ITS and Privacy Laws Overview

Course No: C02-052

Credit: 2 PDH

Mark Rossow, PhD, PE, Retired

Continuing Education and Development, Inc.
22 Stonewall Court
Woodcliff Lake, NJ 07677

P: (877) 322-5800
info@cedengineering.com

ITS and Locational Privacy: Suggestions for Peaceful Coexistence

Final Report

Prepared by:

Frank Douma
Sarah Aue

Hubert H. Humphrey School of Public Affairs
University of Minnesota

CTS 11-21

Technical Report Documentation Page

1. Report No. CTS 11-21	2.	3. Recipients Accession No.	
4. Title and Subtitle ITS and Locational Privacy: Suggestions for Peaceful Coexistence		5. Report Date October 2011 6.	
7. Author(s) Frank Douma, Sarah Aue		8. Performing Organization Report No.	
9. Performing Organization Name and Address State and Local Policy Program Hubert H. Humphrey Institute of Public Affairs University of Minnesota 301 19th Avenue South Minneapolis, Minnesota 55455		10. Project/Task/Work Unit No. CTS Project #2010061 11. Contract (C) or Grant (G) No.	
12. Sponsoring Organization Name and Address Intelligent Transportation Systems Institute Center for Transportation Studies University of Minnesota 200 Transportation and Safety Building 511 Washington Ave. SE Minneapolis, MN 55455		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code	
15. Supplementary Notes http://www.its.umn.edu/Publications/ResearchReports/			
16. Abstract (Limit: 250 words) Continuing developments in the fields of transportation technology and privacy law present an abundance of opportunities for conflict. Without knowledge of the legal framework that applies to emerging technology, Intelligent Transportation System (ITS) developers set themselves up for frustration as ideas that appear flawless in an engineering office may become controversial when they reach the implementation stage. From the legal perspective, advocates of comprehensive privacy law struggle to update existing law at a pace that keeps up with innovative advancements in technology. This paper reviews several cases where implementation of transportation technologies has raised civil liberties arguments, examining them from legal and political perspectives. The understanding of privacy both as a political concept and a legal protection provides the foundation for future ITS progress, allowing new technologies to be developed in ways that can withstand these types of challenges or avoid them altogether.			
17. Document Analysis/Descriptors Intelligent transportation systems, Privacy, Locational privacy, Ignition seat belt interlocks, Automated enforcement, Criminal justice, Vicarious criminal liability, Event data recorders, Automated toll collection, Graduated licensing, Personally identifiable information		18. Availability Statement No restrictions. Document available from: National Technical Information Services, Alexandria, Virginia 22312	
19. Security Class (this report) Unclassified	20. Security Class (this page) Unclassified	21. No. of Pages 42	22. Price

ITS and Locational Privacy: Suggestions for Peaceful Coexistence

Final Report

Prepared by:

Frank Douma
Sarah Aue

Hubert H. Humphrey School of Public Affairs
University of Minnesota

October 2011

Published by:

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

A version of this article first appeared in *Journal of Transportation, Law, Logistics and Policy Technology and Policy*, 2nd Qtr, 78(2), 89 (2011).

Acknowledgments

We wish to acknowledge those who made this research possible. The study was funded by the Intelligent Transportation Systems (ITS) Institute, a program of the University of Minnesota's Center for Transportation Studies (CTS). Financial support was provided by the United States Department of Transportation's Research and Innovative Technologies Administration (RITA).

We would also like to extend thanks to Max Donath, Jordan Deckenbach, and Steve Simon for their support in this and previous research projects. Finally, we would like to extend our deepest gratitude to Dorothy Glancy of the Santa Clara Law School for her patient and insightful reviews and commentary as we developed this paper.

Table of Contents

List of Tables

List of Figures

Executive Summary

Continuing developments in the fields of transportation technology and privacy law present an abundance of opportunities for conflict. Without knowledge of the legal framework that applies to emerging technology, Intelligent Transportation System (ITS) developers set themselves up for frustration as ideas that appear flawless in an engineering office may become controversial when they reach the implementation stage. From the legal perspective, advocates of comprehensive privacy law struggle to update existing law at a pace that keeps up with innovative advancements in technology. Privacy issues related to electronic communications are of primary concern for transportation organizations.

This paper reviews several cases where implementation of transportation technologies has raised civil liberties arguments, examining them from legal and political perspectives. The understanding of privacy both as a political concept and a legal protection provides the foundation for future ITS progress, allowing new technologies to be developed in ways that can withstand these types of challenges or avoid them altogether.

Developers of future ITS projects will benefit by taking these political and legal principles into consideration every step of the way, from initial concept through implementation. The cases we review to illustrate this point are: from before ITS, Seat Belt Ignition Interlocks; and then a number of ITS projects, Automated enforcement, Vehicle miles traveled (VMT) taxes and electronic tolling systems, and electronic enforcement of graduated drivers licenses (GDL). Some of these are updates to existing programs and some are entirely new, but all have the potential to raise significant questions regarding locational privacy. Devices designed to collect tolls electronically, especially for VMT taxes have many privacy implications that merit consideration before implementing. Automated enforcement provides a way to review the privacy policies and practices related to an existing technology. Finally, electronic enforcement of GDL provisions allows examination of driver monitoring technology that is currently used in the private sector on a voluntary basis, but would create much more serious privacy concerns if a government entity were to mandate implementation for all novice drivers.

In light of these case studies, ITS planners and developers should take steps toward reconciling the legal and political privacy issues presented from the beginning of the design phase of a project through its implementation. While navigating the legal questions is necessary, it is just as important to consider the policy impacts of those decisions and the effect on current public perception. Recommendations for ITS planners and developers are as follows:

Recommendation 1: Public perception is as important as legal reality

Gaining public acceptance is as essential as passing legal scrutiny for seemingly intrusive technologies. Because the avoidance of legal obstacles does not guarantee favor with the general public, it is necessary to gain public trust.

Recommendation 2: The problems with personally identifiable information start with collecting it.

The first step is determining the type of information that needs to be collected as it falls along a spectrum from anonymous to personally-identifiable information. Anonymity is always preferred, but is not often seen as a realistic expectation. Anonymous solutions for upcoming technologies should be sought after, such as using a digital cash option for payment instead of collecting credit card information. When a situation does not allow for total anonymity, steps should be taken to reduce the amount of information collected. (Security of information is important as well, but is a separate issue from privacy). Perhaps the most important concept to note is that one must consider *all* of the possible uses of any personally-identifiable information, regardless of the intended use of that information gathered. For instance, if cell phone technology is used in an ITS project, planners need to remember that cell phone signals are traceable through cell tower site location information and that a vehicle's location can thus be determined either from phone records or through real-time tracking.

Recommendation 3: Alternatives increase public acceptance

Although the public perception problem may exist in a situation, it is possible to mitigate the political damage it could cause through presenting the technology as one of several options. By providing alternatives, people who opt in to use of the technology are giving up their information willingly, drastically reducing the potential for legal complaints and creating a positive political response by exercising choice. Providing the opportunity for individuals to choose to use an ITS technology results in higher acceptance of that technology. Also, when given a choice of whether to use a technology, citizens are less likely to attempt to circumvent the devices on their own.

Recommendation 4: Get the public on the same page

In order to give up this information willingly, however, the opt-in choice must be informed. Informed consent demands clarity, trust, and transparency from the agency disseminating the information. Distributing information on a technology's effectiveness and reliability is a necessary step in implementing new technology. Not only does understanding allow people to feel more comfortable with the technology, it also lays the foundation for informed consent necessary to meet legal standards.

