ARTICLE: THE CHALLENGE OF ITS FOR THE LAW OF PRIVACY

NAME: Frank Douma and Jordan Deckenbach+

BIO: + Frank Douma is a Research Fellow and the Assistant Director of the State and Local Policy Program at the University of Minnesota's Hubert H. Humphrey Institute of Public Affairs. Jordan Deckenbach served as Research Assistant on this project and received his Masters of Public Policy and J.D. from the University of Minnesota in 2008. 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. We also acknowledge the valuable input of the anonymous reviewer of this article and the efforts of the Journal editorial staff. 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, indispensable assistance in developing the privacy taxonomy and timely, on-point recommendations of multiple sources.

SUMMARY:
... State Tort Protections of Privacy State privacy torts have been a fundamental source of privacy protection in the United States. ... A higher standard of protection is placed over personal information in a civil case; however, technology and records that are not privately held by a party have not traditionally enjoyed the privacy protections from subpoenas in a civil suit that have been granted to personal records. ... 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, present in almost all states. ... Whether dealing with personally identifiable ITS information collected by public agencies or private companies, ITS planners and developers should adopt best practices principles that 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. ... 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. ... 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.

HIGHLIGHT: Abstract

As Intelligent Transportation Systems ("ITS") incorporate data-gathering and compiling systems into the transportation infrastructure, new privacy implications stemming from the potential misallocation or abuse of collected data have been created. The United States currently has no comprehensive national regulatory structure for privacy, leaving answers to these privacy concerns to be found through a consideration of a variety of sources of federal and state privacy law. In this paper, the authors examine a number of areas where privacy law could impact ITS projects and technologies,
including constitutional privacy protections from criminal prosecution; the developing legal distinctions of reasonable privacy expectations; the role of evolving surveillance technologies in defining privacy rights; the evolution of vicarious criminal liability theories; and the use of tort law in the remediation of privacy violations. There is evidence that privacy law in the United States is undergoing a paradigm shift in response to data collection by new technologies, and the privacy concerns raised by the deployment of ITS are just one of the factors giving rise to a movement towards a stricter, or at least more comprehensive, privacy regime. After a consideration of the legal implications of ITS technologies, the authors present a legal toolbox and taxonomy for ITS developers to utilize in navigating the current legal landscape with their emerging technologies.

TEXT:
[*296] I. 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 alternate 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 of $315.00 worth of traffic infractions that were recorded and reported to local law enforcement agencies by his vehicle's 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.

Whether or not this hypothetical will ever come to complete fruition is yet to be seen. Currently the focus of ITS is largely on improving transportation safety, mobility and enhancing productivity, through the utilization of technologies that can improve individual driving performance and help manage overall traffic congestion. ITS technologies include systems such as automatic toll way transponders, in-vehicle navigation systems, and signal controls. These technologies are placed both in the transportation system infrastructure, as well as in vehicles, and use advanced wireless and wireline communications technologies to transmit information about individual vehicles or traffic zones to centralized databases or other local systems that process the information to produce helpful feedback. Once the driving information is processed, ITS systems can help individual drivers by providing improved route selections, producing alerts to upcoming road hazards, and creating unencumbered access to toll lanes and high-occupancy vehicle lanes. They can even help drivers respond quickly and safely to immediate road conditions or the driving behavior of others around them. ITS technologies can also provide traffic planners and engineers with valuable information pertaining to road usage and general driving patterns and behavior.

ITS technologies that monitor driving behavior are also beginning to be used to enforce traffic laws. Red light cameras as well as speed cameras are two well-known examples of ITS technologies that aim to improve roadways through the direct enforcement of laws. However, the use of other ITS technologies not originally intended to be part of an enforcement regime are beginning to be used towards an enforcement end. For example, the United States Department of Transportation's "Intellidrive" 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 United States 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 ITS technologies 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 States, 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 United States will inform ITS planners and developers in their efforts to alleviate citizens' privacy concerns through technology design and the adoption of privacy protection principles.

This Article 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 affected the management of other information systems and data practices will help ITS developers and planners navigate the current legal landscape, as well as serve as a basis for new legal and technological solutions that could accommodate emerging ITS innovations. After an overview of the implications of both state and federal privacy law on ITS technologies, a toolbox is presented that 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.

II. 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 essence 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." These digital dossiers affect the daily lives of many individuals through influencing what financial institutions 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 potentially showing where that individual works, sleeps, worships and recreates with others.

