find that certain types of personal information collect by ITS technologies are not afforded any privacy protections under the third party doctrine. Banks and financial institutions represent private organizations that the federal and state governments have been the most willing to regulate in regards to how personal information is handled. In the 1970's, the Supreme Court handed down a number of rulings in regards to constitutional protections of citizen's personal bank accounts that left much of this information in the public realm. In United States v. Miller, the Supreme Court established that personal information held by banks are business records and not of a "private" nature, hence citizens did not have a reasonable expectation of keeping them private (24). The court further explained in Smith v. Maryland that when a citizen exposes their personal information to a third party, they assume the risk that such information will be made available to the government (25). These cases established a privacy precedence known as the "third party doctrine" that dictates information in the hands of third party warrants no 4th Amendment protections.

Under this doctrine, information collected by private ITS companies could be made known to the government investigators or other government departments without any warrant. Furthermore, these rulings imply that private ITS companies would have no obligation of keeping personal files about a drivers activities confidential since the driver has made his driving decisions in a public forum (the road) and has submitted that information to the private company willingly (granted that the information can only be gathered from willing participants).

However, California courts have found the third party doctrine to be lacking in certain instances, specifically in regards to information gathered from activities which are necessary for participation in the "economic life of contemporary society" (26). The court in Burrows v. Superior Court of San Bernardino County, found bank records to be within a citizen's reasonable expectation of information that should remain private. The court's main concern was that the "totality of bank records provides a virtual current biography" as the information in the records reflects the "personal affairs, opinions, habits and associations" of an individual (26). Driving also might be considered an activity essential to an individual's ability to engage in the economic life of contemporary society. The ability of ITS databases to compile similar digital dossiers on individuals and their behaviors while driving may raise the same concerns from state courts, triggering state level constitutional information privacy protections which would become an obstacle to sharing data between private ITS information gatherers and other parties, including government agencies seeking to use that information for beneficial state purposes.

As mentioned before, the federal government, states and local jurisdictions are turning to private companies to set up and run ITS technologies on their behalf. Red light camera systems are one example of an ITS technology that is being installed and operated on behalf of numerous local jurisdictions by over one hundred different private ITS companies (27). This is mostly being done out of an effort to lift the burden of managing large and complicated technological systems

from government agencies that lack the capacity to do so on their own. However, federal and state agencies have also increasingly relied on outsourcing the gathering and managing of information to private companies because they do not face the same civil-liabilities and limitations placed over government agencies. Though shifting information collection to private companies might provide ITS developers and users more flexible statutory rules under which information can be utilized, these private companies still remain vulnerable to state courts which have the power to reign in the information sharing practices of private companies. This shifting to the private sector in the collection and management of information has also resulted in proposed overarching federal legislation called the Personal Data Privacy and Security Act which would allow for strong federal oversight of "data brokers" (broadly defined in a way that would include many ITS companies) and also calls for strong penalties on these companies when they "fail to protect consumers" (28). If ITS technologies are run by private companies on behalf of government agencies, they are likely to invite burdensome oversight and regulation in response.

Use of Privately Collected Data in Criminal Cases

ITS service providers have challenged court orders demanding the use of their technologies in assisting a criminal investigation. In The Company v. The United States, a dashboard computer system was used by the FBI in order to eavesdrop on conversations in a vehicle believed to be used by drug dealers (30). The company challenged the court order that required them to allow the FBI to remotely activate the in-car cell phone without the owner's knowledge. The Ninth Circuit Court ruled that the FBI could not use the private system for eavesdropping because of the potential interruption of the companies' services during an emergency as a result of the FBI's monitoring, which would equate to the company failing to meet a contractual obligation. However, the court went on to say that in the event that the service provider developed a way that would permit for monitoring of in vehicle conversations without interruption of the emergency services, law enforcement would be able to listen in on these conversations with a warrant (30). In the face of this kind of government power to utilize ITS systems for surveillance, service providers have an interest assuring customers that they will not participate in invading their privacy, however at the same time are forced to hedge their bets with privacy statements that only promise to "disclose personal information if required to do so by law on (sic) in the good faith belief that such disclosure is reasonably necessary to comply with the legal process" (31).

As threats of domestic and international terrorism continue, private ITS service providers are also likely to find themselves in the situation faced by the telecommunication companies who have been asked to comply with warrantless wiretaps and executive orders by the president in the name of national security. The information about the travels of a potential terrorist through the use of private security cameras or a vehicle's GPS unit may provoke law enforcement agencies to request this information from private companies without going through the courts. ITS services providers face the difficult issue of complying with these requests in order to assist the government in protecting America, while at the same time facing potential civil liabilities for providing access to private information in violation of contractual agreements or law without a court order.

Use of Privately Collected Data in Civil Actions

Undoubtedly, private parties will also have a keen interest in using information gathered by ITS systems in civil actions. For example, private insurance companies have already attempted to assert a right to information from a vehicle's Event Data Recorders (EDR), also known as auto black boxes, in order to ascertain the causes of an accident. Privacy advocates have balked at the assertion that individuals should be required to turn over vehicle data in the event of an accident to private actors, as such information is the personal property of the driver and could be self-incriminating in court. Federal law has looked to make such information more technically accessible to private companies use in civil litigation, however some states have responded with laws which make the information from ERD's private (32). Courts, however, have manifested willingness to accept data collected by these systems in civil cases as long as it complies with the applicable evidentiary standard of "general acceptance" as a legitimate technology (33). There is a great potential for other ITS technology to provide information that would be useful in civil litigation, be it a wife looking to divorce her unfaithful husband wanting to subpoena records of his GPS or be it the private video of a negligent driver in an auto injury case. A higher standard of protection is placed over personal information in a civil case, however technology and records not privately held by a party have not traditionally enjoyed the privacy protections from subpoenas in a civil suit that has been granted to personal records (34).

