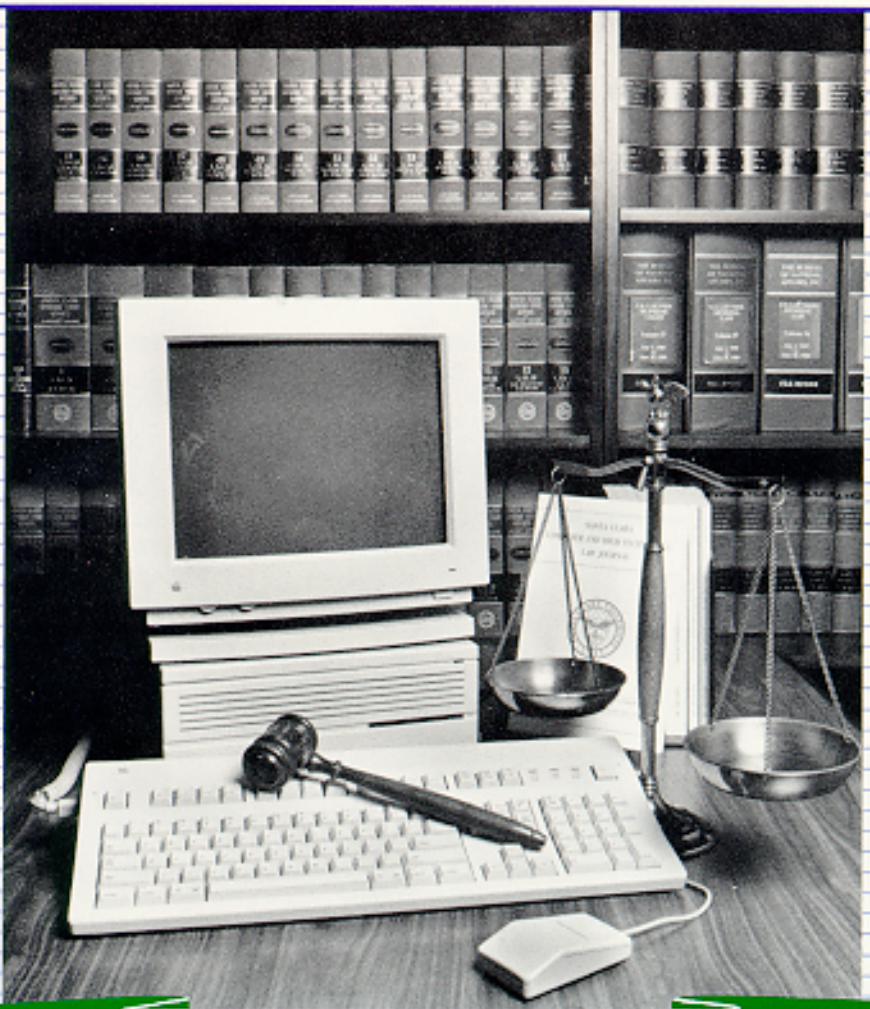
SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL



PRIVACY AND ITS

VOLUME 11, NUMBER 1 MARCH 1995

SANTA CLARA UNIVERSITY• SCHOOL OF LAW

Santa Clara Computer and High Technology Law Journal
March, 1995
Symposium on Privacy and ITS

11 Santa Clara Computer & High Tech. L. J. 151

PRIVACY AND INTELLIGENT TRANSPORTATION TECHNOLOGY

Dorothy J. Glancy*

Since surface transportation moves people and goods along public roads and transit systems, it may seem odd to be concerned about privacy in such a highly public context. And yet, respecting privacy will be important, as advanced technologies improve highways and other surface transportation systems across the American landscape. Without proper respect for privacy, application of advanced transportation technologies to surface transportation could become either a technological road not taken[1] or a veritable web of information which subjugates individuals and trammels personal freedom.[2] Figuring out how to structure transportation applications of advanced computer, communications and other technologies so that the technological infrastructure respects individual privacy will be among the most challenging legal and social issues which confront the new transportation technologies known as Intelligent Transportation Systems, or ITS.[3]

The relationship between privacy and ITS is reciprocal.[4] Privacy will, without doubt, be affected by ITS. But ITS will also be affected by concerns about privacy. This circular relationship between privacy issues and ITS, is complicated by the fact that neither privacy nor ITS is simple or static. This article will explore some of the interesting interactions between privacy and ITS. It will begin by sketching the outlines of ITS technologies and will then consider the nature of privacy concerns about ITS, followed by a discussion of ITS concerns about privacy and privacy laws potentially applicable to ITS. A discussion of some strategies for safeguarding privacy will form the concluding section of this article. Protecting privacy should enhance the effectiveness, as well as the acceptance, of the intelligent transportation systems which will weave together tomorrow's surface transportation infrastructure.

I. The Capacity of ITS Technologies To Affect Privacy

Intelligent transportation technologies have the capacity to affect individual privacy in many ways. Whether ITS is deployed by government agencies, private corporations, or some combination of both in public-private partnerships, ITS technologies provide an unprecedented mechanism for pervasive real-time surveillance of each person's physical location and movement from place to place. These technologies will also be capable of comprehensively collecting, aggregating and manipulating travel and other personal data about an individual throughout the individual's lifetime. ITS technologies will also be able to communicate not only traffic information and transit schedules to travelers, but also other types of information, such as targeted advertising which may be intrusive to some potential ITS users. A few examples of potential

privacy-ITS interaction will highlight the variety of privacy issues ITS is likely to raise. Existing forms of ITS enable remote electronic monitoring of a commercial vehicle, such as a truck or an intercity bus. This form of ITS can be used simply to track the location of the truck or bus. But it can also be used by the truck or bus company to follow and to keep track of every move made by the individual driving the bus. ITS could also provide the exact geographical location of a passenger traveling on the bus. Continuous monitoring of the weight, speed and tailpipe emissions of commercial vehicles, such as trucks or busses will also record much of the working life of the truck's driver. Only slightly more advanced ITS diagnostic systems can automatically inform dispatchers and law enforcement personnel not only about such potential safety problems as worn tires or brakes on the vehicle, but also the physical or psychological impairment of the vehicle's driver. Automatic evaluation of vehicular fitness may be a useful safety measure. But continuously communicating on-going evaluations of driver fatigue (patterns of drift-and-jerk movements) or impairment (weaving) to an ITS monitoring system raises privacy concerns.

In the future, interactive computer and personal communications technologies, such as personal navigation assistance devices, will provide a driver with driving directions (known as route guidance) as well as real-time information about traffic congestion and adverse weather conditions between a driver's current location and her destination. To provide this ITS service, an ITS-equipped traffic management center will maintain a two-directional loop of individualized continuous real-time information about a driver's location and destination and perhaps also about the driver herself. One direction of the ITS information loop will continuously communicate to the traffic management center the driver's location, speed and destination, as well as perhaps other information from on-board diagnostic systems. Going in the other direction, the ITS information loop will communicate back to the driver from the traffic management center such information as traffic flow, directions, and perhaps other information specifically relevant to that individual driver. To the extent information about the traveler in this information loop is computerized and stored, it becomes a detailed travel history of where the driver was at all times in the past, as well as her usual travel patterns and travel plans. All of this information could be very useful to third parties who might want to follow or to keep track of the driver. Such third party trackers might include law enforcement agents, private investigators, advertisers or stalkers.

ITS relational data bases can be designed to compile an individual traveler's planned itineraries, as well as detailed data regarding the times and places of the individual's actual travel. Patterns and profiles of the person's choices can be created and further databases compiled. For example, ITS can collect data regarding how often a particular person goes to a particular location, such as a supermarket. Additional ITS data can be collected regarding how often the person stops along the way at the location of a different type of store, such as a liquor store. A personal profile of the person can be compiled into a database of all travelers who stop at liquor stores on the way to supermarkets. That database can be further sorted according to personal characteristics of this type of traveler (such as gender, race, age, height or weight) or according to particular supermarket chains or types of liquor stores, or according to all of the foregoing factors. In short, ITS applications can be designed to collect, digitize and manipulate transportation data about where individual travelers go, what routes they take to get there, and where they stop along the way. Since digitized data is almost infinitely replicable, and potentially eternal, other relational databases can link ITS transportation data about an individual with other types of information (such as law enforcement, insurance, lifestyle and credit data) to form a comprehensive profile about an individual ITS user. Individual profiles from many ITS users can

be aggregated and used to create valuable marketing forecasts. The privacy concerns about this type of secondary use of ITS data multiply with each additional use of ITS-collected data, particularly when the individual involved may not know about, much less agree to the manipulation of information about her use of surface transportation.