The legal concept of privacy in the United States is an evolving one. The organic development of this concept has led to a vast literature on the concept and its impact on everything from birth to near death. Solove describes "privacy" as a "shorthand umbrella term for a related web of things." Thus, he points out the importance of articulating "what privacy means" before discussing the issues raised by a particular action or policy. We start from a policy-based perspective, where analysis defines 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.

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. 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. 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.

In the context of ITS, concerns primarily implicate the behavioral and informational aspects of privacy. ITS technologies that constantly monitor the movements of a vehicle on behalf of the government or private parties can have a major impact on the driver's behavior and decisions. When it is known that law enforcement agencies, insurers, employers, private companies or family members are utilizing ITS technologies to track a vehicle's movements, the ability to travel where and when one pleases is hampered by the potential for that information to be shared with others. The result of the constant monitoring is the loss of the driver's ability to move autonomously.

A. Relationship between Federal and State Privacy Protections

The legal landscape for privacy in the United States is not easily navigated. Overall, the approach of the U.S. government to comprehensive privacy law has been fragmented, incomplete, and discontinuous as Congress and most presidential administrations have avoided broad overarching reforms and regulations on privacy law since the 1970s. Unlike most Western nations, the United States has failed to create institutions that are charged with direct responsibility in monitoring and regulating a legal regime that comprehensively protects citizen data and information. The U.S. also differs from other Western nations by relying on several legal bases for privacy law, as opposed to relying on centralized privacy legislation. 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 U.S. privacy laws, how they relate to one another, and 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 that are likely to infringe upon expectations of personal privacy, specifically when the utilization of personal information results in the curbing of societal privileges.

While the right to privacy is not expressly protected in the United States Constitution, 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 "fundamental" or "implicit in the concept of ordered liberty." 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 ... the interest in independence in making certain kinds of important decisions." 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.

Congress has supplemented informational privacy protections through 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 that have warranted Congressional attention. Another reason for the lack of overarching federal privacy regulation is the federal government's traditional deference to individual states in the matter of determining their own privacy regimes.

When the federal law has failed to be proactive in providing privacy protections and limitations on how personal information is used, states have established increased levels of protection through local legislation and expanded privacy rights through court rulings and state constitutions. This is in line with the 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."
Though it is 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 Intellidrive are working to establish a nationwide network of integrated ITS programs resulting in a unified federal intelligent transportation system. Though some of these systems seek to only utilize anonymous vehicle information, the Intellidrive 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 regulations. 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. To fully understand how all of these regulations fit together, however, one should start with an analysis of current federal law.

B. Federal Privacy Laws

1. Federal Constitutional Protections of Privacy

The fundamental source of legal protection and redress for privacy violations by state actors is constitutional interpretation. Here, the Constitution provides two routes by for the 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." This has been interpreted 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." Though apparently protective of behavioral privacy, Supreme Court case history incorporates an element of spatial privacy by continuing to use locational factors in determining whether an expectation of privacy has been demonstrated and whether or not that expectation is reasonable. Because the Fourth Amendment addresses searches, seizures, and the issue of warrants, its case law and interpretation comes predominantly from 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 viewed in light of ITS later in this Article.

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 Ninth and Fourteenth 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." Privacy protections stemming from these amendments may be applicable to the privacy concerns raised by ITS as the 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" based in these constitutional provisions.

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

2. Building (Home) v. 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." n62 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 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." n63 In 1983, the Supreme Court then explicitly applied this interpretation to automobile travel, ruling 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." n64

Likewise, vehicles are unlikely locations to benefit from the protections afforded to privacy by 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." n65

3. Evolving Surveillance Technologies

Advances in technology require an examination of their potential impact on 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. n66 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." n67

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]," n68 a warrant is required when the "technology in question is not in general public use." n69

However, it is not clear how this limitation would apply to ITS. The Supreme Court defined this limitation in Kyllo v. United States, a case in which police used heat sensing technology to determine whether the suspect may be growing marijuana inside a home, by finding there is a legally relevant spatial distinction between one's home and elsewhere, including one's car, when it [*305] comes to privacy expectations. n70 A recent case in the Seventh Circuit Court of Appeals indicates that this distinction could be a significant one, as it allowed police to use a GPS device to track the movements of a suspect's car without obtaining a warrant. n71 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. n72