Recommendation 5: Context – Introduce technologies at the right place, right time

It is easier to introduce new devices at a time when a specific incident encourages people to demand a government solution to an ongoing problem. Presentation of the issues within that context shows a practical application of the technology and positively affects acceptance.

Recommendation 6: Violations observed by technology should not create criminal consequences

When alternatives are not available – essentially when there is a mandate for use of a new technology – the most effective way of dealing with the highest levels of scrutiny include securing legislation that supports the program well before implementation. If there can be any

sort of criminal implication whatsoever, vicarious liability in the form of reporting a particular car and not a specific driver, is a viable solution. Imposing civil penalties with the help of advancing technology creates far fewer hurdles than creating criminal liability through technological enforcement. When the penalty is a simple fine that can never be prosecuted as a crime, many of the legal issues quickly dissipate.

Recommendation 7: Take some test runs

Finally, as projects are developed, each state with its own twist, it is best to use states as laboratories to figure out what survives legal challenges and meets public acceptance. Federal legislation, such as the GDL provisions in STAND-UP, is more likely to succeed after being able to analyze similar laws from the 49 states that already have them. The different approaches used will provide useful comparisons for developers and legislators alike, and the result will be a greater likelihood of success when a federal attempt at instituting a technology is made.

Chapter 1: Introduction

Continuing developments in the fields of transportation technology and privacy law present an abundance of opportunities for unpleasant head-to-head collisions. Without knowledge of the legal framework that applies to emerging technology, Intelligent Transportation System (ITS) developers set themselves up for frustration as ideas that appear flawless in an engineering office may cause conflict when they reach the implementation stage. From the legal perspective, advocates of comprehensive privacy law struggle to update existing law at a pace that keeps up with innovative advancements in technology. Privacy issues related to electronic communications are of primary concern for transportation organizations. (1)

This paper will review several cases where implementation of transportation technologies has raised civil liberties arguments, examining them from legal and political perspectives. The understanding of privacy both as a political concept and a legal protection provides the foundation for future ITS progress, allowing new technologies to be developed in ways that can withstand these types of challenges or avoid them altogether.

Developers of future ITS projects will benefit by taking these political and legal principles into consideration every step of the way, from initial concept through implementation. The cases we will review to illustrate this point are: from before ITS, Seat Belt Ignition Interlocks; and then a number of ITS projects, Automated enforcement, Vehicle miles traveled (VMT) taxes and electronic tolling systems, and electronic enforcement of graduated drivers licenses (GDL). Some of these are updates to existing programs and some are entirely new, but all have the potential to raise significant questions regarding locational privacy. Devices designed to collect tolls electronically, especially for VMT taxes have many privacy implications that merit consideration before implementing. Automated enforcement provides a way to review the privacy policies and practices related to an existing technology. Finally, electronic enforcement of GDL provisions allows examination of driver monitoring technology that is currently used in the private sector on a voluntary basis, but would create much more serious privacy concerns if a government entity were to mandate implementation for all novice drivers.

Chapter 2: Privacy Law and ITS

Current Law: An Imperfect, Unclear Guide

Unlike the European Union or other countries developing Intelligent Transportation Systems (ITS), the United States does not have comprehensive law that protects a person's "right to privacy." Instead, an expectation of privacy has primarily been developed through judicial decisions, although there is piecemeal legislation at both the state and federal levels. (2) In the context of transportation, U.S. privacy law has largely evolved in criminal circumstances, articulating the search and seizure protections of the Fourth Amendment as applied to traffic stops. The protections one expects when pulled over by a police officer include standards for arresting a person as well as for searching one's person or vehicle.

The basic rule for whether a person has a reasonable expectation of privacy under the Fourth Amendment was defined in a 1967 U.S. Supreme Court case, *Katz v. United States*. (3) A reasonable expectation of privacy exists when both prongs of the following test are satisfied:

1. A person has an expectation of privacy, and
2. Society deems the expectation to be reasonable.

Clarifying this issue as applied to transportation, the Court stated 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." (4) Even though the location of a vehicle on the open road is not private, in *Gant v. Arizona*, the Court limited the rule that police could search the passenger compartment of a vehicle as a contemporaneous incident of a recent occupant's lawful arrest by finding a reasonable expectation of privacy in the contents of a vehicle under certain circumstances. (5) An expectation of privacy in vehicles was also established in *Indianapolis v. Edmund*, a case where a roadblock was set up to search every vehicle traveling along a certain route for potential evidence of drug running. (6) The Court described this as a mass surveillance system, which did not meet the second prong of the Katz test.

A further wrinkle is added when technology is involved. Current law limits the observational abilities of the officer to that of the average citizen. That is, anything the officer could observe in person, or aided solely by technology that is available to a member of the general public, would be admissible in a criminal prosecution. Evidence obtained through use of technology to further enhance these abilities, however, would not be allowed unless a warrant had been obtained in advance. (7)

These two lines of reasoning then collide in the context of the data collected by transportation technologies, such as ITS. The United States Department of Transportation (USDOT) explicitly states that "ITS improves transportation safety and mobility and enhances American productivity through the integration of advanced communications technologies into the transportation infrastructure and in vehicles."(8) These technologies rely upon the use of data collected "through a broad range of wireless and wire line communications-based information and electronics technologies" (8) to enable applications that provide data regarding vehicle and

highway operations, collect tolls, and even aid in enforcement of red lights and speed limits across an entire transportation system. Some of the tools used to collect this data (e.g. toll transponder readers) are not generally available to the public. Consequently, one might expect some limitation on who can use this data, and how it may be used. (9)

However, a number of other court rulings and opinions have found that data collected by ITS and similar technologies is public data accessible through some state Freedom of Information Act (FOIA) laws. As a result, it is not entirely clear whether departments of transportation, ITS service providers, and others are entitled to have access to this information, and to what extent people in their vehicles have any expectation of privacy in the data created and collected by ITS technologies. [1] (10)

Complicating the issue further is a statement by the Supreme Court that, in the context of technology, the "societal expectation" prong of the Katz test is nearly unworkable, as technology is advancing so rapidly that it is almost impossible to determine its corresponding societal expectation. In a 2010 case, *City of Ontario vs. Quon*, the Supreme Court stated that "the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior." (11)

Chapter 3: ITS and Privacy "Tools"

To aid ITS developers and other interested parties understand how they need to handle the personal information that could be collected, we have developed an ITS and Privacy Toolbox and Taxonomy, which are attached as Appendices 1 and 2, in an attempt to explain the level of restrictions that correspond with different kinds of information being collected. (12) These tools can be summarized as follows:

The "Best" Option: Use Anonymous Information Whenever Possible

ITS information is likely to fall within a spectrum of anonymity as opposed to falling into a strict category of being anonymous or personally identifiable. The more anonymous the information, the less likely the application will encounter legal restrictions that will dictate how that information is collected and used. When the information collected identifies specific vehicle or personally identifiable information, legal issues regarding consent, access, ownership and protection of information are triggered.

The choice by ITS developers and planners of whether to use personally identifiable information is an important one. Generally, personally identifiable information is defined as data or combination of data that carries the potential of being used to identify a single individual. Examples of personally identifiable information include: full name; telephone number; street address; email address; email password; vehicle registration plate number; driver's license number; credit card numbers and one's digital identity. On the contrary, anonymous information carries no indicators of its origin and cannot be tied back to a specific individual or vehicle. Examples of anonymous information would include information collected by traffic counters or devices that detect the presences of vehicles in order to control traffic flows without identifying the vehicle or its owner In these cases, locational information is collected but without information that can identify an individual.