At the current time, these questions are largely left to be decided in the marketplace. Solove points out that there are few, if any, court cases requiring a private entity to enforce its privacy policies (1). However, he also points out that industry does have a relatively significant interest in protecting the trust of their customers, and thus it appears that ITS may be able to avoid significant regulation if they continue to recognize the long term value of keeping promises exceeds any short term value that comes from violating that trust.

Government has mostly acted to regulate use of private data by other private actors in cases where harm has resulted as a result of data sharing. While these provisions may be passed to protect any aspect of privacy, they typically each provide only a limited, specific sort of protection, addressing a particularly defined act that would violate someone's privacy. One example of this was the passage of the previously mentioned U.S. Drivers Privacy Protection Act, which defined permissible and illegal distribution of motor vehicle records, which include "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." (35). While this is an exceptional case in that Congress passed the law in response to the murder of Rebecca Schaeffer, which occurred when a stalker was able to obtain her address from a Department of Motor Vehicles record, it does show that government will intervene if the existing system fails.

As ITS information becomes of interest in criminal and civil cases, ITS developers and planners will have to consider the ability of their technologies to turn over information as part of a trials discovery process. E-discovery is the newest frontier in evidentiary rules, with the most recent amendments to the Federal Rules of Evidence stating that electronically stored information is discoverable and can be compelled by the court (36). However, the rules state that if discovery is too burdensome or costly to a party, the electronically stored information may not be discoverable. ITS planners and developers will have the choice over whether their technologies are programmed in a way which makes the potentially useful ITS information readily available

for the courts. If the ITS technologies are not deliberately set up to easily service discovery requests or purposely avoid collecting relevant information, ITS managers are likely to become bogged down with an overload of requests from lawyers looking to access information relevant to their case.

Automatic Enforcement and Vicarious Liability

One of the most complicated legal arenas ITS technologies face is in the area of law enforcement. Automatic enforcement technologies are quickly becoming a favorite tool of local policy makers and law enforcements agencies. Currently, most automatic enforcement technologies employ the use of cameras which identify offending vehicles, and they have been implemented in 25 U.S. states. Automatic enforcement technologies are appreciated for being an efficient tool which frees up law enforcement officers to take care of more important policing work. They are also appreciated for their ability to effectively enforce traffic and speeding regulations in areas which they are implemented. Automatic enforcement technologies are also beginning to be used to enforce bus lanes, toll booths and double white lines.

Legal issues arise around the question of who is liable for traffic infractions captured by these technologies. When an officer pulls over a vehicle, it is the driver, observed and identified by the officer, who is held liable for the offense. However, automatic enforcement technologies have yet to develop reliable methods for identifying the driver of an offending vehicle; hence liability is shifted to the owner of the vehicle under what is called vicarious liability.

Vicarious liability already exists in some shape or form in most jurisdictions, usually in law defining the enforcement of parking tickets where ownership of the car is prima facie evidence that the owner was the operator of the vehicle at the time of the infraction. A more serious and more relevant type of vicarious qusai-criminal liability exists in the offense of passing a school bus with its stop signal extended. Seldom if ever does the school bus driver observe the face of the driver. These laws allow the registered owner of the vehicle to be found guilty of a petty misdemeanor (a quasi-criminal offense) without any proof that they were actually operating the vehicle at the time of the offense Some state jurisdictions are now expanding their statutory definitions of vicarious criminal liability to include liability of owners for offenses committed by their vehicle which are captured by automatic enforcement technologies including the running of red lights and speeding. Challenges to these laws in most jurisdictions have usually claimed a violation of due process through the automatic assignment of guilt in a judicial system which assumes innocence unless guilt can be proven (37). However, as civil penalties are usually the only remedy sought by jurisdictions employing automatic enforcement technologies, courts have not found the violation of due process they might find if owners of vehicle were being found vicariously liable for criminal charges.

Though courts have not found the civil penalties placed on the owners of offending vehicles to be burdensome enough as to warrant an overturning of vicarious liability, the potential for the expanding use of ITS in enforcing traffic laws and norms could potentially lead to unforeseen burdens on drivers which could result in reconsideration of the issue. While accepting and upholding the constitutionality of quasi-criminal vicarious liability for violation of some traffic regulations, the courts have expressed significant concern about the expansion of this concept to full criminal liability that could result in imprisonment (38).

The potential for in-vehicles technologies to be utilized by law enforcement agencies in enforcing the law is also a real possibility. Already law enforcement agencies have required individuals convicted of drunk driving to install ignition interlock systems which measure the amount of alcohol in a drivers system before the vehicle is able to be started. The potential for monitoring the vehicles of drivers with reckless driving conviction histories could easily be the beginning of a much larger effort to use in-vehicle ITS technologies to encourage better driving through law enforcement monitoring. As this technology matures, its use may be expanded through the concept of implied or explicit consent. This concept ties the reinstatement of a person's driving privileges, lost or restricted because of prior traffic violations, to an agreement that permits the government to install technology in the offender's vehicle that will be used to monitor, record and possibly transmit to the government the offender's future driving conduct.

The private market is already producing incentives for in-vehicle monitoring systems which report illegal behavior. Currently in Arizona, Illinois, New Jersey, Pennsylvania, South Carolina and Washington pilot programs have been put in place by insurance companies which reduces rates for policy holders who are willing to place GPS units in the teenagers vehicles that reports to the company and the parents when the teen has violated any speed limits (39). Though parents' vigilance over their teens' use of their vehicles is an idea that most in society are likely to welcome as an important step in promoting safety, There are serious proposals to expand the availability and access to this data to states driver's license authorities who will then use the data to monitor compliance with graduated driver's laws which almost all states have. The same kind of paternalistic protection by the state over all drivers who wish to operate their vehicles on the states' roads may not be as eagerly welcomed.