ITS may also augment route guidance directions from where a driver is to where she wants to go, with advertisements regarding fuel, food and lodging or, potentially other types of consumer demand-generating information. To the extent that an ITS service has already collected detailed information about the driver and/or the vehicle, ITS advertisements can be personalized and targeted to appeal to particular travelers, based on personal preference profiles. ITS diagnostic technologies designed to evaluate the status of both vehicles and drivers will enable ITS to personalize ITS advertising in remarkable ways, which some might find intrusive. New passenger cars with on-board computers already communicate to their drivers a variety of information about the vehicle, such as fuel and break status and the operational condition of emissions control systems. ITS communications technologies will be capable of automatically sending such information from the vehicle's diagnostic systems to external monitors, such as ITS system managers, regulatory agencies or law enforcement agencies. Commercial applications of ITS on trucks already include automatic, non-stop weighing and clearance at state and national borders. In the future, automatic communication of vehicular diagnostics will be able to send to ITS system managers such data as readings from seat and seatbelt sensors which automatically configure seats, seatbelts, and air bags to account for the presence and size of passengers, to better protect people such as children or those of above or below average height or weight. Communication of such personal characteristics information, along with other diagnostic data, to ITS traveler information service centers, would make possible tempting opportunities for advertisers. [5]

Cruise control devices and anti-lock breaks are already popular automated applications of ITS. In the future, automatic control systems of this type and even automated highways will partially or completely control vehicles by means of expert systems, so that vehicle operators will have little or no control over their vehicles while the vehicles are on an automated highway. From a privacy standpoint, this transfer of control may feel dehumanizing to the individual who no longer controls her vehicle as it carries her to her pre- programmed destination. Individual choice and control, as well as the autonomy associated with driving would be compromised in these automated ITS applications, particularly if participation in ITS were not voluntary.

On the other hand, ITS technologies will in some ways enhance privacy and other personal rights of travelers. Examples of potential ITS contributions to individual rights range from enabling vision-impaired persons to drive more safely to liberating countless drivers whose lives and choices would otherwise be constrained by long lines for toll collection or by foggy road conditions. In all of these and countless additional ways, ITS will profoundly affect the privacy, as well as the mobility, of surface transportation users.

II. ITS Technologies

The technologies associated with ITS include a variety of applications of surveillance, communications, data processing, traffic control, navigation and other advanced technologies as well as applications of expert systems. Most of the technologies contemplated for use in ITS are already existing technologies, a number of which derive from military defense applications.[6] What

is new about ITS is the systematic effort to apply these available technologies to improve surface transportation through combined efforts of both the public and the private sectors. The goals of the ITS program are "to improve safety, reduce congestion, enhance mobility, minimize environmental impact, save energy and promote economic productivity."[7] Currently available forms of ITS include antilock brakes, automatic toll collection, satellite-based vehicle location using Global Positioning Systems (GPS), and many other technological enhancements for both vehicles and highways. Various smart card technologies[8] and a wide range of enhanced communication methods for providing transportation information, including variable message signs, public transit information kiosks and in-vehicle routing assistance based on current traffic conditions, are all aspects of ITS.

Just what ITS is and does has changed somewhat over time and is likely to change a great deal more as ITS develops in the future. As currently conceived, the federal ITS program is organized around user services including pre-trip and in-route travel information, comprehensive real-time traffic management, electronic toll and transit fare payment services, safety and pollution monitoring, personalized public transit, computerized route guidance and tracking systems, and automatic collision avoidance. ITS applications in the next century will include automated highways on which cars, trucks and busses are controlled by computer systems, rather than by individual drivers.[9]

The current official description of ITS contains the following twenty-nine ITS user services categorized in seven common areas or "bundles:"

A. Travel and Transportation Management
   1. In-Route Driver Information
   2. Route Guidance
   3. Traveler Services Information
   4. Traffic Control
   5. Incident Management
   6. Emissions Testing and Mitigation

B. Travel Demand Management
   1. Pre-Trip Travel Information
   2. Ride Matching and Reservation
   3. Demand Management and Operations

C. Public Transportation Operations
   1. Public Transportation Management
   2. In-Route Transit Information
   3. Personalized Public Transit
   4. Public Travel Safety

D. Electronic Payment
   1. Electronic Payment Services

E. Commercial Vehicle Operations
   1. Commercial Vehicle Electronic Clearance

2. Automated Roadside Safety Inspection
3. On-board Safety Monitoring
4. Commercial Vehicle Administrative Processes
5. Hazardous Materials Incident Response
6. Commercial Fleet Management

F. Emergency Management
1. Emergency Notification and Personal Safety
2. Emergency Vehicle Management

G. Advanced Vehicle Control and Safety Systems
1. Longitudinal Collision Avoidance
2. Lateral Collision Avoidance
3. Intersection Collision Avoidance
4. Vision Enhancement for Crash Avoidance
5. Safety Readiness
6. Pre-Crash Restraint Deployment
7. Automated Highway System [10]

The ITS user services noted above combine one or more of the following technical functions:

> *Traffic Surveillance*, which refers to "Surveillance technologies that collect information about the status of the traffic stream. Possible technologies include loop detectors, infrared sensors, radar and microwave sensors, machine vision, aerial surveillance, closed circuit television, acoustic, in-pavement magnetic, and vehicle probes."
>
> *Vehicle Surveillance*, which refers to "Surveillance technologies that collect a variety of information about specific vehicles. These technologies include weigh-in-motion devices, vehicle identification, vehicle classification, and vehicle location."
>
> *Inter-Agency Coordination*, which refers to "Technologies that connect travel-related facilities to other agencies such as police, emergency services providers, weather forecasters and observers, and among Traffic Management Centers (TMC), transit operators, etc."
>
> *One-Way Mobile Communications*, which refers to "Any communication technology that transmits information to potentially mobile reception sites but cannot receive information back from those sites. Possible technologies providing this function include Highway Advisory Radio, FM subcarrier, spread spectrum, microwave, infrared, commercial broadcasts, and infrared or microwave beacons."
>
> *Two-Way Mobile Communications*, which refers to "Any communication technology that transmits information to potentially mobile reception sites and allows

receipt of information from those same sites. Possible technologies include cellular telephones, 2-way radio, spread spectrum, microwave, infrared, and 2- way satellite."

Stationary Communications, which refers to "Any communication technology that connects stationary sites. Technologies include fiber optics, microwave, radio, land lines."

Individual Traveler Interface, which refers to "Devices that provide information flow to a specific traveler. Technologies meeting this function include touch screens, keypads, graphic displays and computer voices at kiosks; keypads, computer voice, and head-up displays in vehicles; personal communications devices carried with the traveler; and audiotext from any phone."

Payment Systems, which refers to "Technologies that enable electronic fund transfer between the traveler and the service provider. The technology areas include Automated Vehicle Identification (AVI), smart cards, and electronic funds management systems. This function overlaps with the Electronic Payment user service."

Variable Message Displays, which refers to "Technologies that allow centrally controlled messages to be displayed or announced audibly to multiple users at a common location such as a roadside display or display board in a transit terminal. These technologies would typically be applied to provide information on highway conditions, traffic restrictions, and transit status."

Signalized Traffic Control, which refers to "Technologies that allow for real-time control of traffic flow. Possible technologies include optimized traffic signals, ramp metering, reversible lane designation, and ramp/lane closures."

Restrictions Traffic Control, which refers to "Operational techniques that restrict the use of roadways according to regional goals. Techniques include HOV restrictions, parking restrictions, and road use (congestion) pricing."

Navigation, which refers to "Technologies that determine vehicle position in real time. Technologies that provide this function include GPS, LORAN, dead reckoning, localized beacons, map database matching, and cellular triangulation."

Database Processing, which refers to "Technologies that manipulate and configure or format transportation-related data for sharing on various platforms. General purpose data base software currently exists and is currently being adapted to transportation needs such as data fusion, maps, and travel services."

Traffic Prediction Data Processing, which refers to "Data processing relating to prediction of future traffic situations. Algorithms under development include areas such as real-time traffic prediction, and traffic assignment."

Traffic Control Data Processing, which refers to "Data processing related to the

real-time control of traffic. Algorithms under development include optimal control and incident detection, and the interaction of route selection and traffic control."

Routing Data Processing, which refers to "Data processing related to routing of vehicles including the generation of step-by-step driving instructions to a specified destination. Algorithms under development include the scheduling of drivers, vehicles, and cargo; route selection; commercial vehicle scheduling, and route guidance."

In-Vehicle Sensors/Devices, which refers to "Technologies providing a range of sensing functions to be located within vehicles. Functions addressed by these technologies include monitoring of vehicle performance and driver performance; determination of vehicle position relative to the roadway, other vehicles, and obstacles; improvement of vision in adverse conditions; and on-board security monitoring." [11]

Some of these ITS functions, such as variable message displays, signalized traffic control and traffic prediction data processing will have very little relationship with privacy, because these technologies do not focus on individual travelers. Other ITS functions, such as traffic control data processing and restrictions traffic control, will indirectly affect privacy by affecting transportation choices. Combining these technical capabilities into a wide variety of interactive and intelligent systems and services is the role of ITS.