The implications for ITS under privacy requirements of the Constitution are currently small as the 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 to determine that a public expectation of a certain level of privacy in their vehicles is reasonable, creating a potential way for the court to extend the protective 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. n73

4. 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, to address the specific privacy issue of surreptitious sexual photography done mostly with cell-phone cameras Congress passed the Video Voyeurism Prevention Act of 2004, criminalizing taking and distributing some types of photograph without their subject's consent.\(^\text{n74}\) Likewise, the Driver's Privacy Protection Act of 1994 was passed in response to stalkers' use of driver's license records.\(^\text{n75}\) It is worth noting 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 Fourteenth Amendment authority to legislatively protect individual rights from state encroachment.\(^\text{n76}\)

The Privacy Act of 1974\(^\text{n77}\) may be the most overarching legislation passed by the federal government in relation to how government agencies are required to handle information about citizens. The Act mandates that administrative and physical security systems be put in place to avoid the unauthorized release of information to third parties.\(^\text{n78}\) Interagency 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.\(^\text{n79}\) Under this act, citizens have the right to demand access to records collected by any ITS programs that collect personally identifiable information about them.\(^\text{n80}\) 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 in the last ten years there have been exceptions to this law. 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.\(^\text{n81}\) 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.

C. State Privacy Laws

As previously mentioned, federal law sets the floor of privacy protection upon which states can 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 uniformly 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 face choices regarding the best strategic legal approach to ITS information gathering and utilization that will realize the greatest benefit of the technologies with as little state interference as possible.

\(^{[*307]}\)

1. State Constitutional Protection of Privacy

Constitutions in ten different states - Alaska,\(^\text{n82}\) Arizona,\(^\text{n83}\) California,\(^\text{n84}\) Florida,\(^\text{n85}\) Hawaii,\(^\text{n86}\) Illinois,\(^\text{n87}\) Louisiana,\(^\text{n88}\) Montana,\(^\text{n89}\) South Carolina,\(^\text{n90}\) and Washington\(^\text{n91}\) - explicitly recognize a citizen's right to privacy. Other states have derived a right to privacy from the text of their constitutions.\(^\text{n92}\) The Supremacy Clause of the U.S. Constitution sets a floor, not a ceiling, on the state's interpretation of citizen privacy rights.\(^\text{n93}\) 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.\(^\text{n94}\) As the U.S. Supreme Court has been reluctant to expand privacy rights based on the Fourth and Fourteenth 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 federal protections 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 that similar phone company records were not protected by the federal constitution. The New Jersey Supreme Court reasoned that "technological 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." 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 are a natural extension of the home under the New Jersey Constitution as well. 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 states have decided that such searches violate their state constitutions, as garbage on the curb is protected as items in the home would be. 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 and would depend 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 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 select jurisdictions. The burdens and inefficiencies of such an approach is unattractive, 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 in some jurisdictions.

2. 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 the kind of information being collected; avenues of access for citizens to see what information is being collected about them and to make appropriate corrections; limitations on secondary usage of individual information; and security requirements for how that information is maintained. 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 that specifically address privacy rights and transportation technologies. Most laws
that have been passed address only those specific technologies whose use is widely unpopular due to public perception of a potential for abuse of such technologies. An example of this would be the banning or limiting of photo radars in at least five different states - California, New Jersey, Oregon, Utah and Wisconsin.

Another example of a state's response to emerging transportation technologies is California's "black box" laws, which regulate the use and access to information gathered by a vehicle's event data record. Insurance companies and automobile manufacturers often desire the information in these boxes to determine liability in instances of crashes or other instances. The California law dictates that 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.

3. 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 and to ensure that the 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. These largely constitute protections 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 when one is on the public streets. Further, most of these torts rely upon an intrusion that occurs where the victim had not consented to giving up his privacy. While government has an interest in possibly observing private acts (albeit with a warrant) to protect the public safety, such action tends not to be in the interest of private industry - or, at least the ITS industry. For example, the Intellidrive initiative explicitly stated that it would not use the information collected to support law enforcement. Rather, 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 pitfall of only relying on the common law for establishing privacy standards to regulated ITS information gathering and utilization 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 that it would create for consumers in challenging abuses of information. Though the private sector enjoys this buffer, arguably protecting them from frivolous claims of abuse, consumer and privacy advocacy groups are likely to demand clear statutory protections that can inform consumers of their rights and remedies without having to wade into the murky legal world of tort litigation.