Collecting and utilizing personal information invites legal restrictions aimed at making sure the information is not misused or inappropriately collected or accessed. 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, it sometimes appears to be more expeditious to collect personally identifiable information if these consequences are not considered. Examples of this include toll transponders that are directly linked to an account holder's credit card, instead of offering pre-paid transponders that could be purchased with cash. In other cases, such as law enforcement, identifying information is needed. In those cases, however, certain requirements must be met, as discussed below.

When Identifying Information Is Needed: Obtain Consent

In the cases where ITS technologies require the collection of personally identifiable information, the issue of consent comes to the forefront. (13) Privacy laws throughout the United States often require consent from an individual before personally identifiable information about them is collected and stored. Government agencies and companies looking to utilize personally identifiable information through ITS technologies must choose between two ways in which

consent from drivers can be garnered. Voluntary consent (or Opt-In) is one way in which consent can be given. Voluntary consent requires individuals to manifest willingness to have their personal information collected. Besides being willing participants in the ITS programs, drivers' consent must be informed of some specific aspects about the information being collected in order for consent to be complete. Examples of information that needs to be conveyed to the willing participants include: what information is being collected about them; how the information will be used; the legal consequences for giving consent; the protections that will be put in place over the collected information; how false information can be corrected; and how long the information will be kept. When drivers voluntarily opt in to ITS programs, liability over ITS information practices can be waived and limited, freeing ITS managers to use the personal information towards ITS goals without fear of legal liability.

The other option is to imply consent (Opt-Out). Local and state statutes can define consent as legally implied by a driver's use of transportation in ways which employ ITS technologies. Currently, driving on roadways is often viewed as a legal privilege in the United States, where drivers statutorily consent to state actions such as field sobriety tests merely by obtaining a license. (14) 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 sufficient when the state interests' in preventing injury, property damage, and loss of life on roadways are served by the practice. However presumed or implied consent usually must allow for individuals to opt-out of such programs and requires that members of the public be made reasonably aware of what they are tacitly consenting to. (15)

Who Uses The Information: Public or Private Actors?

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

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

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

Toolbox in Application: A Taxonomy

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

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

The resulting taxonomy considers the method of observation (i.e. the type of data collected, and how it is collected by ITS systems), the purpose of the technologies and the resulting privacy expectations (See Appendix II).

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 data is needed by the potential application, and how that data could be collected to complete their goals. Next, the purpose for using this data needs to be fully articulated. After the method and purpose 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.

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

The next level of observation by ITS technologies occurs when vehicles are independently and anonymously observed. These types of ITS technologies are usually geared towards system management, such as a loop detector that regulates intersection use through traffic signal controls. Though these technologies are identifying the presences of an individual vehicle, they do 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 rather than traffic as a whole. Examples of such technologies would 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 licenses plate number, transponder code or customer account. These numbers can inevitably be traced back to the specific vehicle through the vehicle registration system, which leads directly to the identity of the vehicle's owner as well. With this much personally identifiable information available, privacy expectation and legal restrictions begin to apply. The administrative purpose of the data collection will mitigate some legal restrictions as the information is being collected from observed public behaviors and being used for the public good. However, restrictions on secondary use of personal information would still apply.

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

Finally, the highest level of legal restrictions and privacy expectations exist where ITS technologies purposefully collect information that directly identifies an individual. 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 either be for criminal or civil purposes; however, the strictest privacy restrictions are triggered when the information is collected for criminal regulatory purposes.

The basic rule is, the more personal the nature of the information that is collected, the greater the number of privacy considerations exist. The proposed purpose for collecting personal

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

Chapter 4: Lessons from the Past

Seat Belt Ignition Interlock

Beyond the legal restrictions, however, ITS technologies can face privacy challenges at the policy and political levels. An examination of the history of the seatbelt ignition interlock of 1974 is instructive as to these issues, as it contains lessons about effective design and implementation.

Occupant Crash Protection

Following the Motor Vehicle Safety Act of 1966, the National Highway Traffic Safety Administration (NHTSA) assigned high priority to occupant crash protection in automobiles throughout the 1970s, ten years before the first state seat belt laws were enacted. The use of various seat belt reminder systems, the ignition interlock, and air bags were the primary technologies implemented for restraint purposes during this time. While the three approaches each had complaints and legal issues to deal with, the development and almost immediate withdrawal of the ignition interlock stood out as a rare case of congressional response to consumer outcry in the name of civil liberties.

Initially, the use of ignition interlocks was not contemplated. What began in 1967 as a requirement for the installation of seat belts in new vehicles under the authority of the Motor Vehicle Safety Act of 1966 turned into a source of NHTSA frustration at the low rate of seat belt usage. (16) NHTSA explored passive-restraint options, deeming air bags as the system of choice in 1971. After announcing a plan for air bags to be installed on all vehicles by 1973, however, the auto industry felt they needed additional time to comply with the new requirements. In February 1972, NHTSA issued a modification of Standard No. 208 that allowed for manufacturers to equip vehicles with an ignition interlock device, which would prevent the engine of a vehicle from starting unless occupants in both front outboard seating positions had their seat belts fastened, instead of passive restraints. (17) This amendment permitted the ignition interlock to serve as an interim measure, but was modified further to require all vehicles made in 1974 to have the interlock, effective August 15, 1973. (18)

Legal Issues Presented

As a mandatory passive restraint, the seat belt ignition interlock requirement did not present direct legal problems. Since the new rules only affected auto manufacturers themselves, there was no legally required action by individual automobile users. While they could face the prospect of their car not operating, users faced no criminal sanction for choosing to not wear their seatbelts. And with no criminal sanction, there was no need to monitor their actions or collect any other information about the user. The practical downfall of this scheme, however, was that, because there were no laws addressing use of the interlock by consumers, it was permissible for individuals to disable the interlocks – indeed, car manuals such as the 1974 Bentley even contained the schematics of how to do so. One-third of new car owners removed the interlock device, according to a survey conducted by the Ford Motor Company in April 1974. (16)

Political Issues Presented

Not only did the public dismantle the devices, people also let their representatives in Congress know that the government was intruding on their lives. Public resistance was so overwhelmingly negative that Congress amended the Motor Vehicle Safety Act. (19) On October 27, 1974, President Gerald Ford signed into law a bill that prohibited any federal motor vehicle safety standard from requiring or permitting as means of compliance any seat belt interlock system.

This case provides a couple practical lessons for ITS developers. First, gaining public acceptance is as important as passing legal scrutiny for seemingly intrusive technologies. NHTSA had not looked outside of its boundaries to determine whether there was a sufficient public call for increased vehicle safety to the point that people would change their behavior. Certainly, the data existed to show people were dying on the roads, and that seat belts and airbags could prevent many of those deaths. However, the public had not been convinced that making everyone wear a seat belt every time they started their car was a reasonable price for possibly saving a life in an accident that likely would not occur on that particular trip. Vogel refers to these types of regulations as those that are perceived by the public as protecting them only from themselves. (16) Without sufficient education that such protection is needed, the regulation will likely not survive public scrutiny, even if it does survive legal scrutiny.

As discussed above, the ability to opt in to a program relieves many legal concerns, and providing alternatives can address political concerns as well. While it is interesting that enforcement of seat belt laws can also raise political objections in the form of privacy “rights” being violated, the legislative history shows that the public is more accepting of a regime where they still control the decision – and bear the risk – of deciding whether to fasten their seat belt. For example, the beeping reminder system still used today, while less effective, has become accepted as the user still has the power to choose.