III. Privacy Concerns about ITS

Privacy is at least as multifaceted and variable as ITS technologies. Privacy laws relevant to ITS will vary depending on where and by whom a particular ITS application is operated. Since ITS is composed of a variety of government and private sector systems, as well as public-private partnerships, privacy concerns about ITS are characterized by a particularly lively variety. As the Santa Clara Symposium papers and other materials in this issue underscore, variability and open-endedness have also been key features of privacy law, since Brandeis's initial suggestion in 1890 that the law ought to recognize and protect a legal right of privacy.[12] Privacy concerns have come a long way since then. [13]

The notion of a general legal right to privacy first suggested by Samuel D. Warren and Louis D. Brandeis presented privacy as an already existing common law right which protects each individual's "inviolate personality." [14] They asserted that "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others . . . fix[ing] the limits of the publicity which shall be given them." [15] Almost thirty years later, Brandeis maintained that this same privacy right constrains government, just as he had earlier argued for legal redress for invasions of privacy by the private sector. According to Brandeis, the purpose of the Constitution is "to protect Americans in their beliefs, their thoughts, their emotions and their sensations." He insisted that the makers of the Constitution "conferred, as against the Government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the employed, must be deemed a violation" of the Constitution.[16]

By 1960, William Prosser had decided that the right to privacy was articulated in a group

of four distinct bases for civil liability in tort: appropriation of another person's name or likeness, intrusion on a person's seclusion or into his private life, public disclosure of embarrassing private facts about an individual, and publicity which places a person in a false light. [17] A few years later, the Restatement, Second of Torts, for which Prosser was the Reporter, adopted these four torts as parts of the Second Torts Restatement.[18] In 1967, Alan Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[19] Westin suggested that privacy performs four types of functions for individuals in democratic societies: "personal autonomy, emotional release, self- evaluation, and limited and protected communication."[20] Arthur R. Miller, whose influential The Assault on Privacy was published in 1971, remarked in a 1991 speech that, "I have come to realize that there is something quite primordial about privacy. It is a value people believe in and want. Even people who do not necessarily seek it out on a day to day basis would like to know that they can have it when they want and seek it. The ever-changing character of the issues is a constant reminder that the value is something that we cherish and we constantly think about and need."[21]

In a sense, the many commentators about the meaning of privacy are all persuasive in one way or another. But that multi-faceted quality does not dissolve privacy in meaningless ambiguity. Constitutional law scholar, Paul Freund in his provocative essay, "Privacy: One Concept or Many" suggested that even if a right of privacy is not a very precise legal rule, "it would be impoverishing to exclude it as the term of a legal principle."[22] Professor Freund noted the difference between principles and rules: "A higher order of generality is not only tolerable in the statement of principles; it is to be encouraged . . . A rule is a particularization that describes the state of the law in a defined context, and prescribes with a relatively high degree of immediacy and precision. A principle is a more plastic formulation, useful for predicting and shaping the course of legal development. It is in the latter context that the right of privacy is of cardinal worth."[23] Senator Sam J. Ervin, Jr., the chairman of the Senate Watergate Committee, agreed. Senator Ervin suggested that "In the end, privacy depends upon society's recognition, and protection of, the importance and uniqueness of each individual."[24] That suggestion seems to direct attention back to the original notion of the right to privacy as protection for individual personality initially suggested by Warren and Brandeis. In this most general of senses, privacy is certain to affect twenty-first century technologies,[25] such as ITS, in significant ways. People want technology, such as ITS, to be structured and managed so that the technology does not interfere with privacy. Their demand is not that ITS needs to manage privacy; but rather that ITS needs to respect privacy. This broad understanding of privacy as a principle associated with respect for individual human dignity underlies this discussion of privacy and ITS.[26]

A different way to understand privacy concerns about ITS comes from asking ordinary people what they think about ITS transportation technologies and the potential impacts of ITS on privacy. That was the strategy adopted in creating the following "top-ten list of privacy concerns." The list is not the product of a scientific survey. Rather, it reflects informal conversations with people who expressed interest in ITS technologies.[27] The list highlights some recurring patterns in what potential ITS users had to say about how intelligent transportation technologies were likely to affect privacy.

In addition to the ten listed privacy concerns, two initial reactions to ITS seem to be nearly universal when people begin to think and to talk about ITS. First, most people have difficulty understanding ITS. In part because of the dynamic and variable qualities of the many

different ITS technologies and in part because only a few examples of ITS are parts of everyday experience, ITS has an almost science-fiction quality for many people. That lack of understanding is in itself a potential privacy problem. To the extent that respecting privacy will involve real choices on the part of ITS users with regard to whether or not they will use various ITS services, such choices must be understandable and informed. Assuring that choices to use or to avoid ITS services are based on meaningful information will be one of the major challenges ITS will face in meeting privacy concerns. A second interesting initial response to descriptions of ITS, even before privacy was mentioned, was the nearly universal reaction that ITS "sounds interesting, but creepy."

After these two initial reactions to ITS, the following Top-Ten List of Privacy Concerns about ITS emerged. The list begins with the most frequently expressed privacy concern - automatic secret surveillance.

1. *ITS applications can be used invisibly to track a targeted individual's movements from place to place.*

Although no extensive law enforcement uses of ITS systems and technologies are contemplated by ITS development plans,[28] many people believe that remote, real-time surveillance of individuals is the main purpose of ITS. People seem concerned not only about law enforcement surveillance by government agencies, but also about non-governmental surveillance by private investigators. The possibility that stalkers might be able to use ITS was a matter of great concern to a number of people. The fear that ITS will be used to track and collect detailed information about an individual's movements without the individual's knowledge or consent was palpable. Even people who consider themselves unlikely to be targeted for any kind of surveillance seem to feel that their privacy would be affected by an ITS operation which at any time could target them. Some people describe ITS as an unseen system of potential surveillance which would cause them to constrain their travel choices to avoid potential scrutiny, whether or not they were actually being tracked.[29]

The suggestion that ITS might adopt a single "smart" transportation card to be used to pay for the use of toll roads, toll bridges and parking facilities, as well as for transit fares, intensified privacy concerns about ITS as a comprehensive surveillance system. Such multimodal ITS payment systems magnify fears that ITS will enable a central automated monitor to keep minute-by-minute track of where a targeted individual is located at virtually all times, "with no escape." The fact that ITS vehicle surveillance would be electronic and invisible, gave rise to concerns that targeted individuals will be followed remotely so that they never even become aware that they are being, have been, or will be tracked.

2. *ITS applications can be used automatically to collect comprehensive information about when and where every person travels.*

This second most frequently expressed type of privacy concern about ITS is particularly interesting because the people who express it usually are well aware that the information which ITS applications collect is neither very personal, nor very private. ITS

information about individuals consists almost entirely of information about a person's movements in such public settings as roadways and transit systems. What seems to trouble people from a privacy standpoint is that the information is potentially so comprehensive - a nearly complete reflection of when and where each individual has traveled, possibly over an entire lifetime. The fact that ITS systems, in the short run at least, will not contain anywhere nearly comprehensive information about any particular individual does not seem to affect these privacy concerns. It is the potential for ITS to develop into such a comprehensive information collection enterprise which seems to generate serious privacy concerns, even before any information has been collected.

Moreover, people also seem to feel that ITS technologies will take from them something which is uniquely theirs, has value, and which at the same time both reflects them and can have consequences for them - the way they move about in the world. Many people are willing to consent to use of various types information about themselves, including transportation information. But they want to be given the choice. That independent-minded Americans want to be asked to cooperate voluntarily in intelligent transportation systems, and to be given a choice whether to cooperate or not, seems to reflect a basic part of American culture, in which independent individuals demand respect and resist manipulation.

As a practical matter, people are also concerned that the purpose of collecting comprehensive transportation information regarding everywhere each individual goes is so that individual transportation information can be retrieved and used, or manipulated, later. Should someone (whether in law enforcement, litigation, direct marketing or out of simple curiosity) want to establish an individual's travel profile or detailed travel history, such ITS records would provide a convenient information source. People prefer not to have ITS collect the information in the first place, rather than have to worry about preventing others from using it to invade their privacy sometime in the future. Often people talked about keeping the camel's nose out of the tent. In the last century Justice Bradley used a Latin phrase, obsta principiis, (withstand beginnings) in Boyd v. United States,[30] to insist on the importance of preventing even the first initial steps toward interfering with the privacy interests protected by the fourth and fifth amendments.

3. *ITS will create a computerized personal travel profile which will be used to make decisions about an individual, as well as to predict and to manipulate the individual's future choices about transportation and other matters.*

People are concerned that ITS-generated travel profiles will threaten privacy because such a profile can become a substitute for the person herself. Profiles of this type seem dehumanizing to individuals at best. If a profile is different from the individual's own self-image, the disjunction can be damaging psychologically. At the least, such disjunction tends to undermine a person's self-respect. These types of privacy concerns about ITS are sometimes expressed in complaints about the tendency of ITS to reduce the complexity of an individual human personality to ciphers and formulas. It makes no difference that ITS information is not very personal or private, when compared, for example, with data about a person's health or financial status. People seem to be concerned when a comprehensive information profile is constructed about any aspect of their lives. Moreover, the

transportation information which ITS will collect is likely to reveal other aspects of a person's private life. For example, locations can indicate places of worship, theaters, libraries and bookstores.

4. *ITS applications can aggregate, or connect up, stored information about an individual's travel patterns with other information regarding that individual.*

People are very concerned that ITS information about a person will be linked with other types of information, such as the person's political affiliation, religion, known associates, buying patterns, insurance, health and the like. In part, this is an objection to manipulation and use of ITS information about an individual without the individual's consent. This type of privacy concern also reflects people's objections to being treated impersonally. If ITS information is incorporated into an overall information profile of an individual, that the profile can be used as a substitute for dealing with the individual personally. People also want to be able to decide for themselves whether or not ITS information about them will be compared or matched or compiled with other information.

5. *ITS applications can use or disclose information about an individual's travel history or profile in ways which may both reflect him or her and affect his or her future opportunities and choices.*

People are concerned that ITS will result in labels, such as "chronic speeder," "polluter," or "frequently visits red light district," being attached to people. An individual, who does not perceive herself the way she is labeled, may not only find such labels jarring. She may also be concerned that some of these labels can affect her life and her opportunities as, say, a school bus driver, environmental activist or pastoral counselor.