The expanding ability to identify, track, monitor and determine the illegal operation of vehicles on roads and highways through technology without direct observation of the violation by a law enforcement official does not completely open the gates for widespread application of these types of ITS technologies. While the 7th Circuit opined that use of cameras on lamp-posts would not raise privacy issues, the Minnesota Supreme Court recently struck down the use of such cameras for red light enforcement over the issue of vicarious quasi-criminal liability. The Court found that an owner of a vehicle could be held liable for an infraction committed by his or her car in the event that the state could identify the owner as the driver at the time of the offense, which they currently could not since the red light cameras only identified the car's license plate (40). The Court declared that the only other way an owner of a vehicle could be held liable for a traffic violation captured by an ITS system would be through a statutory extension by the legislature of vicarious quasi-criminal liability to that specific offense. Currently, vicarious quasi- criminal liability is limited in Minnesota to a few serious offenses, such as passing a school bus that has its stop arm extended and red lights flashing (41).

Chapter 7
ITS Privacy Law Toolbox

The ITS technologies discussed above cover a range of applications, from law enforcement to transportation system use management. The numerous functions of ITS technologies each trigger their own unique set of privacy concerns and legal restrictions on a state, federal and local level. Consequently, developers and planners looking to utilize ITS technologies are forced to navigate a myriad of legal considerations and consequences that correspond with the ways in which they utilize the technologies and the information they collect. In an attempt to assist in that endeavor, the next part of this paper looks to establish tools for ITS developers and planners that explain the level of restrictions that correspond with different kinds of information being collected.

The more anonymous the information, the less likely the government will adopt legal restrictions that will dictate how that information is collected and used. When the information collected identifies vehicle specific or personally identifiable information, legal issues regarding consent, access, ownership and protection of information are triggered. The following is a toolbox description of the legal issues that ITS developers and planners will face when they seek out different kinds of information through ITS technologies (See Appendix A). The toolbox is meant to help planners and developers anticipate the legal implications of their technology design and utilization choices.

Anonymous vs. Personally Identifiable Information

ITS information is likely to fall within a spectrum of anonymity as opposed to falling into a strict category of being anonymous or personally identifiable. Generally, personally identifiable information is defined as unique data that carries the potential of being used to identify a single individual. Examples of personally identifiable information include: full name; telephone number; street address; email address; email password; vehicle registration plate number; driver's license number; credit card numbers and one’s digital identity. On the contrary, anonymous information carries no indicators of its origin and cannot be tied back to a specific individual or vehicle. Examples of anonymous information would include information collected by traffic counters or devises that detect the presences of vehicles in order to control traffic flows without identifying the vehicle or its owner.

Some ITS technologies require the collection of personally identifiable information in order for their purpose to be achieved (i.e. charging tolls to drivers (arguably tollway only identifies vehicles); congestion pricing; red light cameras, etc.). In order to avoid legal barriers to the functionality of these technologies, ITS developers have made attempts to anonymize personally identifiable information by stripping data pieces of unique identifiers through use of partial plate numbers, the immediate dump of personal information after initial use, or the assignment of random account numbers to ITS users. However, these steps have not always proven to completely anonymize the ITS data, as steps can be taken to reverse the anonymization process or through correlating anonymized information with a subset of identifiable data.

The choice by ITS developers and planners to use personally identifiable information is an important one. Collecting and utilizing personal information invites legal restrictions aimed at

making sure the information is not misused or inappropriately collected. Hence, anonymous information should be preferable to ITS planners and developers as there will be less legal liabilities and requirements restricting the access to and use of the ITS technology. However, as personally identifiable information will be necessary for some ITS technologies to function correctly, planners and developers should work hard to find creative solutions to minimize the necessity of its collection and storage in order to avoid the burdensome legal restrictions. This will require new approaches to collection anonymization processes.

Consent

In the cases where ITS technologies require the collection of personally identifiable information, the issue of consent comes to the forefront. Privacy laws throughout the United States often require consent from an individual before personally identifiable information about them is collected and stored. Government agencies and companies looking to utilize personally identifiable information through ITS technologies must choose between two ways in which consent from drivers can be garnered. Voluntary consent (or Opt-In) is one way in which consent can be given. Voluntary consent requires individuals to manifest willingness to have their personal information collected. Besides being willing participants in the ITS programs, drivers' consent must be informed of some specific aspects about the information being collected in order for consent to be complete. Examples of information that needs to be conveyed to the willing participants include: what information is being collected about them; how the information will be used; the legal consequences for giving consent; the protections that will be put in place over the collected information; how false information can be corrected; and how long the information will be kept. As mentioned before, when drivers voluntarily opt-in to ITS programs, liability over ITS information practices can be waived and limited, freeing ITS managers to use the personal information towards ITS goals without fear of legal liability.

The other option is to imply consent (Opt-Out). Local and state statutes can define consent as legally implied by a driver's use of transportation ways which employ ITS technologies. Currently, driving on roadways is viewed as a legal privilege in the United States and drivers statutorily consent to state actions such as field sobriety tests merely by obtaining a license. Implied consent could also be implied for the collection of personal information on roadways as an additional requirement of using the roadway and or receiving the driving privilege. Legally, courts have found implied consent to be appropriate when the state interests' in preventing injury, property damage, and loss of life on roadways are served by the practice. However presumed or implied consent usually must allow for individuals to opt-out of such programs and requires that members of the public be made reasonably aware of what they are being assumed to consent to. ITS developers and planners relying on implied consent should be cautious as legal challenges where the public has not been reasonably informed could lead to a greater amount of legal challenges to ITS information practices. Hence, when ITS programs collect information under implied consent statutes, efforts will need to be undertaken to communicate with the driving public the nature, methods and types of information that is being collected by the ITS technology.