III. Potential Legal Issues for ITS Information

A. Personal Information in the Context of the Third Party Doctrine

It is possible that courts may find that certain types of personal information collected by ITS technologies are not afforded any privacy protections under the third party doctrine, which dictates that certain information in the hands of a third party does not warrant Fourth Amendment protection.
In the 1970's, the Supreme Court handed down a number of rulings in regard to the constitutional protections of citizen's personal bank accounts that established the "third party doctrine," leaving much of this information in the public realm. In United States v. Miller, the Supreme Court established that personal information held by banks constitutes business records and is not of a "private" nature, so citizens did not have a reasonable expectation of keeping their records private. 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.

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

However, California courts have found the third party doctrine to be lacking in certain instances, specifically in regards to information gathered from activities necessary for participation in the "economic life of contemporary society." 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. 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 similar concerns from state courts and trigger state level constitutional information privacy protections that 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.

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 many different private ITS companies. 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 increasingly relied on outsourcing the gathering and managing of information to private companies because they do not face the same liabilities and limitations placed over government agencies. While 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 that 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 any business entity (defined in a way that would include many ITS companies) and also calls for strong penalties on these companies when they fail, inter alia, to reasonably protect sensitive personally identifiable information. If ITS technologies are run by private companies on behalf of government agencies, they are likely to invite burdensome oversight and regulation in response.

C. 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 one instance, a dashboard computer system was used by the FBI to eavesdrop on conversations in a vehicle believed to be used by drug dealers. 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 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. 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 to provide the prescribed services or if required to do so by law.

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 that have been asked to comply with warrantless wiretaps and executive orders by the president in the name of national security. 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.

D. 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, as discussed earlier, private insurance companies have already attempted to assert a right to information from a vehicle's Event Data Recorder ("EDR"), also known as an auto black box, in order to ascertain the cause of an accident. Privacy advocates have balked at the assertion that individuals should be required to turn over vehicle data to private actors in the event of an accident, as such information is the personal property of the driver and could be self-incriminating in court. Federal law has tried to make such information more technically accessible to private companies for use in civil litigation, however some states have responded with laws which make the information from EDR's private. Courts, however, have manifested a 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. 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 that are not privately held by a party have not traditionally enjoyed the privacy protections from subpoenas in a civil suit that have been granted to personal records.

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. However, he also points out that the 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 that the long term value of keeping promises exceeds any short term value that comes from a violation of 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, as including "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." 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. 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 that 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 could become bogged down with an overload of requests from lawyers looking to access information relevant to their case.

D. Automatic Enforcement and Vicarious Liability

One of the most complicated legal arenas ITS technologies face is 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 that identify offending vehicles, and they have been implemented in 25 U.S. states. Automatic enforcement technologies are appreciated as an efficient tool that 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.

[*316] 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 vicarious liability.

Vicarious liability already exists in some shape or form in most jurisdictions, usually in laws 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 quasi-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, usually claim a violation of due process because of the automatic assignment of guilt in a judicial system that assumes innocence unless guilt can be proven. 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 that 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, potentially resulting 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.

[*317] The potential for in-vehicle 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 that measure the amount of alcohol in a driver's system before the vehicle is able to start. 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 used to 
monitor, record, and possibly transmit the offender's future driving conduct to the government.

The private market is already producing incentives for in-vehicle monitoring systems that report illegal behavior. An 
insurer in Arizona, Illinois, New Jersey, Pennsylvania, South Carolina, and Washington implemented pilot programs 
in 2007 that reduce rates for policy holders who are willing to place GPS units in teenagers' vehicles to report to the 
insurer and the parents when the teen has violated any speed limits. 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, present in almost all states. 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 Seventh Circuit 
opined that use of cameras on lamp-posts would not raise privacy issues, the Minnesota Supreme Court recently 
considered whether the use of red light enforcement cameras to assign vicarious quasi-criminal liability violated due 
process. The court, ultimately ruling on preemption grounds and not considering the constitutional issue, 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. 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.

E. 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 article looks to establish tools for ITS developers and planners that explain the level of restrictions 
corresponding 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 I). The toolbox is meant to help planners and 
developers anticipate the legal implications of their technology design and utilization choices.