Automated Enforcement

The idea of enforcing traffic laws with cameras is almost as old as the automobile itself. Since states began deploying speed cameras in the late 1980s, the field of automated enforcement has changed rapidly in response to advancements in technology, changing legal requirements, and public demand.

A 1905 English patent for time-recording cameras proposes the following, "to trap motorists, the over-speedy car is photographed by an officer with a time-camera at each end of a pre-determined stretch of boulevard and on the difference in the recorded time and the distance traversed the speed is determined, while the occupants of the car may be identified by photograph, also." (20) Called the "time trap for scorchers" by the New York Times, the camera was declared a mechanical method of noting speeds, "the results of which are absolutely beyond question."(21) While technological developments have increased the sophistication of this design, it is likely that the motivation for this invention – to combat reckless driving, "one of the evils of the age" – has not changed much. (21) The lack of publicity in the years following the announcement of the time-recording camera suggests that it was never put into use. Whether this was due to public reaction similar to those experienced by modern-day officials is not known,

but this report will look at both the legal and political issues faced by automated enforcement technology.

The first photo radar was developed by a rally car driver wanting to improve his time around the race track. In 1958, Maurice Gastonides and his company, Gastometer, introduced the first reliable speed-measuring device. (22) Seven years later, Gastometer presented its red light camera. (22) While it was roughly 30 years before the implementation of speed and red light camera programs took place in American cities, the development of advancing technologies have since begun providing for the automated enforcement of many traffic laws, including the regulation of railroad crossings, bus lanes usage, and parking violations. Speeding and red light violations will be the focus here because they are the primary applications of automated traffic enforcement, having faced the most significant challenges presented both in court and in the court of public opinion.

Function

The terms "speed camera" and "red light camera" will be used generically to describe a broad group of automated systems that enforce the two infractions for which they are named. Speed cameras, or photo radar systems, detect speeders using either radar or laser in conjunction with one or two cameras that capture images to identify violators without law enforcement officers operating the equipment. Red light cameras capture images of vehicles and/or their drivers proceeding through red lights with the help of loop detectors buried in the pavement. Because the laws for the use of automated traffic enforcement vary from state to state, as discussed below, the design of traffic cameras differ accordingly.

Purpose

Safety is the ultimate selling point for the installation of traffic cameras. Many state and local governments' justification of camera programs rests on an aim to reduce the fatalities, injuries, and huge economic costs associated with traffic accidents caused by running red lights and speeding. Along with reducing the number of traffic accidents, other benefits of automated enforcement include freeing up time for police officers to focus on more important police work, making it possible to patrol intersections and stretches of road where traffic stops are dangerous, and reducing the danger to police officers who themselves might have to run a red light or speed to catch up with the offender. Specific safety issues, such as speed limits in school zones and construction zones, are often the targets of automated enforcement. Others argue that citing safety issues is just a guise for ulterior motives for automated enforcement, such as a "non tax increase revenue generation," as it was called in Arizona, or a conspiracy between the government and private contractors who provide and maintain the equipment. (23)

Paradise Valley, Arizona, along with other municipalities in Texas, Arizona, and California are credited with implementing the first speed camera programs in 1987. Today, Arizona and California both have significant state-wide programs, while Texas no longer allows for the automated enforcement of speeding.

An accident in which a toddler's stroller was dragged 13 blocks by a car that ran a red light served as the catalyst for developing a red light camera program in New York City. (24) It

wasn't until 1993 – ten years after the incident – that the program came into fruition, making it the first of its kind in the United States. A year later, after a similarly terrifying incident in which 13 pedestrians were injured by a red light runner in San Francisco, the Bay Area saw its first pilot program for red light enforcement. (25)

Legal Issues Presented

The most common uses of traffic cameras are for enforcing the speed limit and catching red light violators while deterring future violations, although cameras have been deployed to monitor areas such as railroad crossings and bus lanes as well. Since the late 1980s, penalties both criminal and civil have been imposed in many states with mixed results. The National Committee on Uniform Traffic Laws and Ordinances (NCUTLO) developed a model law for automated enforcement, but there continues to be instances where public backlash results in the removal of traffic cameras even when those guidelines are met. [2] (26)

Enacting legislation to permit automated enforcement is left up to individual states, because the federal government does not typically regulate traffic laws. Each state has set up its own structure for the types of automated enforcement allowed within it, creating a wide range of possible uses. Here are some examples of the variations from one extreme to the other in several jurisdictions:

- West Virginia prohibits all photo enforcement. (27)
- Wisconsin prohibits the use of photo radar.(28)
- New York allows red light cameras in large cities and specifies how many intersections may be monitored daily.(29)
- Washington allows speed cameras in school zones and red light cameras at arterial intersections.(30)
- Arizona allows statewide use of traffic cameras for both speeding and red light running. (31)
- The District of Columbia allows automated enforcement for all moving infractions. (32)
- California allows red light photo enforcement statewide, issuing a traditional citation.(33)

Approximately 20 states, including Minnesota, have no law regarding automated enforcement.

Legal challenges to automated enforcement have been frequent, presenting constitutional questions such as confrontation clause and due process issues in criminal cases and conflict of interest or machine malfunction complaints in civil cases. In 2005, within a year of its inception, the Minneapolis Police Department's "Stop on Red" PhotoCop program was shut down when the Minnesota Supreme Court ruled it conflicts with a state law imposing uniformity of traffic laws across the state. The program issued petty misdemeanor violations, which also exposed the program to legal challenges because of the combination of a reduced burden of proof for the state and the potential of vicarious criminal liability.[3] While laws nationwide are often modified as a result of litigation, political pressure has also forced programs to change or even be withdrawn completely. The random placement of cameras on the open road often leads to protests of

government surveillance citing privacy infringements, but more substantial claims are based on frustration with malfunctioning machines, a lack of awareness of how ticketing works, and the use of automated enforcement as a revenue raiser for both states and the companies that maintain the equipment.

Political Issues

While this means of enforcement appears quite efficient, it faces its own obstacles that can slow the process. Since their inception, many speed and red light camera programs throughout the United States have consistently been met with opposition. Some of these criticisms are expressed via the legal system in the form of lawsuits against both the government and private entities, asserting the violation of constitutional rights, invalidity of statutes, fraud, and conspiracy. Other negative opinions are expressed at the water cooler, in newspapers, and even through violence towards workers who use the equipment. The loudest criticism thus far, however, has been through the legislative process. Elected officials have responded to their constituencies, making automated enforcement major issues of their platform and also by putting the issues themselves on the ballot. Issues such as these and others drove some citizens to take their opinions to the voting booths. As recently as November 2008, cities in Ohio and Texas voted to remove red-light cameras. (34)

While major problems in automated enforcement have been encountered, many states effectively implement the use of traffic cameras. As suggested by NCUTLO's model law, the most successful programs are based on civil ordinances rather than criminal fines and assign penalties to the vehicle owner instead of the driver. Another important factor in public acceptance is the driving force behind the initiation of cameras in a certain region – programs are welcomed more readily when the motivation was preventing accidents after people were killed by a red-light runner in San Francisco than when the Arizona governor announced traffic cameras were going to fix state budget problems. One concern that cannot be easily addressed, however, is the difficulty of informing drivers of the state-by-state variations in traffic laws.