Whether or not policy makers resort to opt-in versus opt-out consent will also determine how privacy torts are used to limited informational practices of ITS technologies. Opt-in technologies would negate most tort claims against information collectors as consumer consent nullifies most

tort actions. However the consequence of an opt-in system for ITS technologies would result in less then universal application of the technologies on the road, resulting in a lack of information being made available to traffic engineers and planners who might hope to gain more holistic insights from ITS technologies. Opt-out programs may result in more participants in ITS programs, however consumer ability to bring tort suits would not be diminished as contractual obligations with state-mandated ITS programs would be automatic instead of a choice, leaving more room for the courts to apply torts due to the lack of contractual consideration on behalf of consumers. Legislatures will hold the ultimate say in tort liability of ITS providers. If legislatures statutorily define consent to be implied by use of public roadways which utilize ITS technologies, it would result in ITS providers being protected from tort actions. Those protections would be limited to the authorized agencies while potential third parties who look to access ITS collected information for secondary use would not be protected.

Once ITS developers and planners have determined what information they are going to collect, they must form a plan to secure consent, either through individual ITS users, or through the legislature. They also must make an effort to inform those consenting on what information is being collected and how they plan to use it, regardless of whether the consent is implied or voluntary.

Public vs. Private Actors

States' willingness to enact protections over collected information varies greatly. Who is collecting the information, and who that information might be shared with, are large determinates in how much regulation the government is willing to place over information. One consistent theme in regulatory schemes has been federal and state governments' willingness to proscribe controls over their own collection of information, while providing few restrictions over information that has been gathered by private entities. The previously mentioned Privacy Act of 1974 is currently the principle federal regulation limiting how government entities share and collect information on citizens, while only a few private industries and companies, such as medical providers and credit agencies, have warranted their own specifically tailored state and federal laws dictating the ways in which they are permitted to collect, share and utilize personal information. The different approaches to regulating publicly and privately collected information will result in different kinds of legal challenges and liabilities for ITS managers.

When ITS information is gathered by public agencies, preexisting state and federal privacy regulations proscribe the agencies ability to share that information with outside parties. However, fewer restrictions exist over interagency sharing of information, including open access to law enforcements agencies.

When private companies collect personal information, fewer preexisting restrictions exist over their information sharing practices. This can be a benefit to ITS developers and managers as it allows the companies to be flexible and innovative in their use of different data types and it allows them to freely collaborate with other sources of information. However, there is also a potential risk of information being sold to and misused by third parties. Private companies desire to obtain ITS information for the purposes of target marketing, consumer behavior monitoring or qualifying driver's insurance rates. To ensure these uses of collected information do not fall outside of the scope of the driver's consent, companies that collect ITS information should

clearly establish privacy policies and secondary use guidelines so that ITS users can have clear expectations around how their information is going to be used. Without these guidelines, the interest in keeping this ITS information private will be in direct competition with the economic benefits companies stand to gain from selling this information, leaving individual's personal information vulnerable.

ITS developers and planners should also inquire into local laws in there jurisdiction that severely limit secondary use of personal information. Some privacy advocates have proposed personal information be protected through transferring ownership of collected personal information from the company to the individual. Under this legal requirement, secondary use of personal information is limited to when the individual consents, potentially limiting the ability of ITS companies and information managers to share information with each other and future clients.

Law enforcement agencies are also interested in gaining access to information collected by private ITS companies. Law enforcement agencies generally require a warrant or subpoena to gain access to the collected information unless the private ITS company chooses to voluntarily hand over the information to inquiring parties. In contrast, when law enforcement agencies seek personal information that has been collected and stored by a government agency, they do not always require a warrant or a subpoena. Choosing private or public entities to collect ITS information will directly determine how much judicial review is required to compel the sharing of ITS information with law enforcement agencies.

Though companies are not required to share information with law enforcement agencies outside of a judicial order, law enforcement agencies at both state and federal levels are beginning to garner large amounts of personal information from private companies by purchasing it. This information is then aggregated into digital profiles of citizens which can be used for investigatory and security purposes (42). As the public becomes more aware of this kind of secondary use, individual drivers will likely resist the collection of personal information by ITS technologies, especially as the information becomes more detailed and identifiable. ITS planners must consider the impacts sharing personal information of their systems users with law enforcement will have on the willingness of individuals to participate. Where widespread use of ITS programs are required for the systems success, personally identifiable information should be protected from the reach of law enforcement as much as possible in order to encourage participation.

Whether dealing with personally identifiable ITS information collected by public agencies or private companies, ITS planners and developers should adopt best practices principles which guarantee personal information will not be sold for secondary use by law enforcement agencies or any other parties unless consent is given by individual users or there is a court order demanding the information be shared. Best practices protections for personal information, by either public or private ITS agencies, should: establish an articulated privacy policy that is strictly followed; ensure data is insulated and controlled at all times; and confirm that data retention and sharing protections are firmly in place. Even with privacy guarantees from ITS providers, it remains to be seen whether those assurances can be kept in the face of law enforcement agencies that aggressively use government court orders and subpoenas demanding access to the privately collected information. Currently, law enforcement can easily access private video, records and data in relation to criminal investigation through court warrants and

subpoenas. As the pool of privately held personal information increases, courts will be forced to determine whether they will limit the breadth of criminal searches to pre-determined information targeted because of its direct relationship to the investigation, or whether they will loose law enforcement to freely scavenge large amounts of data in a way that could turn up useful information and uncover further wrong doing, while at the same time potentially exposing innocent parties to egregious violations of their most intimate privacy expectations.