1. Anonymous vs. Personally Identifiable Information

ITS information is likely to fall within on a wide 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 [*319] vehicle. Examples of anonymous information would include information collected by traffic counters or devices that detect the presence 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 to achieve their purpose (i.e., charging tolls to drivers; congestion pricing; red light cameras, etc.). To avoid legal barriers to the functionality of these technologies, ITS developers have attempted 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. n163 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. n164

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 that minimize the necessity of its collection and storage, thus avoiding the burdensome legal restrictions. This will require new approaches to collection anonymization processes.

2. 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 drivers can give consent. Voluntary or opt-in consent is one way that consent can be given. This 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 for consent to be complete. Examples of information that need 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 [*320] 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, so-called opt-out consent. Local and state statutes can define consent as legally implied by a driver's use of roadways that 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. n165 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. n166 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. n167 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 choose opt-in or 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 [*321] ultimate say in tort liability of ITS providers. If legislatures statutorily define consent to be implied by use of public roadways that 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.

3. Public vs. Private Actors

States' willingness to enact protections over collected information varies greatly. n168 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. n169 The previously mentioned Privacy Act of 1974 is currently the principal federal regulation limiting how government entities share and collect information on citizens, n170 while only a few private industries and companies, such as medical providers n171 and credit agencies, n172 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 benefit 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 [*322] collaborate with other sources of information. However, there is also a potential risk of information being sold to and misused by third parties, such as private companies that want to obtain ITS information for the purposes of target marketing, consumer behavior monitoring or qualifying driver's insurance rates. n173 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 about 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 of their jurisdiction that severely limit secondary use of personal information. Some privacy advocates have proposed that personal information be protected through transferring ownership of collected personal information from the company to the individual. n174 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 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 that can be used for investigatory and security purposes. 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 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 that 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 allow law enforcement to freely scavenge large amounts of data in a way that could turn up useful information and uncover further wrong doing, while also potentially exposing innocent parties to egregious violations of their most intimate privacy expectations.

F. 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 that 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 Article 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 his 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 II).

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 identify the presence of an individual vehicle, they do not 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 include automated toll systems, congestion 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 license 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 expectations arise 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 infrared 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 driver's age, race, and gender. As previously mentioned, these technologies also can capture vehicle information that can be traced back to the owner. When this information is collected for general administrative purposes, such as managing system use, only a small amount of privacy expectation exists. However, when this information is collected for the purpose of enforcing laws on the road, it increases the privacy expectation and legal restrictions on how that information can be collected.

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 establishing clear privacy guidelines that dictate the extent to which they are going to manage and protect individual users' information from inappropriate use by both private and public parties.

IV. 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."\(^{186}\) 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.\(^{187}\) 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\(^{188}\) and must be litigated in a legal environment that is, at times, openly contemptuous towards allegations of a privacy violation.\(^{189}\) It is through this understanding that a paradigm of "privacy in public" can emerge in a manner that is applicable to ITS.

A. 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."\(^{190}\) 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\(^{327}\) movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.\(^{191}\)

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.
B. Trends in academic analyses

Legal academics have pushed strongly for a whole new paradigm of privacy, due in part to the belief that the construction of the existing privacy rule was inadequate to begin with and in part to the assessment that "however sound this rule once may have been, it is flawed in a modern technological society." 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. 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" that 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." The idea is that privacy be treated as "a matter of degree," not "as an all-or-nothing concept." 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 rejects the legal equivalency of unaided visual observation, technology-assisted observation, and technology-enabled recording. This train of thought calls 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. Others criticize the treatment of technological surveillance as equivalent to actual or hypothetical visual surveillance because it focuses on the behavioral aspect of privacy and ignores the social harms of enhanced surveillance, such as the loss of trust it engenders and its enhancement of state power against the individual, and the greater dignitary harm and chilling effect of data collection incorporating artificial aids. 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.

V. 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.

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 [*329] 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. Strategic privacy regime reform needs to take place at all levels of government to overcome these obstacles. 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.