6. *ITS can manipulate individual decisions about modes, times and destinations of travel by means of route guidance, traffic congestion information, persuasion and advertisements of products and services.*

People raise privacy concerns about these ITS functions because they fear that ITS will be used to manipulate individual choices about transportation and other matters. People express concern about being subjected to unwanted advertising information and manipulation by ITS traffic congestion information or congestion pricing, known as travel demand management. They dislike the idea of being "managed" by a faceless and unseen ITS traffic management system. This type of privacy concern reflects the general preference people have to manage and control themselves. Some people express particular concern that they will be unable to switch off what they fear will be a barrage of ITS information intruding into their private lives and thoughts, in their homes and automobiles. Just the suggestion that an overriding 911 system could issue warnings of dangerous weather or driving conditions, whether or not the person has turned on her ITS system, causes people to fear the use of ITS as an involuntary communications medium for other sorts of messages, political, social or advertising.

7. *ITS monitoring and reporting of vehicle and operator conditions can be used to override individual travel decisions.*

This type of privacy concern objects to use of ITS monitoring capabilities, combined with automatic controls over whether and how vehicles and drivers will be allowed to travel. People are concerned that ITS will be used automatically to monitor information about the condition of a driver and her vehicle and then, just as automatically, to use this information to decide whether or not the driver or vehicle will have access to transportation facilities. This concern is far from illusory, since utilization of such an access control function is already part of an application of ITS congestion management in Singapore. This type of privacy concern focuses primarily on whether the individual will be fully informed and allowed to voluntarily consent, or not, to participation in ITS.

8. *ITS can take over control of vehicle or transit operations by means of intelligent automated systems, which substitute ITS control for control by an individual.*

Privacy concerns of this type focus on the capacity of ITS to override individual control. People are concerned that ITS will take from the individual control over her own movements and mobility. Advanced ITS applications, such as Automated Highways, are expressly designed to transfer control over many vehicle operation functions to automated intelligent systems. Individuals who prefer to retain control over such functions sometimes describe this type of ITS operation as interfering with their privacy, in the sense of overriding individual choices, decisions and control.

9. *Government agencies can use ITS to collect, to manipulate and to disclose information about individual travelers and to control their travel by means of government-controlled automated systems.*

People are concerned that ITS will give government agencies control over an important aspect of daily life. They fear that ITS will endanger privacy by giving government too much power to manage and control individual lives. Federal, state and local government agencies are all feared in this regard. ITS is perceived as threatening to shift the balance of power from the individual to the government, at least with regard to transportation aspects of an individual's life. This type of privacy concern was roughly equal in importance to the tenth concern noted below. However, people older than forty years old tended to mention the Watergate abuses of government agencies or the loyalty checks of the McCarthy era and generally expressed greater concern about misuse of ITS by government to invade people's privacy, than about misuse of ITS by private entities.

10. *Private entities, especially large corporations, will use ITS to collect, to manipulate and to disclose transportation information about individuals and use ITS to take over control of travel.*

To the extent that a private ITS provider controls individual travel information, transportation options and sometimes both, privacy concerns arise because of the power

the ITS provider would then have over the individual. Historically, concerns about the power exercised by large private-sector entities have, historically, sometimes been as serious and as deeply felt as concerns about government power. This type of privacy concern was roughly equal in importance to the ninth concern noted above. However, people who were younger than forty years old tended to be more concerned about private companies misusing ITS to invade privacy, than they were about government misuse of ITS.

This list of privacy concerns is not presented as a scientific catalogue of privacy concerns about ITS and other transportation technologies of tomorrow. But it does suggest some general themes and some areas in which ITS will need to design proper respect for privacy into the very structure of ITS. Development of ITS architecture, which is well under way, already includes consideration of privacy.[31] Deployment of ITS will need to put respect for privacy into ITS practice.

Considered from yet a different standpoint, there are many political and philosophical reasons why concerns about individual privacy are likely to be raised about ITS. One reason for protecting privacy is to prevent the individual from being overwhelmed by the larger society of which the individual is a part. Privacy is often described as a way to fence off the individual from unwanted attention on the part of big business and big government - the composite threat personified by George Orwell's Big Brother in the novel, 1984. When people react to ITS as a "Big Brother" technology, that is a way of underscoring concerns about the impact these transportation technologies could have upon an individual vulnerable to being oppressed by a much more powerful society.

However, not everyone agrees that individual privacy is desirable. Some commentators and legal scholars reject the legal concept of privacy and both deride and attack it.[32] Privacy is sometimes criticized as class-based, offering little of interest or utility to the population as a whole. Political viewpoints which place more importance on the community or society than on its individual members generally disapprove of privacy. Ruth Gavison has extensively explored this problematic status of privacy among feminists.[33] In addition to feminists, others have objected to privacy as wrongheaded, literally with the priorities of society and the individual upside down. For them, privacy is fundamentally subversive of what they feel are more important societal or group objectives. Inevitably controversial as a political matter, privacy concerns insist on protecting the individual from the power of the state and of society at large. Being concerned about privacy is essential to the attitude of non-conformists and independent-minded individualists.

Because privacy also can become somewhat antisocial, policy makers usually seek to balance privacy with other societal values, such as social control, deterrence of anti-social behavior, and public health and safety. In the ITS context, such competing values which will be balanced with privacy concerns include highway safety (for example, keeping speeders, drunk drivers and unsafe vehicles off the roads) and environmental quality (for example, alleviating air pollution by reducing traffic congestion).

IV. ITS Concerns About Privacy

ITS is concerned about privacy, and privacy laws in particular, for at least three reasons.

In the first place, recognition of privacy as a value seems worthy of concern in designing ITS systems, because in the long run public acceptance and use of ITS services will depend on public confidence in the technology as not predatory or harmful.[34] Respecting privacy fosters public confidence in ITS and will add to the consumer appeal of ITS services. Second, taking account of privacy is mandated under the federal organic act which created the federal ITS program.[35] Third, a variety of existing privacy laws will constrain how ITS can be operated. Structuring ITS in ways which avoid violating federal and state privacy laws will be important for an ITS industry which will operate nationwide. In the United States, ITS services will have to comply with a wide range of both federal and state privacy laws.

Existing privacy laws which may potentially affect ITS are enormously varied and dynamic. The nature of the privacy laws which will apply to ITS will depend in part on where and by whom a particular ITS application is operated. Since ITS technologies will be created and operated by private-sector entities, by government entities, and also by public-private partnerships, almost every type of privacy law is potentially applicable.[36] Both state and federal privacy laws will apply to ITS, including constitutional privacy protections, many different privacy statutes and regulations, as well as common law tort actions for invasion of privacy.

Legal conceptions of privacy are notoriously uncertain. Within the universe of legal concepts, privacy laws often seem to behave like the fractals in chaos theory - ever-changing in unpredictable but patterned ways.[37] Some years ago, Chief Justice Rehnquist described the privacy cases decided by the United States Supreme Court as "defying categorical description."[38] Professor Arthur R. Miller chose "A Thing of Threads and Patches" as the title of one of the chapters in his influential book, The Assault on Privacy.[39] A federal judge once described privacy law as like a "haystack in a hurricane."[40] Privacy laws seem to have this amorphous quality in part because privacy depends to some extent on each person's expectations regarding respect for her individual personality. Based on connotations of respect for individuality, privacy laws have developed through richly suggestive, but hardly very precise, metaphors. Perhaps because privacy operates as a value and a legal principle,[41] privacy laws resist being fitted into any fixed catalogue of legal rules and requirements. As a result, the precise interaction of changing and varied privacy laws with the dynamic and multifaceted ITS technologies will be very difficult to predict. What is certain is that ITS technologies and systems will have to comply with a seemingly bewildering variety of both federal and state privacy laws.

Nevertheless, engineers and scientists who work with ITS projects and policymakers who decide which ITS projects will be undertaken need a framework of privacy laws to outline some logical categories to guide selection and design of ITS plans and projects. For example, a traffic engineer suggested preparation of a privacy law chart for ITS operations which would look something like this:

Clearly legal	Not clearly legal or illegal	Clearly illegal

ITS development would certainly be simpler from a privacy standpoint if most intelligent transportation technologies fit under the left column, a few clearly rogue applications fit in the right column, with nothing much left in the middle. Unfortunately, most privacy laws place ITS squarely in the uncertain middle category.

Privacy laws are most likely to affect ITS by constraining how ITS is managed and operated. ITS technologies[42] do not appear to be outlawed by existing privacy laws. Plans for

ITS do not, for example, include use of wiretaps or scanners, which are outlaw technologies prohibited under the federal electronic surveillance statues. Rather, because the "intelligent" part of ITS depends on information, most of the privacy laws which will apply to ITS will focus on ITS communication functions and information use. In particular, privacy laws will govern how ITS information is communicated from, to and about individual drivers or travelers.

Because federal and state privacy laws differ in applicability, federal and state privacy laws need to be considered separately. The nation- wide reach of federal privacy laws (including constitutional provisions, statutes and regulations), contrasts sharply with the more limited territorial reach of state privacy laws (including state constitutional provisions, state statutes and regulations, as well as common law civil liability in tort for invasion of privacy), which apply within the geographical boundaries of each jurisdiction. This difference in applicability makes it sensible to discuss the federal privacy laws which apply throughout the United States and then to turn to the much greater variety of state privacy laws.