Toolbox in Application: A Taxonomy

While the toolbox explained the spectrum of information that ITS technologies can collect and use, as well as the number of corresponding legal questions developers will have to consider in the development of their ITS programs, the key questions they will have to contemplate relate to

- consent,
- secondary use,
- the involvement of private vs. public collectors and
- the use of ITS collected information by law enforcement agencies.

The next section of this paper applies the privacy toolbox to the current range of ITS technologies. The resulting taxonomy considers the method of observation, the purpose of the technologies and the resulting privacy expectations.

ITS developers must consider what transportation goal is being sought, what type of information is needed to accomplish that goal and what level of privacy expectation and legal protection of an individual's privacy does the type of information implicate. First, the ITS developer or planner should ask what kind of observation is necessary to complete their goals. Next, the purpose of the observation needs to be fully articulated. After the method and purpose of the observation are understood, a list of the unique information captured about the vehicle, as well as any occupants, needs to be created. After consideration of all these factors, the level of privacy restrictions and legal protections can be determined based on the how, why and what questions of ITS surveillance (See Appendix B).

Observing general traffic conditions is one of the original uses of ITS technologies and warrants few legal considerations. The purpose of the collecting information about traffic flow is to monitor and improve system use. An example of this kind of basic ITS technology would be a traffic counter or traffic classifier. These types of technologies do not record identifiable vehicle or occupant information; hence the anonymous nature of the collected data triggers no legal restrictions or expectations of privacy.

The next level of observation by ITS technologies occurs when vehicles are independently and anonymously observed. These types of ITS technologies are usually geared towards system management, such as a loop detector that regulates intersection use through traffic signal controls. Though these technologies are identifying the presences of an individual vehicle, they do no identify any unique information about the driver or the vehicle; hence the information remains anonymous and does not trigger any legal restrictions or privacy expectations.

Privacy expectations and legal restrictions come into play when ITS technologies begin to observe and identify specific vehicles. These observations are usually carried out for the administrative purpose of managing the transportation system's use, however they are different from other methods as they do so through regulating the operation of specific vehicles. Examples of such technologies would include automated toll systems, congestive pricing through license plate recognition, and other automated fees or services that require a vehicle to be identified in order for it to receive access to roadways. The types of information gathered by these technologies relate directly to the vehicle through assigned identification numbers in the form of the licenses plate number, transponder code or customer account. These numbers can inevitably be traced back to the specific vehicle through the vehicle registration system, which leads directly to the identity of the vehicle's owner as well. With this much personally identifiable information available, privacy expectation and legal restrictions begin to apply. The administrative purpose of the data collection will mitigate some legal restrictions as the information is being collected from observed public behaviors and being used for the public good. However, restrictions on secondary use of personal information will still apply.

ITS technologies that specifically record information about the occupants of the vehicle also carry heightened legal restrictions and privacy interests. Car pool lane infra red scanners and enforcement cameras produce semi-anonymous information about the number of occupants in a vehicle, while also capturing personally identifiable information such as an occupants' digital image which can indicate a drivers age, race and gender. These technologies also can capture vehicle information that can be traced back to the owner as mentioned previously. When this information is collected for general administrative purposes, such a managing system use, then only a small amount of privacy expectation exists. However, when this information is collected for the purpose of enforcing laws on the road, the privacy expectation and legal restrictions on how that information can be collected increases.

Finally, the highest level of legal restrictions and privacy expectations exist where ITS technologies purposefully collect personally identifiable information. Technologies that identify drivers and occupants through in-vehicle cameras, biometrics, voice command, interlocking ignition systems and other control devices, all implicate a heightened level of privacy expectation and legal restriction as their purpose is the administrative and criminal regulation of the driver. The collection of this information can be for criminal or civil purposes; however the strictest privacy restrictions are triggered when the information is collected for criminal regulatory purposes.

The basic rule is, the more personal the nature of the information that is collected, the greater the number of privacy considerations exist. The proposed purpose for collecting personal information also triggers different levels of privacy considerations, as information collection for the administrative purposes of roadway safety and efficiency will raise less of a legal expectation of privacy, compared to when ITS information is being gathered for criminal and law enforcement purposes. By choosing to work with the most anonymous data sets possible, ITS developers and planners will avoid many legal restrictions and obstacles in the utilization of their technologies. When personally identifiable information is required, ITS developers are best served by established clear privacy guidelines which dictate the extent to which they are going to manage and protect individual users' information from inappropriate use by both private and public parties.

Chapter 8
Other Privacy Trends

There is now recognition that "technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive" (13). There has also been a growing recognition that existing privacy law is predicated on antiquated and incorrect assumptions about the nature and value of privacy, the extent of possible privacy violations and the ease of committing them with generally-available technology, and the harms inflicted by privacy violations (2, 9, 43). This is coupled with awareness that for all the respect purportedly assigned to privacy as a human right or social value, it is typically sacrificed in favor of other interests (1) and must be litigated in a legal environment that is at times openly contemptuous towards allegations of a privacy violation (43). It is through this understanding that a paradigm of "privacy in public" can emerge that is applicable to ITS.