[*330]
Appendix I

[SEE APPENDIX I IN ORIGINAL]

[*331]
Appendix II

Vehicle & Person Using Transportation System

Observation & data gathering - purpose for information - privacy expectations and legal protection of privacy interest

[SEE APPENDIX II IN ORIGINAL]

Legal Topics:

For related research and practice materials, see the following legal topics:

FOOTNOTES:


n7. E.g., Intelligent Transportation Systems Fact Sheet, supra note 1.

n8. Id.

n9. Id.


n15. See Agomo v. Fenty, 916 A.2d 181, 194 (D.C. 2007) ("It is entirely rational to presume that a vehicle is in the custody, care, or control of its registered owner.").


n17. See id. at 4-5 (explaining that marketers are able to collect detailed dossiers of personal information in order to predict consumer behavior and "encourage customers to consume.").

n18. See id. at 170-72 (describing the government's use of data in various security measures inspired by the September 11th terrorist attacks).

n19. Id. at 5.
n20. Id. at 166-68.

n21. Id. at 4.

n22. Id. at 3.

n23. Id.

n24. Id.


n26. Id. at 754.


n28. Id.

n29. See Solove, Misunderstandings of Privacy, supra note 27, at 759 (arguing that real problems arise and they are ignored by the law because they do not fit into prefabricated notions of privacy).
n30. Id. at 760.


n32. Kokotovich & Munnich Jr., supra note 27.


n34. Kokotovich & Munnich Jr., supra note 27.


n37. Kokotovich & Munnich Jr., supra note 27.

Privacy Protections in State Constitutions (last visited Oct. 27, 2009)


n40. See id. at 41-44 (discussing the torts related to privacy).


n45. See, e.g., Sandra Byrd Petersen, Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?, Fed. Comm. L.J. 163, 182-83 (1995) ("Congress has looked only to the problem immediately facing it. This has resulted in solutions that are far too shortsighted and reactionary.").


n49. See Glancy, supra note 10 at 365-66 (describing how anonymous traffic flow information becomes personally identifiable information when a vehicle license plate or toll tag identifier is matched to a vehicle owner, which can be cross-checked with comprehensive data containing name, address, security number, etc. of the vehicle owner).

n50. Id.

n51. Kokotovich & Munnich, Jr., supra note 27.

n52. U.S. Const. amend. IV.


n55. United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).


n60. U.S. Const. amend. XIV § 1.


n63. Id. at 361.


n66. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

n67. Prosser, supra note 65, at 394-95.

n68. Knotts, 460 U.S. at 282.


n70. Id. at 29.

n71. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

n72. Id. at 997. See generally Ramya Shah, From Beepers to GPS: Can the Fourth Amendment Keep up with Electronic Tracking Technology?, 2009 U. Ill. J.L. Tech. & Pol’y 281 (discussing the Fourth Amendment and GPS tracking technology).

n73. See Shah, supra note 72 (distinguishing a case where technology that served as a substitute for physical intrusion from this case featuring permissible uses of technology).


n75. Driver’s Privacy Protection Act, 18 U.S.C. § 2721 et. seq. (2006); Solove, Misunderstanding of Privacy, supra note 25, at 768.
n76. See Reno v. Condon, 528 U.S. 141, 151 (2000) (declining to address the claim that general applicability of a statute is a constitutional requirement for regulation of the states).


n78. § 552(e)(10).

n79. §§552(b), (d)(1).

N80. § 552(d)(1).


n82. Alaska Const. art. 1, § 22.


n84. Cal. Const. art. 1, § 1.

n85. Fla. Const. art. 1, § 23.


n89. Mont. Const. art. II, § 10.


n92. See e.g., Jegley v. Picado, 80 S.W.3d 332, 350 (Ark. 2002) ("[A] fundamental right to privacy is implicit in the Arkansas Constitution."); Commonwealth v. Wasson, 842 S.W.2d 487, 495 (Ky. 1992) ("The right of privacy has been recognized as an integral part of the guarantee of liberty in our 1891 Kentucky Constitution since its inception.").

n93. See Oregon v. Hass, 420 U.S. 714, 719 (1975) ("[A] State is free as a matter of its own law to impose greater restrictions on police activity than those this Court holds to be necessary upon federal constitutional standards" (emphasis in original)); Cooper v. California, 386 U.S. 58, 62 (1967) ("Our holding, of course, does not affect the State's power to impose higher standards on searches and seizures than required by the Federal Constitution if it chooses to do so.").


n97. Hunt, 450 A.2d at 954-55.


n101. See Conn. Gen. Stat. § 4-193 (2007) (governing state agency collection and dissemination of information on individuals); § 4-194 (governing petitions to state superior court to disclose medical information, which a state agency refused to disclose).


n109. See Gellman, supra note 36, at 201 (listing several different areas in which the government regulates records).