Federal Privacy Laws

Much of the federal constitutional privacy law potentially applicable to ITS is derived from the federal constitutional prohibition against unreasonable searches and seizures under the fourth amendment to the United States Constitution. This federal constitutional privacy protection applies only to privacy invasions by federal, state or local government, usually in a law enforcement context. This branch of privacy law depends in part on whether the person objecting to a search or seizure has an expectation of privacy which is reasonable.[43] Law enforcement use of remote electronic tracking technology similar to that which ITS will utilize has, for the most part, not been found to be an unreasonable search or seizure under federal law.[44]

In addition, constitutional privacy protection associated with rights to liberty and rights to freedom in making personal choices guaranteed under the fifth and fourteenth amendments to the United States Constitution could affect ITS. Were public sector ITS applications to constrain transportation choices through demand management strategies, this type of privacy concern might arise, despite the fact that transportation choices are not at all intimate, in contrast to family planning or healthcare choices which have been the focus of this branch of privacy law. In a much more speculative area of constitutional theory, were ITS to require people to give up privacy rights in exchange for permission to use public highways, questions could arise with regard to whether compulsory participation in ITS would impose unconstitutional conditions.[45]

With regard to federal statutes designed to protect privacy, in some ways the most important for ITS are the federal electronic surveillance statutes, particularly the Electronic Communications Privacy Act of 1986,[46] as amended by the 1994 Communications Assistance for Law Enforcement Act.[47] These statutes, which regulate the interception of wireless oral and electronic communications, including ITS data transmissions, will generally protect ITS communications against interception both by law enforcement and by eavesdroppers. Vehicle-identifying time and place information, sometimes called a transmission record, continuously transmitted between a vehicle and an ITS traffic management facility should be protected against unlawful interception under the 1994 Communications Assistance for Law Enforcement Act.[48] Although under these federal statutes a variety of ITS information about individual ITS users may be used and disclosed by an ITS provider "in the ordinary course of business," the 1994 amendments are likely provide additional protection for the communications privacy of ITS.

Because ITS will employ many different types of communications technologies in providing different types of ITS services, the application to ITS of the federal electronic surveillance laws as amended by the 1994 Communications Assistance for Law Enforcement Act is not completely certain. For example, the portions of the 1994 amendments designed to apply to the relationships between telecommunications common carriers and law enforcement agencies seeking to intercept digitized telecommunications probably will not apply to ITS. ITS communications functions may utilize services provided by telecommunications common carriers, but probably will not. Overall, the 1994 changes in federal electronic communications law should, for the most part, enhance safeguards for the privacy of ITS users.

The law enforcement interceptions facilitated by the 1994 amendments are, however, invasive of privacy interests. The provisions of the 1994 Act worthy of special note from an ITS perspective appear in Title II. Law enforcement access to transactional data associated with "on-line communication systems" now requires a warrant under sections 201 and 207. But this warrant need not be based on probable cause, but rather on "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[49] This law enforcement access authority is described in the House Report as

> an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

Law enforcement could still use a subpoena to obtain the name, address, telephone toll billing records, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized.[50] These changes in federal electronic surveillance law on ITS will probably mean that the use of the intermediate-level warrant requirement will apply to most law enforcement access to most ITS vehicle surveillance data.

In addition to law enforcement interceptions, which are the primary focus of the 1994 legislation, other aspects of the Communications Assistance for Law Enforcement Act will more generally affect privacy in a positive fashion. According to the House Report,

> The legislation also expands privacy and security protection for telephone and computer communications. The protections of the Electronic Communications Privacy Act of 1986 are extended to cordless phones and certain data communications transmitted by radio. In addition, the bill increases the protection for transactional data on electronic communications services by requiring law enforcement to obtain a court order for access to electronic mail addressing information.

The bill further protects privacy by requiring the systems of telecommunications carriers to protect communications not authorized to be intercepted and by restricting the ability of law

enforcement to use pen register devices for tracking purposes or for obtaining transactional information. Finally, the bill improves the privacy of mobile phones by expanding criminal penalties for using certain devices to steal mobile phone service.[51] Prominent among the purposes underlying the legislation, according to the House Report, are concerns about "protecting the privacy of communications" and avoiding "impeding the introduction of new technologies, features, and services."[52]

The 1994 amendments also provide new protection against interception of radio portions of a cordless telephone communication between the handset and the base unit and impose a $500 penalty for intentionally intercepting cordless telephone communications.[53] Although ITS does not, at least at present, generally employ cordless telephones, the Congressional commitment to the privacy of short-distance radio communications expressed in the 1994 amendments may suggest potential support for similar protections for the short-distance radio communications which are frequently used in ITS. In general, radio-based communications are included among "electronic communications" which the 1994 amendments protect against eavesdropping.[54] The House Report notes that these provisions "provide protection for all forms of electronic communications, including data, even when they may be transmitted by radio."[55] In addition, the 1994 amendments extend protection to data and communications "encrypted or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communications, . . . "[56] These provisions may affect the privacy ramifications of particular communications media and encryption strategies which may be used by ITS applications. The 1994 amendments also add both scanning receivers and "hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services, . . ." to the list of prohibited electronic eavesdropping devices.[57] This provision designed to protect personal privacy will also safeguard important rights of ITS providers and users to proprietary data.

Other federal privacy statutes which may apply to certain aspects of ITS are concerned with consumer credit and financial matters. These statutes include the Right to Financial Privacy Act,[58] the Fair Credit Reporting Act,[59] the Fair Credit Billing Act [60] and the Fair Debt Collection Practices Act.[61] These federal consumer privacy statutes are designed to prevent misuse of particular types of personal information. To the extent that consumer credit and financial information is incorporated into particular ITS applications, such as toll-collection or toll-billing functions, these federal statutes may apply. The Drivers' Privacy Protection Act of 1994, which was part of the 1994 Crime Bill[62] will not directly apply to ITS unless ITS records become part of state motor vehicle and driver licensing records. But this statute may make it more difficult to link ITS information attached to Vehicle Identification Numbers with identifiable individuals.

At present, it does not appear likely that federal agencies will operate ITS or collect or maintain ITS data regarding individuals. If, in the future, ITS were to be operated by federal agencies, two additional federal privacy statutes might apply to ITS: the Privacy Act and the Freedom of Information Act. The Freedom of Information Act, or FOIA,[63] would probably require public disclosure of most ITS information held by federal agencies, unless the interference with personal privacy caused by the disclosure were found to be clearly unwarranted. Keeping in mind that the application of this and other FOIA exemptions tends to be very context-specific, it seems unlikely that ITS transportation information would always be withheld from disclosure.[64] If ITS information about individuals were collected by a federal agency, the Privacy Act of 1974[65] would generally restrict disclosure and use of personal ITS data collected by federal agencies to

those purposes for which the information was originally collected. Moreover, the Computer Matching and Privacy Protection Act of 1988,[66] would regulate federal data matching programs were they to make use of ITS information. At present, no such matching of ITS data with data held by various federal agencies has been proposed. Were ITS data to become part of individual information databases held by federal agencies, from the Internal Revenue Service to the Department of Veterans Affairs, concerns about privacy with regard to this ITS information would rise sharply. Moreover, because the FOIA, and to a lesser extent the Privacy Act, are frequently followed in state court interpretations of state public records and privacy laws, the federal FOIA, and other federal statutes affecting privacy, are likely to provide persuasive precedent when state courts interpret similar state privacy and public records statutes.

State Privacy Laws

In contrast to federal privacy laws which apply uniformly throughout the United States, state privacy law is both highly differentiated on a state- by-state basis and more intensive in its regulation of private sector privacy invasions, as well as government agency intrusions. Many different types of state laws will govern the handling of information about individuals collected by ITS operations, whether that collection is accomplished by state or local agencies or by private sector transportation, financial service or credit reporting organizations.

Overall, state privacy laws are characterized by remarkable volume and variety. The map at the end of the Appendix to this article illustrates some general estimates of the varying intensities of privacy laws across the United States. The five tables which precede the map summarize some of what the Santa Clara Privacy and ITS Legal Research Project found in looking at five groups of twenty-five different types of state privacy laws which could affect the deployment of ITS. Types of state privacy laws potentially applicable to ITS include state constitutional privacy laws, state statutory privacy laws and also state common law privacy torts. Privacy law often applies in overlays, with federal law applicable in all states and then various patterns of state privacy laws providing additional privacy protections. The privacy laws which govern electronic surveillance are a good illustration of this overlay pattern in which several layers of state constitutional and statutory privacy law often operate simultaneously with federal constitutional privacy provisions and federal privacy statutes.

State constitutional provisions guaranteeing privacy will present a distinct privacy challenge for ITS in the handful of states where state constitutions specifically guarantee a right of privacy.[67] These state constitutional privacy guarantees raise interesting legal questions because they generally signal the likelihood of more intense privacy protection in these states. At present, there are no state court interpretations of state constitutional privacy guarantees in the ITS context. One potentially analogous type of public activity in which privacy rights have been protected as a matter of state constitutional privacy law is trash disposal. Although the United States Supreme Court does not recognize privacy rights in trash left on the curbside to be removed by refuse collectors, several state supreme courts have protected such privacy rights as a matter of state constitutional privacy law.[68] If this view was extended to tailpipe emissions from vehicles, such an interpretation might make it difficult to operate the proposed ITS emissions testing and mitigation user service. When emissions testing ITS services target individual drivers and vehicles for enforcement of environmental standards,[69] such testing would be particularly susceptible to challenge as an invasion of privacy.[70] Unless law enforcement applications of ITS

are on a state-by-state basis or are as privacy-protective as the most restrictive states, such differential rulings among the states may stand in the way of uniform operation of an ITS system nationwide. The fact that in some states,[71] state constitutional privacy guarantees apply to both the private sector, as well as the public sector, means that state constitutional privacy guarantees in those states will constrain privately operated ITS, as well as publicly operated ITS.