Trends in Recent Cases

Courts have consistently held that permitted intrusions on privacy are not without limit, but they have treated each case as calling upon them to define for a specific set of facts "what limits there are upon this power of technology to shrink the realm of guaranteed privacy" (14). However, the incrementalist nature of the American judicial system and its reliance on precedent in deciding cases means that courts have been reluctant to articulate a general doctrine of privacy protection beyond the "reasonable expectation of privacy" standard.

Courts have also been reluctant to make decisions on privacy outside the factual circumstances presented in their cases. Seventh Circuit Judge Richard Posner, in rejecting a claim that warrantless police installation of a GPS tracking device constituted a search, forecasted, "One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns. One can even imagine a law requiring all new cars to come equipped with the device so that the government can keep track of all vehicular movement in the United States.[…] Should government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search" (13). The concern with ITS is that some systems too closely resemble, or are even the functional equivalent of, of such a mass surveillance program that will eventually trigger a significant legal response. It is important for planners and engineers deploying ITS to craft systems that will collect and handle information not only in accordance with the existing legal framework for privacy, but that will survive legal challenges in a stricter privacy regime.

Trends in Academic Analyses

Legal academics have pushed strongly for a whole new paradigm of privacy, in part due to the belief that the construction of the existing privacy rule was inadequate to begin with and in part due to the assessment that "however sound this rule once may have been, it is flawed in a modern technological society" (24). The first rationale stems from disagreement with the propositions, fundamental to established privacy law, that venturing into public entails giving

consent “to any and all public inspection” and that there is no distinction between naked-eye observation of a person and technologically enhanced observation or recording (24). The second rationale makes much of the ubiquity of devices that allow for the rapid collection, accumulation, and distribution of data and images.

The treatment that legal academics advocate for privacy is one of allowing for a sort of “public privacy,” which would grant a degree of privacy protection – and relief for its violation – to activity in public, including on the road. This is grounded in the understanding that “most reasonable people would agree that we sacrifice some of our privacy when we walk out our front doors, but this does not mean that we necessarily forgo or want to forgo all solitude, secrecy, and anonymity” (9). The idea is that privacy be treated as “a matter of degree”, not “as an all-or-nothing concept” (43). This would increase the legally protected privacy in an automobile, though the degree of protection would still be less than that given to people while in their homes.

Also important for the future of ITS, this academic trend is to reject the legal equivalency of unaided visual observation, technology-assisted observation, and technology-enabled recording. The law reviews contain articles calling this element of the historic legal paradigm erroneous for reasons including the difference in the duration of the privacy violation, the degree of scrutiny to which a person is subjected, and the number of people who may infringe on the victim’s privacy when technology is incorporated (43). Law review articles also criticize the treatment of technological surveillance as equivalent to actual or hypothetical visual surveillance as focusing wholly on the behavioral aspect of privacy and ignoring the social harms of enhanced surveillance, such as the loss of trust it engenders and its enhancement of state power against the individual, as well as ignoring the greater dignitary harm and chilling effect of data-collection incorporating artificial aids (44). Furthermore, many hold that this equivalency treatment, even if valid when originally formulated, has become inappropriate and fails to adequately protect privacy in a world of the internet, satellite and digital photography, and the incorporation of electronic data collection and storage into all parts of life (9, 43).

Chapter 9
Conclusion

The rise of ITS technologies such as electronic toll collection systems or public feeds from traffic cameras as part of traveler information websites has prompted the call for a new treatment of privacy in the law. Former U.S. Representative and Secretary of Transportation Norman Mineta once compared the state of privacy law regarding ITS to that of copyright law at the dawn of the digital age: "Copyright law at that time preceded those technologies and understandably failed to deal with such issues as circuit design protection. No one would suggest that we should have blocked all the efficiencies and power of the PC revolution simply because chip designs were not anticipated in existing law. Instead we reviewed the situation and modified the law to apply our copyright concepts to new technology" (45). Just as the new technology of computers required extension of an existing legal framework to accommodate the new reality, so too will ITS require extension of existing legal concepts. Just as the PC revolution's realities of open-source software and copyright licensing have challenged the conceptual underpinnings of copyright law, so too do existing and near-future ITS applications necessitate reconsidering some of the foundational ideas behind privacy law. The existing jurisprudence and statutory protections appear to do little to require privacy-sensitive ITS, but recent cases, state and federal statutes, and a growing discussion among legal scholars appear to reflect the emergence of a new paradigm of privacy law that could affect the way that ITS programs are developed, deployed, and used. Consequently, in addition to keeping an eye on developing technologies, ITS planners should also continue to stay aware of legal developments that will impact what information is, and is not, "private." The current fragmented nature of privacy protections in the United States is likely to create obstacles for the implementation of ITS technology networks that cross jurisdictional lines. In order to overcome these obstacles, strategic privacy regime reform needs to take place at all levels of government. This reform should create guidelines for the managing of ITS information and data practices which maximizes the benefit of developing ITS technologies while also providing uniform protections for citizens' privacy interests.