Emerging Technologies: Electronic Tolling

Joining popular items such as cell phones, DVDs, and digital cameras, it might come as a surprise that electronic tolls were recognized as one of the top 25 life-changing inventions since 1982. As a celebration of its 25th anniversary, the USA Today credits the North Texas Tollway Authority with implementing the first electronic tolling devices in 1989 and turning the process of "throwing quarters into a tollbooth bin" into a thing of the past. (35)

Toll transponders first hit the nation's highways to put the burden of maintaining the road on the users. Hailed as a cost-efficient and time-saving device, toll transponders were warmly welcomed into widespread use and continue to enjoy public acceptance. Since the inception of electronic toll collection in 1989 even drastic modifications to the tolling systems – which vary by state or region and now include open-road tolling in many places – met little resistance. Millions of Americans show their appreciation for an alternative to throwing coins in a bin by purchasing a transponder that gathers information about the movement of their vehicles on a particular stretch of road and bills them accordingly. This acceptance has been one argument for consideration of replacing the gasoline tax with a fee charged per mile driven. With the ability to

know exactly where a car is for the purpose of paying a toll, proponents argue that the concept of "paying for what you use" could be even more tightly bound.

Legal Issues

As shown above, "privacy" is often the buzzword used to create a public uproar over an issue. In this case, however, the data collected creates a legitimate legal privacy concern as it can be used in proving a person's location in both criminal and civil cases. The constitutional protection from unreasonable search and seizure applies if location information is be used as evidence against a criminal defendant, requiring a warrant or probable cause to retrieve the information. Subpoenas, as well as federal and state Freedom of Information Acts (FOIA), provide different avenues of access to (and protection of) the data collected. While information may be available, some jurisdictions' toll authorities have restricted FOIA reach from extending to vehicle travel history information on the basis of an unwarranted intrusion of privacy. On a much lesser scale than data collection matters, the possibility of tracking vehicles by third-party roadside RFID readers also raises privacy concerns.

This case study varies significantly from the two previous for the simple reason that it does not affect the population generally. As discussed above, by opting in to the technology, the expectation of privacy is diminished significantly. There is an argument to be made that the necessity of using toll transponders is almost so great as to make it impossible to survive without one. Even so, no person is compelled to use the highway: they could use the back roads or a cash-only option could be made available. However, opponents might still argue that this is not a viable option due to the time penalties that could result from alternative routes not being as direct or back-ups caused by the requirement to stop and pay cash tolls.

Political Issues

It may seem ironic that the technology with the greatest potential for violating a person's right to privacy is also the most widely accepted. Significant safeguards – most notably the provision of alternatives that create an opt-in environment – make this acceptance possible. Presenting a technology as one of several options reduces the political expectation of privacy associated with it. Alternatives of either paying cash or taking another route are always available, making participation in electronic toll collection completely voluntary. The association of a toll transponder to a vehicle or vehicles instead of a person, creating some anonymity, is a secondary protection in regard to legal privacy; travel history details only provide information about the location of the transponder, not about a specific individual. The potential vehicle-tracking problem is relatively insignificant, as it can largely be eliminated in the transponder design process. (36)

Having dealt with the possible legal issues, it is equally important to emphasize that this technology wins on the political side of the scale as well: the transponders are easily accessible and user advantages are incredibly high. Electronic toll collection saves users both time and money while making travel more convenient, providing benefits to the daily commuter and weary traveler alike.

Graduated Drivers License Enforcement

Vehicle crashes claimed about 3,500 lives of 15- to 19-year-olds in 2008. (37) In the same year, over 350,000 of that age group suffered injuries in motor vehicle crashes that resulted in emergency room treatment. (37) From April 23 to 26, 2010, three separate traffic accidents involving teen drivers left eight Minnesotan teenagers dead. (38) While it may be unusual for so many fatalities to occur during one weekend, vehicle crashes are the leading cause of death among young adults. (39) With the exception of North Dakota, all states have three-phase programs of graduated drivers licensing in an attempt to curb these sobering statistics. (40)

These laws cover many areas of driving, but generally focus on phasing in responsibility through a teen driving permit, and include categories such as limits on the number of teen passengers in the vehicle, restrictions on nighttime driving, and harsher punishments for infractions like texting while driving. In 2010, New Jersey became the first state to require a special decal on their license plates. (41) Along with the development of state laws, members of Congress are pushing federal legislation called the Safe Teen and Novice Driver Uniform Protection (STAND UP) Act. (42) STAND UP would establish a three-stage process before novice drivers could attain an unrestricted drivers license, including prohibitions against nighttime driving and non-emergency usage of cell phones in the first two stages. The legislation would create uniformity in an area of law that varies widely from state to state.

Devices such as the Intelligent Transportation Systems Institute at the University of Minnesota's Teen Driver Support System (TDSS) are being developed to monitor a teen's driving behavior in relation to known risk factors and GDL provisions. (43) The system requires a teen's smartphone to be plugged into the car, which disables calling and texting functions while the teen is driving, and provides feedback to both the teen driver and the driver's parents. The risk factors to be monitored are programmed into the cell phone and can be based on specific driving habits, local traffic laws, and/or GDL laws. Teens will receive almost immediate feedback when their driving behavior is not in compliance with set expectations, and will have the opportunity to respond to a warning before a notification is sent to their parents. Some of the risk factors include unsafe driving behaviors, like hard braking or cornering, as well as violations of traffic laws, such as stop sign violations and failure to wear a seat belt. GDL provisions such as curfew and the presence of unauthorized passengers can also be supervised.

Parents can override the TDSS when they are present in the vehicle with their teen driver. In an example of how ITS technologies can be modified to accomplish similar ends with less invasive data, the designers of this technology originally used a biometric fingerprint reader "to enroll, capture, and identify the driver and parent/supervisor's fingerprint." (44) While an effective method for distinguishing who was driving, and thus shutting the system off when the teen was not driving, it still created information as to when the adult was driving. Since then, researchers have noted that the fingerprint reader could be dropped in favor of using a key fob or similar technology that does not identify the person disabling the system. (45)

Research shows that teens find the Teen Driver Support System implies distrust of teens and restricts their freedom, but also that they felt limiting the number of passengers, the volume of the radio, and nighttime driving hours would reduce the number of teen traffic crashes. (46)

When informed about the new system, a 17-year-old Minnesotan showed resistance to the idea: "It's an invasion of privacy," said Tyler Elms. (47) The extent to which this right of privacy exists in either its legal or political forms should be a primary concern as implementation of this technology moves forward.

Legal Issues

As shown in the toolbox and taxonomy, the first step in addressing legal privacy issues is to examine whether the information is personally identifiable. The purpose of the TDSS is to provide an opportunity for parents to know how their teen is driving when they are not with them, through automatically generated reports of driving behavior transmitted via smartphone. As the system is designed to only engage when the teen is driving, the parent should have little doubt as to who was driving the vehicle at the time of the report. The fingerprint reader provided the most accurate data regarding the driver, as it generates data specifically identifying the driver. The key fob or similar technology is not as accurate, creating the possibility that the teen could allow a friend to get behind the wheel, or that the parent could even provide the fob to the teen, thus allowing them to operate the car with the system disengaged. Since the nature of cell phones includes providing cell tower site location information, both historical and real-time, the use of a smartphone that is registered to an account in the teen driver's name creates access to the location of the teen driver at all times, sufficient identifying data that the system cannot be considered to provide "anonymous" data. The tool box then suggests we consider whether participation is voluntary – opt-in – or mandatory.