Virtually every state constitution also specifically prohibits unreasonable searches and seizures. However, various state courts around the country have expressed many different views regarding the types of privacy expectations which should be protected as reasonable. Variation in state court views about the reasonableness of privacy expectations is particularly pronounced with regard to vehicles. For example, although law enforcement use of electronic vehicle tracking technology has generally not been found to be an unreasonable search or seizure under federal law, some state courts have found law enforcement use of electronic beeper surveillance to be a violation of reasonable expectations of privacy protected under state constitutions. In other states, courts have specifically held that this same electronic tracking technology does not invade privacy. Privacy laws regarding electronic vehicle tracking illustrate how context-sensitive and geographically varied state privacy law can be.

All states and the District of Columbia have adopted public records acts, typically similar to the federal Freedom of Information Act. These statutes pose at least fifty-one different privacy challenges to operation of public-sector ITS by state and local government entities. A number of these open public records laws contain privacy exemptions. But none of these exemptions for private or confidential information appears to specifically require nondisclosure of ITS information about individuals. Some state agencies may treat some ITS information regarding individuals with some degree of confidentiality. But, since none of the state public records laws clearly provides for confidentiality of ITS information, ITS users are likely to be justifiably concerned about the privacy of information about them collected by public sector ITS operations. Unless state public records statutes are amended to exempt ITS information from disclosure, the ready availability of information about individuals contained in ITS systems is likely to pose serious privacy problems for publicly operated ITS.[72] The nature of the information about individuals collected by ITS is generally not very intimate. It will consist mostly of an individual's requests for directions and trip reports reflecting how and when the individual has moved from place to place on roadways or public transit systems. The fact that even such mundane information can sometimes be revealing, destructive, or both with regard to an individual,[73] may cause potential ITS users to prefer not to use ITS if the result is that such information becomes public, or available to anyone who asks for it.

The courts of most states recognize damage actions for invasion of privacy. Generally, privacy damage actions under state common law reflect the four categories outlined in the Restatement, Second, of Torts, Sections 652A - 652I: appropriation of name or likeness, presentation of a person in a false light, intrusion on seclusion, and public disclosure of private facts. Exactly how various state courts will apply these common law tort doctrines to the many different ITS applications is difficult to predict, since there is no reported court decision regarding tort liability for invasion of privacy in a context similar to ITS. As a general matter, tort liability for invasion of privacy requires intentional conduct on the part of the defendant. A few states expressly disapprove negligence as a basis for privacy tort liability. Moreover, in those states which require that the conduct infringing privacy be willful or outrageous, ITS routine operations are unlikely to result in tort liability for invasion of privacy. To the extent that ITS is operated by

state or local government agencies, the potential for successful common law privacy damage actions against public sector ITS agencies may well also be limited by sovereign immunity. Nevertheless, whether or not privacy litigation ultimately results in damage liability, the risk of costly litigation over invasion of privacy will likely constrain the activities of ITS operators.

This brief overview of federal and state privacy laws potentially applicable to ITS can only suggest the contours of a geographically diverse and complicated body of many different types and sources of privacy law.[74] Overall, ITS is likely to benefit from the effects of these various privacy laws in at least three ways. First, privacy law will promote ITS efficiency. The purpose of ITS is not to collect personal information about individuals. To the extent that privacy laws constrain ITS collection and use of personal information, privacy laws will assist ITS in keeping in focus the ITS goals of improving safety, reducing congestion, enhancing mobility, minimizing environmental impacts, saving energy and promoting economic productivity. Second, some of the privacy laws will reinforce protection for the integrity and security of ITS computer hardware, software and data by preventing and punishing interferences with personal information held by ITS computer operations. Third, compliance with these privacy laws should, by demonstrating respect for individual privacy, increase the confidence of ITS users in ITS as a valuable technology the benefits of which can be enjoyed without sacrificing individual privacy.

V. Safeguarding Privacy

Safeguarding privacy is certain to be important if ITS is to be accepted in the United States. Exactly how to safeguard privacy is much less clear. Three general types of privacy safeguards can help ITS properly respect individual privacy: technological safeguards, industry standards and legal requirements. The best privacy strategy for ITS will be to adopt combinations of these privacy safeguards, with multiple types of privacy protections and mechanisms to assure that privacy is respected by the various types of ITS applications which will operate in different parts of the United States. The diversity of existing privacy laws around the United States suggests that there will be many types and degrees of concerns about privacy as ITS is deployed in various localities.

Technological Privacy Safeguards

Common sense suggests that, since individual people are at the center of privacy, the best safeguard for privacy would be to structure ITS technologies so that ITS nowhere identifies individuals. It is at least theoretically possible to protect privacy by designing ITS so that it does not contain private information about individuals at all. In such an arrangement, ITS applications would have general, non-individualized, traffic management functions, such as traffic flow measurements. ITS would also be able to monitor ambient air standards. But ITS would lack the technical capacity to identify individuals. As a result, privacy would be protected by keeping the individual person out of the ITS information loop. Since ITS would not recognize, much less keep track of, individuals, privacy concerns would fade into the background.[75]

Many existing ITS operations are already non-individualized in that they do not deal with information about identified individuals except perhaps for billing purposes. For example, toll collection technologies frequently use numeric identifiers such as a vehicle registration number or Vehicle Identification Number (VIN), rather than an individual's name, social security number, or

driver's license number. Nevertheless, since most states have allowed wide-open public access to vehicle registration records which link a vehicle's registration number with the name and address of the vehicle's owner, it has been relatively simple, not to mention cheap and perfectly legal, to associate a vehicle with a person or vice-versa. The Drivers' Privacy Protection Act of 1994 will make it only slightly more difficult to connect vehicle registration numbers with individuals.

Several important difficulties would result from protecting privacy by completely eliminating the individual. To begin with, such an approach to protecting individual privacy would result in ITS disregarding the very individual person who is at the core of why people care about privacy. In addition to this dehumanizing factor, eliminating the capacity of ITS to identify individual transportation users may also eliminate many of the benefits of some ITS user services. Rather than eliminating the individual, minimizing collection of information about individuals might be a better technical strategy to protect individual privacy and should also be cost-effective in reducing ITS infrastructure costs.

To the extent that ITS does deal with at least some information related to individuals, certain technical privacy safeguards, particularly for ITS communications, will be essential tools for protecting the privacy of ITS users. That is why data security techniques and technologies, such as encryption, designed to secure the privacy of communications will be important technical safeguards for the privacy of ITS users. Other technical strategies, such as automatic data destruction, non-transferability of information about individuals for secondary and tertiary uses, and audit trails reflecting every access to ITS data about individuals, are additional types of technical privacy safeguards. These technical mechanisms for privacy protection might well be required as a matter of industry policy or imposed as legal requirements.

However, technical strategies for safeguarding privacy in ITS raise a number of practical concerns. Consider, for example, an ITS application designed for privacy reasons to operate solely on the basis of user addresses which are both randomly assigned and subject to frequent, random change. In this ITS application toll and transit operations are equipped to remotely deduct vehicle toll charges from "smart" stored-value devices with both "read" and "write" capabilities. Each device is identified only by random transient addresses and is under the sole control of the ITS user. The memory of the smart stored- value device provides the ITS user with detailed records of all of her toll charges and transit fares. But the central ITS system manager, with the capacity only of deducting charges from randomly identified user addresses, can neither collect nor store information about identifiable ITS users or vehicles. Specific vehicles or transit riders identified in traveling from one place to another (for example in calculating tolls or fares based on distance traveled) are only transitorily identifiable and then only by the randomly assigned and changeable address of the "smart" stored value device. The ITS system has no technical capacity for centralized ITS retention of even non-individually-identified trip reports. Since the individual ITS user has sole control over her individual travel data, she has the choice whether to share it with others or not.

Such an ITS system could be designed to restrict the technical capacity of ITS to invade privacy by rendering the ITS infrastructure incapable of collecting, much less retaining, vehicle-specific or traveler-specific data in a form which could be associated with any individual ITS user. The ITS equipment costs to the individual user would be likely to be relatively high in such a system. On the other hand, the infrastructure cost of a limited central ITS management system would be less than the cost of similar central ITS systems with added technical functions designed to collect, store and manipulate information about individuals. The practical privacy provided by

such an ITS system would depend on the physical and electronic security of the individual's "smart" stored-value device.

Industry Standards

In some ways the most appealing of the potential strategies for protecting privacy in ITS is for the ITS industry voluntarily to adopt and to follow privacy principles and standards. In the first part of this issue, Congressman Mineta suggests such an approach in urging adoption of fair information practices through voluntary industry action. Moreover, industry adoption of effective privacy standards might avoid or limit the necessity of imposing privacy requirements by legal mandate. When technologies are relatively new and unfamiliar, as is the case with ITS, industry privacy principles are particularly important in fostering consumer confidence.[76] Since safeguarding privacy in ITS operations will require proper training of ITS personnel to respect the privacy of ITS users and to respond appropriately to privacy concerns, standards and guidelines for effective privacy-protective ITS practices will be essential. The quality of the ITS industry response in terms of privacy principles and standards will be an early and important measure of this new industry's commitment to the interests of the individual ITS user. To the extent that ITS industry privacy standards fall short of the respect for privacy potential ITS users expect and desire, ITS will likely be avoided by potential users and subjected to more restrictive legal safeguards.