n116. Cal. Veh. Code § 9951(c) (requiring that only the registered owner may download or otherwise retrieve data on an event data recorder; provided, however, that access may be allowed to another individual pursuant to consent of the registered owner or a court order).


n118. See id. at 19-24 (listing such states and citations to their supreme courts' decisions).

n119. Prosser, supra note 65, at 389.

n120. Resendes, supra note 48, at 20.


n124. Id. at 594.

n125. Id. at 596.


n129. In re United States for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d 1132 (9th Cir. 2003).

n130. Id. at 1146.

n131. Id.
See, e.g., OnStar.com, OnStar Privacy Statement (2009), http://www.onstar.com/us_english/ jsp/privacy_policy.jsp (including broad purposes such as "to provide OnStar services to you, including checking and maintaining your OnStar equipment; to communicate with you about your account; for trouble shooting; for analysis and research; as required by law; to protect our rights or property of the safety of you or others; to prevent fraud or misuse of the OnStar service; and to offer you new and additional products or services") (emphasis added).


No person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V.


Solove, Misunderstanding of Privacy, supra note 25, at 754.

Id. at 746.


n146. Id. at 306-07.


n151. Glancy, supra note 12, at 304.


n153. E.g., Agomo v. Fenty, 916 A.2d 181, 193 (D.C. 2007) (“Systems of vicarious liability that impose civil liability are not contrary to the notions of due process.”).

n154. E.g., State v. Guminga, 395 N.W.2d 344, 346 (Minn. 1986) (holding that statute imposing vicarious liability violates substantive due process because of penalties that may include jail time and because, even if prison sentence is not imposed, a conviction would affect the defendant’s criminal history score should he “be convicted of a felony in the future.”).


n158. U.S. v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007).

n159. State v. Kuhlman, 729 N.W.2d 577, 584 (Minn. 2007).
n160. Id. at 579.

n161. Id. at 581-82.


n165. E.g., 625 Ill. Comp. Stat. 5/11-501.1 (providing for the suspension of one's driver's license if they are found to be driving under the influence of intoxicating materials).

n166. E.g., State v. Hudes, 128 N.J. Super. 589, 605 (1974) ("defendant did not even have the legal right to refuse to submit to the breathalyzer test since his very driving upon the highway acted as his consent to the taking of samples of his breath").

n167. For example, most states have implied consent statutes subjecting licensed drivers to chemical sobriety tests if charged with driving under the influence. Drivers are typically made aware of such implied consent through published driver licensing handbooks. E.g., Cal. Vehicle Code, Div. 11.5, Ch. 4, Art. 1 § 23612(a)(1)(A).

n168. See supra II.C.1.


n173. Glancy, supra note 10, at 313, 323.


n177. See Joseph T. Thai, Is Data Mining Ever A Search Under Justice Steven's Fourth Amendment?, 74 Fordham L. Rev. 1731, 1738 (2006) (discussing marketing by LexisNexis of their Accurint software to law enforcement agencies as a way to save time and costs).


n181. See e.g., Steven Hansen, Robert Bertini, Using an Intelligent Transportation System Data Archive to Improve Student Learning at Portland State University, (June 2005) (presented to American Society for Engineering Education) (describing use of loop sensors).


n183. Glancy, supra note 10 at 301.

n184. See id.; Pool supra note 182 (describing techniques using technology to return identifying information about vehicles).


n186. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).
n187. Rupert, supra note 11; Solove, Taxonomy, supra note 33; K&L Gates supra note 143.

n188. Solove, Misunderstandings of Privacy, supra note 25, at 745.


n191. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

n192. McClurg, supra note 189, at 990.

n193. Id. at 1036.

n194. E.g., Coleman, supra note 54, at 225-27; Glancy, supra note 10, at 353-54; McClurg, supra note 189, at 991-92.

n195. Coleman, supra note 54, at 225.

n196. McClurg, supra note 189, at 1040-41.
n197. Id. at 1041-44.

n198. See Glancy, supra note 10, at 320-22, 327-32 (discussing potential harms to individuals and society that can result from data gathering and surveillance through technology).

n199. See Solove, Taxonomy, supra note 33, at 506-11, 539 (discussing the new privacy issues and risks introduced by data aggregation, as well as online accessibility of data).


n201. See Janet Hope, Biobazaar: The Open Source Revolution and Biotechnology 10-13 (2008) (discussing the proprietary and open-source approaches to software copyright).