Some drivers currently use driver-monitoring devices voluntarily to reduce the rate of their car insurance. This opt-in arrangement creates relatively little legal scrutiny. The use of the key fob, as discussed above, even creates the opportunity for the parents and teens to opt in on a trip-by-trip basis. However, over time, this kind of flexibility may be problematic. First, if usage of such devices increases over time, it is possible that so many people choose to use a GDL-monitoring device that it becomes de facto mandatory due to exclusive demand for the benefits of this product. On the other hand, if most users take the opt-in provision to its furthest limit, only the lowest risk teens and lowest risk trips would use the system, defeating the purpose of identifying and providing the opportunity to correct dangerous behaviors. Consequently, it is reasonable to consider the legal privacy effects of Congress or a state requiring GDL-monitoring in order to insure teen drivers: a teenager's first driver's license would require use of equipment such as the TDSS.[4] In this situation, it is likely that the data would not be available just to the drivers' parents, but that the state would claim an interest in information regarding traffic and/or GDL violations to the state, and that failing to use the equipment would be an offense in itself. When consent is presumed by statute, an opt-out provision or other provisions for protecting identifying data would be necessary to avoid intensive judicial scrutiny and the highest level of legal liability.

Limiting the use of information gathered provides some opportunities for controlling the level of privacy expectations as well. If the information sharing takes place between teen driver and a parent, there is not an immediate concern. In the best situation, the teen and/or the parent choose the insurance company they want to use, and provide consent for the information to be collected within a state-mandated regulatory structure. Even if the teen does not consent, the parents may have the power to consent on behalf of the teen.[5] A problem lies, however, in the potential that

the insurance company could release or sell that information, or that it could be summoned by subpoena or warrant. The other private actor in this situation is the cellular service provider. As noted above, cell phones provide cell tower site location information, both historical and real-time, thus creating data regarding the location of the teen driver at all times. Another concern is that the content of the reported violations could be accessed through that same service provider. Again, the greatest concern with the use of information would be with a GDL-monitoring mandate. To pass legal muster, statutory limitations would need to be in place to remove the possibility of criminal liability through this technology.

The opportunity to attach the phone to the car rather than the driver could provide a way to significantly reduce the privacy concerns raised with GDL-monitoring devices. If the cell phone in the TDSS were registered to the car itself the driving behavior of a certain vehicle would be reported. To make this work the owner of the car would have to be held liable. In this way the devices would not specifically identify the driver; by removing that connection the data would pose much less concern on the spectrum of anonymity.

Taking into consideration the type of information gathered, the nature of the consent, and the potential usage of the information, a GDL-monitoring device like the TDSS would fall into a medium to high level of privacy expectation and legal protection in the taxonomy. Legally speaking, the vicarious liability option would most effectively reduce the privacy concerns, taking away the potential for individual behaviors to be reported to anyone, particularly the government. When the system collects personally identifying information, however, the privacy protections increase greatly. As discussed above, reporting information to a teenager's parents does not create very much of a problem.

Reporting the data is not the most serious problem however. Rather, the problem is in the creation of the data itself, and controlling who will have further access to it. As soon as personally identifiable information about violations is created, the data cannot be fully protected from third parties or the state. Without legislation providing otherwise, the third-party risks of disseminating data will be present with private actors, and a warrant can access the information, provided a probable cause standard is met. The highest legal protections, as stated earlier, would be come into play if Congress were to mandate the use of a GDL-monitoring system. Imposing "surveillance" of this sort, coupled with the possibility of reporting violations to the state, would likely fail to meet even the most restrictive definitions of what data can be protected. Privacy problems of a political nature would be created to the extent that they become legal problems.

Thus while the 17-year-old Elms quoted earlier may be disappointed to know that it is legally possible for the government to "invade his privacy," his sentiment likely rings true with enough people to create a political privacy issue. The good news for ITS developers, however, is that this seemingly intrusive device has potential to gain public acceptance. To begin with, GDL-monitoring affects a limited percentage – not to mention a non-voting percentage – of the population. In addition, there is a great public safety interest in protecting other drivers from these novices and, quite frankly, teens from themselves. Although the teen drivers may reject the notion of being babysat as they receive their first taste of freedom on the open road, it is possible for their parents – and the rest of the voting public – to be won over when faced with the bleak

statistics associated with teenage driving and the gory details of vehicle crash fatalities. The privacy concerns here are great, but are not insurmountable.

Chapter 5: Conclusions and Recommendations

In light of these findings, ITS planners and developers should take steps toward reconciling the legal and political privacy issues presented from the beginning of the design phase of a project through its implementation. The Toolbox (App. A) and Taxonomy (App. B) serve as guides for navigating the legal questions, but, as one addresses the points raised there, it is just as important to consider the policy impacts of those decisions and the effect(s) on current public perception.

Recommendation 1: Public perception is as important as legal reality.

Gaining public acceptance is as essential as passing legal scrutiny for seemingly intrusive technologies. Because the avoidance of legal obstacles does not guarantee favor with the general public, it is necessary to gain public trust.

Recommendation 2: The problems with personally identifiable information start with collecting it.

The first step is determining the type of information that needs to be collected as it falls along a spectrum from anonymous to personally-identifiable information. Anonymity is always preferred, but is not often seen as a realistic expectation. Anonymous solutions for upcoming technologies should be sought after, such as using a digital cash option for payment instead of collecting credit card information. When a situation does not allow for total anonymity, steps should be taken to reduce the amount of information collected. (Security of information is important as well, but is a separate issue from privacy). Perhaps the most important concept to note is that one must consider *all* of the possible uses of any personally-identifiable information, regardless of the intended use of that information gathered. For instance, if cell phone technology is used in an ITS project, planners need to remember that cell phone signals are traceable through cell tower site location information and that a vehicle's location can thus be determined either from phone records or through real-time tracking.

Recommendation 3: Alternatives increase public acceptance.

Although the public perception problem may exist in a situation, it is possible to mitigate the political damage it could cause through presenting the technology as one of several options. By providing alternatives, people who opt in to use of the technology are giving up their information willingly, drastically reducing the potential for legal complaints and creating a positive political response by exercising choice.

Providing the opportunity for individuals to choose to use an ITS technology results in higher acceptance of that technology. Also, when given a choice of whether to use a technology, citizens are less likely to attempt to circumvent the devices on their own.

Recommendation 4: Get the public on the same page.

In order to give up this information willingly, however, the opt-in choice must be informed. Informed consent demands clarity, trust, and transparency from the agency disseminating the information.

Distributing information on the effectiveness and reliability of a technology, as well as how the resulting data can and will be used, is a necessary step in implementing new technology. Not only does understanding allow people to feel more comfortable with the technology, it also lays the foundation for informed consent necessary to meet legal standards.

Recommendation 5: Context – Introduce technologies at the right place, right time.

It is easier to introduce new devices at a time when a specific incident encourages people to demand a government solution to an ongoing problem. Presentation of the issues within that context shows a practical application of the technology and positively affects acceptance.

Recommendation 6: Violations observed by technology should not create criminal consequences.

When alternatives are not available – essentially when there is a mandate for use of a new technology – the most effective way of dealing with the highest levels of scrutiny include securing legislation that supports the program well before implementation. If there can be any sort of criminal implication whatsoever, vicarious liability in the form of reporting a particular car and not a specific driver, is a viable solution.

Imposing civil penalties with the help of advancing technology creates far fewer hurdles than creating criminal liability through technological enforcement. When the penalty is a simple fine that can never be prosecuted as a crime, many of the legal issues quickly dissipate.