References

1. Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 *San Diego L. Rev*. (2007)

2. Daniel J. Solove, "A Taxonomy of Privacy." 154 *U. Pa. L. Rev*. 477 (2006)

3. Adam Kokotovich & Lee W. Munnich Jr., "Thinking Privacy with Intelligent Transportation Systems: Policies, Tools, and Strategies for the Transportation Professional." In Transportation Research Board 2007 Annual Meeting CD-ROM, Transportation Research Board of the National Academies, Washington, D.C., 2007, paper number 07-2646

4. Paris Adult Theatre I v. Slaton, 413 U.S. 49, 93 S.Ct. 2628 (1973)

5. Whalen v. Roe, 429 U.S. 589 (1977)

6. Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age.* NYU Press, New York, NY, 2004

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

8. U.S. Const. amend. IV

9. Jim Barr Coleman, "Digital Photography and the Internet, Rethinking Privacy Law," 13 *J. Intell. Prop. L.*, 205 (2005)

10. Paul v. Davis, 424 U.S. 693 (1976)

11. United States v. Knotts, 460 U.S. 276 (1983)

12. William L. Prosser, "Privacy," 48 *Cal. L. Rev*. 383 (1960)

13. United States v. Garcia, 474 F.3d 994 (7th Cir. 2007)

14. Kyllo v. United States, 533 U.S. 27 (2001)

15. United States v. Garcia, 474 F.3d 994 (7th Cir. 2007)

16. Reno v. Condon, 528 U.S. 141 (2000)

17. Privacy Act of 1974, 5 USC Sec. 552a

18. William J. Brennan, "State Constitutions and the Protection of Individual Rights," 90 *Harv. L. Rev.* 489 (1977)

19. State v. Hunt, 91 N.J. 338, 450 A.2d 952 (1982)

20. Smith v. Maryland, 442 U.S. 735 (1979)

21. California v. Greenwood, 486 U.S. 35 (1988); California Exception:. People v. Krivda, 486 P.2d 1262 (Calif. 1971), vacated and remanded, 409 U.S. 33 (1972), reaff'd, 504 P.2d 457 (1973), cert. denied, 412 U.S. 919 (1973). Hawaii Exception: State v. Tanaka, 701 P.2d 1274 (Haw. 1985). New Jersey Exception: State v. Hempele, 576 A.2d 793 (N.J. 1990). Washington Exception: State v. Boland, 800 P.2d 1112

22. Colo. Rev. Stat. sec. 24-27-204 (3)(a); Conn. Gen. Stat. Ann. Sec. 4-190; Fla. Stat. Ann. Sec. 282.318; Haw. Rev. Stat. sec. 286-172; Minn. Stat. sec. 13.01; N.Y. Pub. Off. Law sec. 91; Ohio Rev. Code sec. 1347.01

23. Cal. Veh. Code § 9951

24. United States v. Miller, 425 U.S. 435 (1976)

25. Smith v. Maryland, 442 U.S. 735 (1979)

26. Burrows v. Superior Court of San Bernardino County, 13 Cal.3d 238, 529 P.2d 590 (1974)

27. Carli Cutchin, "Red Light Cameras," California Center for Innovative Transportation at the University of California at Berkeley and Caltrans, August 2005. Available at http://www.calccit.org/itsdecision/serv_and_tech/Safety/redlightcameras.html (accessed December 17, 2008)

28. S.495.RS, Personal Data and Privacy and Security Act of 2007 (Reported in the Senate). Available at http://thomas.loc.gov/cgi-bin/query/z?c110:S.495.RS: (accessed December 17, 2008)

29. Ray Resendes, *Vehicle Infrastructure Integration Program Status,* 2005, NHTSA, http://www-nrd.nhtsa.dot.gov/pdf/nrd-1/NRDmtgs/2005Honda/Resendes_VII.pdf (accessed October 26, 2007).

30. The Company v. United States of America, No. 02-15635, 2003 CV 01-01495, (9th Cir. Nov. 15, 2003)

31. On Star, On Star Privacy Policy (2007), available at http://www.onstar.com/us_english/jsp/privacy_policy.jsp (accessed November 15th, 2007).

32. Cal. AB 213, Chap. 427 (2004); Ark. SB. 1419 (2004)

33. Matos v. Florida, 899 So. 2d 403 (Fla. App 2005)

34. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, (S.D.N.Y. 2003)

35. 18 U.S.C. §§2721- 2725 (1994)

36. K&L Gates, "E-Discovery Amendments to the Federal Rules of Civil Procedure Go Into Effect Today", December 2006, http://www.ediscoverylaw.com/2006/12/articles/news-

updates/ediscovery-amendments-to-the-federal-rules-of-civil-procedure-go-into-effect-today/ (accessed December 17, 2008)

37. Agomo v. Fenty, 916 A2d 181 (Dist Col App 2007)

38. State v. Guminga, 395 NW2d 344 (Minn. 1986)

39. John Gartner, "Insurance Company Offers Discounts to Tracked Teens," *Telematics Journal*, April 9, 2007

40. State v. Kuhlman, 729 N.W.2d 577 (Minn.2007)

41. Minn. Stat. § 169.444 Subd. 1a

42. Robert O'Harrow Jr., "Centers Tap Into Personal Databases," *Washington Post*, Apr. 2, 2008

43. Andrew J. McClurg, "Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places." 73 *N.C. L. Rev*. 989 (1995)

44. Dorthy J. Glancy, "Privacy on the Open Road" (The Twenty-Seventh Annual Law Review Symposium Privacy and Surveillance: Emerging Legal Issues). 30 *Ohio N.U. L. Rev*. 295 (2004)

45. Norman Y. Mineta, "Remarks to Santa Clara University Community Meeting on Privacy and Intelligent Vehicle Highway Systems August 30, 1994." 11 *Santa Clara Computer & High Tech. L.J.* 3 (1995)