Legal Safeguards for Privacy

Even if ITS adopts both excellent technical safeguards and effective industry standards, it is likely that protection for privacy in ITS will also require legal safeguards. Legal requirements mandating ITS privacy safeguards assist in fostering public confidence that ITS industry standards and technical strategies are, in actuality, being followed. Moreover, privacy laws will also provide added assurance that, if ITS interferes with privacy, legal redress is available. The precise contours of legal safeguards for privacy in ITS will be affected by a number of important policy choices, both with regard to ITS operations and with regard to types of privacy protections. In general, there are two very different types of choices regarding legal safeguards for privacy in ITS. First, there are the choices among appropriate legal mechanisms for imposing privacy safeguards. Second, there are choices about the substantive nature of the privacy requirements which should be imposed by law.

With regard to legal mechanisms for imposing privacy safeguards, such protections can be provided at the federal state and local levels. They can be enacted in statutes or promulgated in administrative regulations. Legal privacy safeguards can be enforced by means of administrative sanctions, criminal penalties, civil liability, licensing standards for ITS providers and operators, procurement and contracting requirements, and various other regulatory enforcement mechanisms. Statutes may also authorize individuals to vindicate their own privacy interests by means of civil actions for invasion of privacy. In fact, statutory damage actions for invasion of privacy by ITS might well be enacted to substitute for the uncertainties of potential common law tort liability. However, for those concerned about privacy, civil liability may be problematic because, although damages may deter future privacy invasions, civil liability for invasion of privacy provides only after-the- fact compensation and exacts a price in terms of further publicity

with regard to private matters.

Which level or levels of government should impose legal safeguards for privacy in ITS depends in part on the extent to which ITS is structured as a uniform national system, as opposed to a non-uniform, decentralized pattern of diverse operations varying from state to state and location to location around the United States. Current plans for ITS contemplate an interoperable nationwide system. If a unified national ITS system remains a high priority, then it may be necessary for the federal government, either through Congressional enactment or through promulgation of administrative regulations, to set national privacy standards for ITS which could by statute expressly preempt state privacy laws regulating ITS privacy. In some ways such preemptive federal privacy laws would provide the widest and most uniform reach of privacy protection wherever ITS operates in the United States. However, such a preemptive approach would be controversial unless the federal standards were at least as protective of privacy as the most privacy-protective of the state laws.[77]

In the absence of preemptive federal privacy standards for ITS, state legislatures may well adopt specific privacy laws or standards applicable to ITS operations within their borders. Credit card operations are already subject to such specific legislation. Hawaii[78] and California[79] have for example, enacted state law privacy regulations for credit card operations which might be used as models for ITS privacy law regulations. Moreover, in some states, state public utility regulatory agencies may consider privacy regulations in the course of developing licensing standards or permit criteria for some aspects of ITS, such as toll roads and bridges. Localities may also adopt ordinances requiring local transportation authorities to require ITS operations within their local boundaries to safeguard privacy in various ways. Such varying state and perhaps local ITS privacy requirements may make operation of standardized ITS technologies and a nationally unified, interoperable ITS deployment more difficult. To the extent that ITS policymakers place a high priority on uniform interstate ITS operations, uniformity in state ITS privacy protections and standards will also be a high priority.[80]

Substantively, legal privacy safeguards can encompass many types of legal requirements in responding to various types of privacy concerns about ITS discussed throughout this article. At a minimum, ITS should emphasize individual choice and control over ITS. This type of privacy safeguard would come from legal requirements that ITS users be notified about ITS operations affecting privacy and be given a clear choice whether or not to participate in ITS. Informed and realistic choices regarding ITS will also enhance the sense of personal autonomy which is a part of privacy. However, informing the general public about each ITS application and securing truly informed consent to participation in it, is likely to be an especially challenging task. As is the case with regard to many technologies, ITS is infested with nearly impenetrable and constantly changing acronyms, not to mention obscure technical language, which are frequently understandable only to the most intrepid technophile. Making ITS clear to the ordinary people who will use ITS services will be vital for privacy protection as well as important for acceptance of ITS products and services. The user services approach taken in the National Program Plan for ITS is a wise step in this direction. But average consumers, drivers and transit riders are likely to have significant difficulty figuring out which bundle of the 29 user services is involved in a particular ITS application they might want to consider. Without clear and understandable information, informed consent is not possible. Without informed consent, safeguarding the privacy of individuals using ITS will not occur. Requiring ITS operators to provide each ITS consumer with what is in effect a privacy impact analysis before the consumer decides to use an

ITS service would be a particularly effective legal safeguard for privacy in ITS.

Privacy laws may also require that all ITS providers first establish the need for individually identifiable information about ITS users and then publish privacy statements describing the personal information which the ITS system intends to collect, the reasons for collecting it, how the information will be used and how long it will be kept. Privacy laws may also establish a legal right on the part of each ITS user to access all information about herself collected by ITS providers, as well as the identities of everyone requesting or receiving personal information about her from an ITS system. Privacy laws may further require destruction of individually identifiable information, once the described need for it is satisfied, and, in any event, after the passage of a short specified period of time. Privacy laws could also prohibit compilation by ITS of individual travel profiles and travel histories without the consent of the person involved.

Unless state open records statutes contain clear exemptions for ITS information about individuals, public agencies operating ITS will be required to disclose information about ITS users. As a result, disclosure exemptions for ITS information under the open records statutes in every state and the District of Columbia will need to be enacted to prevent disclosure of ITS information about individuals collected by publicly operated ITS applications. An even better legal protection for the privacy of individuals who use ITS would be legislation providing that all ITS information regarding individuals is confidential and cannot legally be disclosed or used for non-ITS purposes without the consent of the individual or a court order, whether ITS is operated by government agencies, private companies or public-private partnerships.

Warrant requirements for law enforcement access to ITS information about individuals will also be an important issue for ITS privacy law safeguards to address. Law enforcement access to most ITS communications and transaction information relating to individuals already generally requires some type of judicial warrant. A probable cause standard for such judicial warrants would provide better privacy protection than the relevant-to-a-criminal- investigation standard specified under the 1994 amendments to the federal electronic surveillance statutes. Moreover, broader legal requirements for judicial warrants based on probable cause before any type of ITS information is accessed by law enforcement agencies and for notification of access to the individual involved, would offer even better privacy protection.

One aspect of ITS which may affect the feasibility and cost of legal privacy safeguards is whether individually identifiable information about people who use ITS is separated from other ITS information so that special legal requirements and restrictions can apply. Such separation could be required by law or simply part of the structure of ITS. It would be easier for ITS managers to comply with legal privacy safeguards, such as requirements that individually identifiable information cannot be disclosed by an ITS provider without the prior, informed written consent of the individual who is the subject of the information, if individually identifiable information were maintained in a dedicated system or separated from other ITS information in some way. However, in the last analysis, even with multiple privacy laws, industry standards and legally mandated technical safeguards, it will not be possible to perfectly protect privacy once ITS is woven into the surface transportation infrastructure.

VI. Conclusion

No technological privacy fix, nor industry privacy standard, nor legal requirement that privacy must be respected, will completely answer privacy concerns about ITS. Policymakers

considering what to do about privacy and ITS will likely seek to balance privacy against other individual and societal interests in deciding how to respond to privacy concerns. The papers from the Santa Clara Symposium published elsewhere in this issue consider both the privacy concerns and some appropriate responses. As ITS develops into a technological web of information and communication systems tying together surface transportation infrastructure in the United States, many choices about safeguards for privacy in the transportation systems of tomorrow will require further exploration. The simple idea that the future of ITS depends in no small part on proper respect for the privacy of ITS users is a starting point from which to begin to understand some of the relationships which bind together ITS and privacy. Insistence on respect for individuality and personal choice will be among the great benefits which privacy and privacy law will contribute to the successful development and operation of ITS.

APPENDIX

* Professor of Law, Santa Clara University School of Law. B.A. Wellesley College; J.D. Harvard Law School. Professor Glancy directed the Santa Clara Privacy and IVHS Legal Research Project sponsored by the Federal Highway Administration, United States Department of Transportation. The views expressed in this article are those of its author and do not represent the views of the Federal Highway Administration or the United States Department of Transportation.

1. I shall be telling this with a sigh
Somewhere ages and ages hence
Two roads diverged in a wood, and I...
Robert Frost, "The Road Not Taken" (1916).

2. Alexander Solzhenitsyn described such a web of information in depicting bureaucratic recordkeeping in the Soviet Union:

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. ... There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, busses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence.... Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads. Alexander Solzhenitsyn, Cancer Ward (1969).

3. Currently known as Intelligent Transportation Systems, or ITS, the most prominent of these technologies were called Intelligent Vehicle-Highway Systems, or IVHS, during the early 1990s. They had earlier been called "Mobility 2000" and "Smart Highways." In early 1991, Sections 6050 et seq. of the Intermodal Surface Transportation Efficiency Act of 1991 (known as ISTEA, informally pronounced "ice tea") enacted the Intelligent Vehicle-Highway Systems Act of 1991 and established the "IVHS" moniker for the technologies. By 1994, increased emphasis on intermodalism and public transit applications of these advanced surface transportation technologies seemed to require a broader umbrella term for these highly varied transportation technologies. ITS, or Intelligent Transportation Systems, seems to be more clearly inclusive of the range of various types of surface transportation systems which will be parts of ITS, including not only highways but also public transit and other intermodal transportation links. Nevertheless, the many changes in ITS terminology, not to mention technologies, seems to some people to give ITS an almost covert quality, as if these technologies were taking on a intentionally confusing series of multiple personas. Actually, the reason for the change in names has been quite

the contrary - an effort to present the technologies as clearly as possible.