Recommendation 7: Take some test runs.

Finally, as projects are developed, each state with its own twist, it is best to use states as laboratories to figure out what survives legal challenges and meets public acceptance. Federal legislation, such as the GDL provisions in STAND-UP, is more likely to succeed after being able to analyze similar laws from the 49 states that already have them. The different approaches used will provide useful comparisons for developers and legislators alike, and the result will be a greater likelihood of success when a federal attempt at instituting a technology is made.

References

1. 2008 Field Visit Program, *TR News*, January-February 2009, p. 6. This issue received increased attention in the Spring of 2011, with U.S. Senate hearings and the introduction of S. 1223, "Location Privacy Protection Act of 2011."
2. The Electronic Communications Privacy Act of 1986 (18 U.S.C. §2510); Driver's Privacy Protection Act (18 U.S.C. §2721). See the Massachusetts Data Privacy Act (201 CMR 17) for an example of privacy legislation on the state level.
3. *Katz v. United States*, 389 U.S. 347 (1967).
4. *United States v. Knotts*, 460 U.S. 276 (1983).
5. *Gant v. Arizona*, 129 S.Ct. 1710 (2009).
6. *Indianapolis v. Edmund*, 532 U.S. 32 (2000).
7. *Kyllo v. United S*tates, 533 U.S. 27 (2001). (This ruling could be distinguished in the context of transportation, as the *Kyllo* concerned the search of a home.).
8. U.S. Department of Transportation, Research and Innovative Technology Administration (RITA), *ITS List of FAQ's*, http://www.its.dot.gov/faqs.htm (last accessed July 6, 2011).
9. *U.S. v. Maynard,* 615 F.3d 544 (D.C. Cir., 2010), stating that use of a GPS unit to track a person's location over the course of an entire month violates a person's expectation of privacy as "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."
10. Illinois Tollway Response Letter, September 3, 2010, available at http://www.illinoistollway.com/pls/portal/docs/PAGE/TW_CONTENT_REPOSITORY/TW_CR_FOIA/10-126%20RESPONSE%20%282%29.PDF (last accessed October 1, 2010).
11. *Ontario v. Quon*, No. 08-1332, 529 F. 3d 892 (2010).
12. F. Douma and J. Deckenbach, "The Challenge of ITS for the Law of Privacy," *Journal of Law, Technology, & Policy*, 295, 330-331 (2009).
13. C. Cottrill, "Protecting Location Privacy: A Policy Evaluation," as presented at the Annual Meeting of the Transportation Research Board, Washington, D.C., Jan. 2011.
14. See, e.g., Or. Rev. Stat. § 813.135.
15. U.S. Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Internet Policy Task Force Green Paper,* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf (last accessed July 7, 2011).
16. D. Vogel, "When Consumers Oppose Consumer Protection: The Politics of Regulatory Backlash," *Journal of Public Policy*, 10(4), 449, (1990).
17. Federal Register 37 FR 3911. See also, 15 U.S.C. 1410(b).

18. L. Robertson, *Safety Belt Use in Automobiles with Starter-Interlock and Buzzer-Light Reminder Systems*, http://ajph.aphapublications.org/cgi/reprint/65/12/1319.pdf (last accessed July 7, 2011).

19. Federal Register 39 FR 10272, March 19, 1974.

20. "Time Recording Camera for Trapping Motorists," *Popular Mechanics*, VII(9), 926 (1905), available at http://books.google.com/books?id=Dt4DAAAAMBAJ&pg=PA926&hl=en#v=onepage&q&f=false (last accessed September 23, 2011).

21. "Time Trap for Scorchers," *The New York Times*, (Aug. 6, 1905), http://query.nytimes.com/mem/archive-free/pdf?res=F50B15F7385A12738DDDAF0894D0405B858CF1D3 (last accessed February 25, 2011).

22. B.V. Gastometer, "History," B.V. Gastometer Company website, http://www.gatsometer.com/web_en/history (last accessed January 17, 2011).

23. "Arizona Speed Cameras Expect $165 Million Annual Revenue," *TheNewspaper.com: A Journal of the Politics of Driving*, (Jan. 19, 2008), http://www.thenewspaper.com/news/21/2180.asp (last accessed February 25, 2011).

24. The National Campaign to Stop Red Light Running, "Stop on Red = Safe on Green," http://www.stopredlightrunning.com/pdfs/StopOnRedSafeOnGreen.2002.pdf (last accessed February 25, 2011).

25. San Francisco Municipal Transportation Agency, "Can We Make Red Light Runners Stop?" http://www.sfmta.com/cms/venf/14440.html (last accessed January 17, 2011).

26. National Committee on Uniform Traffic Laws and Ordinances, "Automated Traffic Law Enforcement Model Law," http://www.ncutlo.org/autoenforce622.htm (last accessed February 25, 2011).

27. W. Va. Code § 17C-6-7a.

28. WIS. STAT. § 349.02.

29. New York Vehicle & Traffic Law § 1111-a.

30. Washington State Chapter 46.63 RCW.

31. Ar. Rev. Stat. § 28-654.

32. D. C. Code § 40-751.

33. Cal. Veh. Code §§ 210, 21455.5, 21455.6, 40518-40521.

34. See, e.g., City of Cincinnati Charter Amendment, Issue 7: Limits of Photo Monitoring for Traffic Violations. (Amendment passed on November 4, 2008).

35. B. Acohido, J. Hopkins, J. Graham, and M. Kessler, "25 years of 'eureka' moments," *USA Today*, http://www.usatoday.com/news/top25-inventions.htm (last accessed January 17, 2011).

36. D.J. Glancy, "Privacy and Intelligent Transportation Technology," 11 *Santa Clara Computer & High Tech. L. J.* 151 (1995). See e.g., J. Opiloa, "Privacy Matters, *Thinking Highways*, Vol. 5, No. 2 pp 23 – 25.

37. National Highway Traffic Safety Administration, *Fatality Analysis Reporting System*, Washington, DC: U.S. Department of Transportation, National Highway Traffic Safety Administration, National Center for Statistics and Analysis, http://www-fars.nhtsa.dot.gov/Main/index.aspx (last accessed January 17, 2011); Center for Disease Control and Prevention, *Fatality Analysis Reporting System. Centers for Disease Control and Prevention, Teen Drivers: Fact Sheet*, Atlanta, GA: Center for Disease Control and Prevention, http://www.cdc.gov/motorvehiclesafety/teen_drivers/teendrivers_factsheet.html (last accessed January 17, 2011).

38. T. Tolentino, "Deadly Weekend for Teen Drivers," *Fox 21 News*, (Apr. 26, 2010), http://www.fox21online.com/news/deadly-weekend-minnesota-teen-drivers (last accessed January 17, 2011).

39. A.M. Miniño, "Mortality among Teenagers Aged 12-19 Years: United States, 1999-2006," Washington, DC: National Center for Health Statistics, NCHS Data Brief, No. 37 (May 2010), http://www.cdc.gov/nchs/data/databriefs/db37.pdf (last accessed February 25, 2011).

40. Governors Highway Safety Association, "Graduated Driver Licensing Laws," February 2011, http://www.ghsa.org/html/stateinfo/laws/license_laws.html (last accessed February 23, 2011).

41. L. Copeland, "National Standards Sought for Teen Drivers," *USA Today*, http://www.usatoday.com/news/nation/2010-05-03-teen-drivers_N.htm (last accessed January 17, 2011).