Appendix A

Toolbox for Identifying Privacy Issues

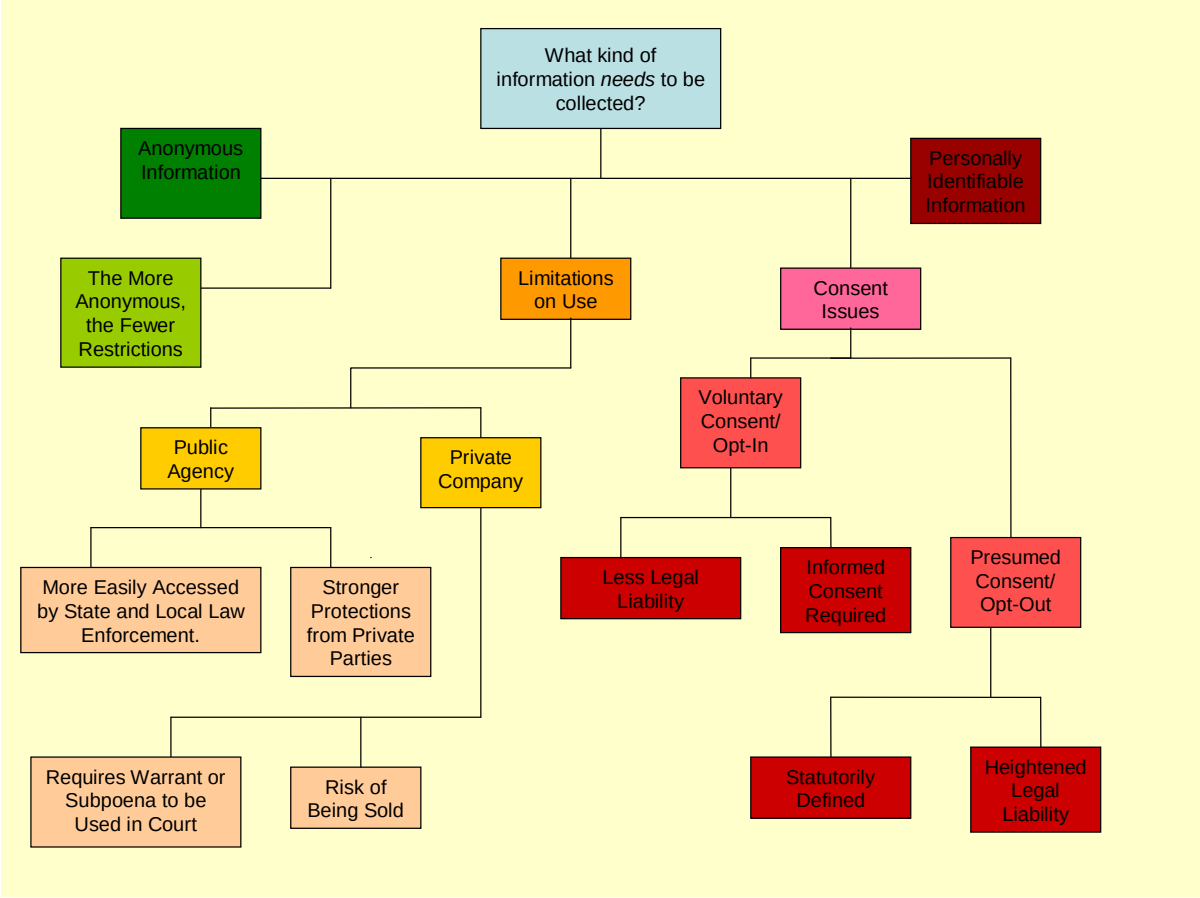

Figure A-1: Toolbox for Identifying Privacy Issues

Appendix B

Taxonomy of Privacy Expectations and Legal Protections

Table B-1: Taxonomy of Privacy Expectations and Legal Protections

TYPE OF OBSERVATION	**PURPOSE OF OBSERVATION**	**VEHICLE INFORMATION / IDENTIFICATION**	**OCCUPANT DRIVER INFORMATION / IDENTIFICATION**	**PRIVACY EXPECTATION & LEGAL PROTECTION**
TRAFFIC FLOW (I.E. TRAFFIC COUNTER, TRAFFIC CLASSIFIER)	INFORMATION ABOUT SYSTEM USE	NO INIVIDUAL VEHICLE INFORMATION OBTAINED	NONE	LOW
ANONYMOUS INDIVIDUAL VEHICLE OBSERVATION (I.E. LOOP DETECTOR AT INTERSECTION TO CONTROL TRAFFIC SIGNAL)	MANAGING SYSTEM USE	NO INIVIDUAL VEHICLE INFORMATION OBTAINED	NONE	LOW
INDIVIDUAL VEHICLE OBSERVATION (I.E. LISCENSE PLATE READER, TOLL TRANSPONDER)	REGULATING OPERATION OF SPECIFIC VEHICLE ADMINISTRATIVE REGULATION OF VEHICLE ACCESS TO SYSTEM (ALSO TWO ABOVE PURPOSES)	VEHICLE IDENTIFICATION OBTAINED; LICENSE PLATE OBSERVATION RFI SIGNAL FROM VEHICLE WITH VEH ID INFO	POSSIBLE THRU ACCESSING VEHICLE REGISTRATION SYSTEM	MEDIUM
OCCUPANT OBSERVATION ANONYMOUS (I.E. INFRA RED CAR POOL LANE SCANNER)	SYSTEM USE INFORMATION (ALSO THREE ABOVE PURPOSES)	ABOVE INFORMATION	ANONYMOUS INFORMATION ABOUT DRIVER & PASSENGERS (I.E. # OF OCCUPANTS, GENDER, AGE)	MEDIUM
OCCUPANT OBSERVATION:DRIVER IDENTIFICATIONCAMERA, BIO-METRIC (FINGER PRINT TOUCH PAD VOICE ID)	ABOVE PURPOSES AND ADMINISTRATIVE AND CRIMINAL REGULATION OF DRIVER	ABOVE INFORMATION	ACTUAL OR ASSUMED(REGISTERED OWNER) ID OF DRIVER VACARIOUS CRIMINAL LIABILITY	CIVIL:HIGH CRIMINAL:HIGHEST