42. Teen and Novice Driver Uniform Protection Act (STANDUP), legislation proposed as H.R. 1895 and S. 3269.

43. M. Donath, *Smartphone Based Novice Teenage Driver Support System*, Intelligent Transportation Systems Institute, Center for Transportation, University of Minnesota, http://www.its.umn.edu/Research/ProjectDetail.html?id=2009015 (last accessed February 25, 2011).

44. S. Brovold, N. Ward, M. Donath, and S. Simon, *Developing Driving Support Systems to Mitigate Behavioral Risk Patterns among Teen Drivers*, Center for Transportation Studies, University of Minnesota, http://www.cts.umn.edu/pdf/CTS-07-05.pdf (last accessed 9/29/2010).

45. N. Lerner, J. Jenness, J. Singer, S. Klauer, S. Lee, M. Donath, M. Manser, and N. Ward, *An Exploration of Vehicle-Based Monitoring of Novice Teen Drivers: Final Report*, Report number DOT HS 811 333, Washington, D.C.: U.S. Department of Transportation, National Highway Traffic Safety Administration, http://www.nhtsa.gov/DOT/NHTSA/NVS/Human%20Factors/Reducing%20Unsafe%20Behaviors/%EF%BB%BFDOT%20HS%20811%20333.pdf (last accessed September 29, 2010).

46. M. Manser, M. Rakauskas, and N. Ward, *Generational Perspectives in Teen and Older Drivers on Traffic Safety in Rural and Urban Communities*, Presentation at Stakeholder Breakfast of Toward Zero Deaths (July 8, 2009), http://www.minnesotatzd.org/events/breakfasts/documents/7-8-09-Manser.pdf (last accessed February 25, 2011).

47. D. Nordine, "U Researchers Tackle Teenage Driver Safety," *Minnesota Daily*, http://www.mndaily.com/2010/06/09/u-researchers-tackle-teenage-driver-safety (last accessed February 25, 2011).

Endnotes

[1] These cases include opinions regarding similar use of GPS units from other U.S. Courts of Appeals, a ruling from the Georgia Supreme Court (Devaga v. State of Georgia), and opinions from the Illinois Attorney General stating that photos showing the location of a particular I-Pass account holder on the Illinois Tollway at a particular time is public data.

[2] The guidelines include instruction for times and locations to use automated enforcement, insures revenue generation is not a motive, and imposes only civil fines similar to parking tickets instead of the typical criminal violation when the same offense is observed by a police officer.

[3] Fining a car owner, rather than the car driver, for a red-light violation is generally a legally-acceptable form of vicarious liability. However, in jurisdictions such as Cook County, Illinois, red-light violations are enhanceable, that is to say the severity of punishment increases with multiple violations. At some point the violations become a crime, and the vicarious liability then has criminal consequences. Some states allow vicarious criminal liability, such as Minnesota, where a vehicle owner may face criminal charges when the vehicle passes a school bus with its stop sign extended according to Minn. Stat. § 169.44.

[4] While not mandating tracking devices as discussed here, the "Safe Teen and Novice Driver Uniform Protection Act of 2010," or "STANDUP Act," (S.3269) did call for the creation of a national standard for graduated drivers licenses, thus creating at least a federal floor in an area where states had previously been able to set their own requirements.

[5] In Vernonia School District v. Acton, 132 L.Ed.2d 564, 515 U.S. 646, 115 S.Ct 2386 (S.Ct., 1995), the Supreme Court discussed this point, stating, "Traditionally at common law, and still today, unemancipated minors lack some of the most fundamental rights of self-determination--including even the right of liberty in its narrow sense, i. e., the right to come and go at will. They are subject, even as to their physical freedom, to the control of their parents or guardians. See 59 Am. Jur. 2d, Parent and Child § 10 (1987).

Appendix A: Toolbox for Identifying Privacy Issues

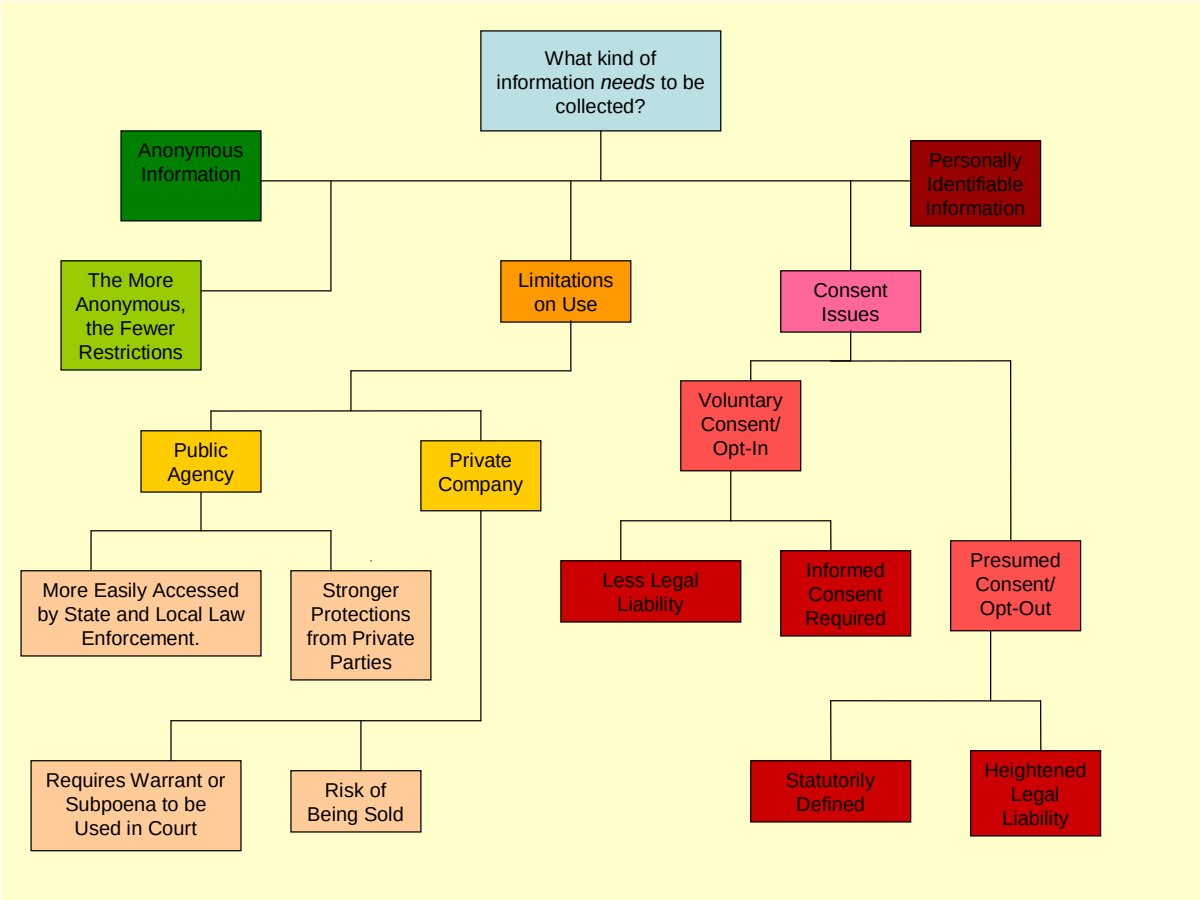

Figure A-1: Toolbox for Identifying Privacy Issues

Appendix B: Taxonomy of Privacy Expectations and Legal Protections

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

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