4. From the initiation of the IVHS program in ISTEA, the Congress recognized that privacy was among the "nontechnical constraints" which the intelligent transportation technologies would face. Pub. L. No. 102-240, 105 Stat. 2189, s 6054. The United States Department of Transportation also foresaw that privacy would be an important issue for ITS and has supported privacy research such as the Santa Clara Project. Some of the project's research is reflected in this article and in the materials from the Santa Clara Symposium on Privacy and IVHS presented in this special issue of the Santa Clara Computer and High Technology Law Journal.

5. For example, imagine a parent driving along a highway with a preschool child carefully buckled into her seatbelt. The ITS communications loop is automatically sending data that a small person is in one of the seats. Back comes the following traveler service message: "Hi! This is your old friend Yoggie the Dinosaur. A creamy yogurt cone would be great right now. There is a Yoggie Shoppe at the next exit. What is your favorite flavor? Chocolate? Vanilla? Strawberry? Yoggie's got them ALL! Your pretty green Chrysler Caravan will be welcome at Yoggie's, next exit. NEXT EXIT! I will be looking for you at the next exit." Such a communication might delight the child to whom it is designed to appeal. But it may be considered a gross intrusion by the parent who is driving the car.

6. ITS sometimes refers to using off-the-rack existing components. But most of the available technology, such as missile guidance systems and infrared vision-enhancement devices for jet pilots, must be adapted from defense applications for use in the surface transportation context. Facilitating that adaption to peaceful uses is part of the defense-conversion objective of the ITS program.

7. United States Department of Transportation , National Program Plan for Intelligent Transportation Systems (ITS) (Final Draft, Nov. 1994) at II-5. [hereinafter National Program Plan]

8. ITS contemplates use of read-only cards or tags, read-write devices, and even various versions of stored-value cards and digitized cash.

9. The Automated Highway Systems (AHS) aspects of ITS will develop automatic vehicles which are autonomous of driver control. A major development program is already under way.

10. National Program Plan , supra note 7, at III-2 - III-3.

11. Id. at V- 4 - V- 6.

12. See Dorothy Glancy, The Invention of the Right to Privacy, 21 Ariz. L. Rev. 1 (1979).

13. The development of privacy law is detailed in J. Thomas McCarthy, The Rights of Publicity and Privacy (1987 and supps.) and Sheldon W. Halpern, The Law of Defamation, Privacy, Publicity and "Moral Rights " (1988).

14. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 205 (1890).

15. Id. at 198.

16. Olmstead v. United States, 277 U.S. 438 (1928) (Brandeis, J. dissenting).

17. William Prosser, Privacy, 48 Calif. L. Rev. 383 (1960).

18. Restatement, Second, of Torts , ss 652A - 652I.

19. Alan F. Westin, Privacy and Freedom 7 (1967).

20. Id. at 32.

21. Arthur R. Miller, The Right of Privacy -- A Look through the Kaleidoscope, 46 S.M.U. L. Rev . 37, 38 (1992).

22. Paul Freund, Privacy: One Concept or Many, Nomos XIII: Privacy 182, 198 (1971).

23. Id. at 197.

24. Sam J. Ervin, The Computer vs. Our Constitution, 1 Barrister 14, 16 (1974).

25. See Lawrence Tribe, The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier, First Conference on Computers, Freedom & Privacy (James Warren ed. 1991) and Steven Bercu, Toward Universal Surveillance in an Information Age Economy: Can we Handle Treasury's New Police Technology? 34 Jurimetrics J . 383 (1994).

26. See also Edward Bloustein, Privacy as an Aspect of Human Dignity, 39 N.Y.U. L. Rev . 962 (1964); Charles Fried, Privacy, 77 Yale L. J. 475 (1968). In contrast, those who have suggested that individual privacy can and should be managed may have forgotten the old-fashioned privacy demand from the bygone era of punch-cards: "Do not fold, spindle or mutilate" people.

27. The conversations reflected here took place between February and September of 1994, at a time when ITS technologies were known as IVHS. Although the questions and comments were in terms of IVHS, the nature of the privacy concerns expressed was not affected by the change in acronym.

28. In fact only two, of the twenty-nine, ITS user services have law enforcement ramifications. They are emissions testing and commercial vehicle operations.

29. Professor Reiman's, Driving to the Panopticon, supra at , discusses this troubling sense of being a potential target.

30. 116 U.S. 616, 635 (1886).

31. IVHS Architecture Development Program Interim Status Report (Ap. 1994) and ITS Architecture Development Program Phase I Summary Report (Nov. 1994).

32. E.g. , Catharine MacKinnon insists that "For women the measure of the intimacy has been the measure of the oppression. This is why feminism has had to explode the private. This is why feminism has seen the personal as the political. The private is public for those for whom the personal is political. In this sense, for women there is no private, either normatively or empirically." Catherine A. MacKinnon, Toward a Feminist Theory of the State 191 (1989).

33. Ruth Gavison, Feminism and the Public/Private Distinction, 45 Stan. L. Rev . 1 (1992).

34. See discussion, supra at notes 28 -31.

35. Pub. L. No. 102-240, 105 Stat. 2189, s 6054.

36. The aspect of privacy law which deals with protection for intimate choices related to such matters as childbearing is just about the only area of privacy law not potentially applicable to one aspect or another of ITS. Privacy rights regarding these intimate choices are generally associated with the United States Supreme Court decision in Roe v. Wade, 410 U.S. 113 (1973).

37. See James Gleick, Chaos: Making a New Science (1987).

38. Paul v. Davis, 424 U.S. 693, 713 (1976).

39. Arthur R. Miller, The Assault on Privacy 169 (1971).

40. Ettore v. Philco Telev. Broad. Corp., 229 F.2d 481, 485 (3d Cir. 1956).

41. See text, infra, at notes 12 -26.

42. See text, infra, at notes 6 - 11.

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

44. See Robert Weisberg, IVHS, Legal Privacy and the Legacy of Dr. Faustus, supra.

45. See Richard A. Epstein, Unconstitutional Conditions, State Power and the Limits of Consent, 102 Harv. L. Rev . 5 (1987) and Kathleen M. Sullivan, Unconstitutional Conditions, 102 Harv. L. Rev . 1415 (1987). Professor Epstein further explored the parameters of unconstitutional conditions doctrines in Bargaining With the State (1993).

46. 18 U.S.C. s 2510.

47. Pub. L. No. 103 - 414, 108 Stat. 4279 (1994).

48. Id. ss 201, 107.

49. Pub. L. No. 103 - 414, 108 Stat. 4279 s 207 (1994), amending 18 U.S.C. 2703(d).

50. H.R. Rep. No . 827, 103d Cong., 2d Sess., at 31-32 (1994).

51. H.R. Rep. No. 827, 103d Cong., 2d Sess., at 10 (1994).

52. H.R. Rep. No . 827, 103d Cong., 2d Sess., at 9 (1994).

53. Pub. L. No. 103 - 414, 108 Stat. 4279 s 202 (1994).

54. Pub. L. No. 103 - 414, 108 Stat. 4279 ss 203, 204 (1994).

55. H.R. Rep. No. 827, 103d Cong., 2d Sess., at 31 (1994).

56. Pub. L. No. 103 - 414, 108 Stat. 4279 s 204 (1994).

57. Pub. L. No. 103 - 414, 108 Stat. 4279 s 206 (1994).

58. 12 U.S.C. s 3401.

59. 15 U.S.C. s 1681, regs. at 16 C.F.R. s 600.

60. 15 U.S.C. s 1666.

61. 12 U.S.C. s 1692.

62. Pub. L. No. 103 -322 , 108 Stat. 2094 (1994).

63. 5 U.S.C. s 552.

64. See U.S. Dept of Defense v. F.L.R.A., 114 S. Ct.. 1006 (1994). In this Freedom of Information Act case, the United States Supreme Court split sharply over whether disclosure of the names and addresses of federal employees who were not labor union

members to union organizers would invade privacy protected under the FOIA. Justice Thomas' opinion for the court found that release of federal employees' home addresses to labor union organizers would constitute a clearly unwarranted invasion of privacy. He wrote: "An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form." Id. at 1015.

65. 5 U.S.C. s 552a.

66. These provisions are also found at 5 U.S.C. s 552a.

67. These states include Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and West Virginia.

68. California v. Greenwood, 486 U.S. 35 (1988). The states which have adopted a contrary view as a matter of state constitutional law are California, Hawaii, New Jersey, Washington and perhaps Indiana, where the intermediate appellate courts are divided on the issue.

69. E.g., California and Arizona are experimenting with ITS programs involving remote infra-red monitoring of tailpipe emissions from "gross polluters."

70. The Supreme Court of Washington has already extended the analogy from trash searches to police use of remote infra-red heat detection to discover an indoor marijuana-growing operation. State v. Young, 867 P.2d 593 (Wash. 1994).

71. Alaska, California, Hawaii, Illinois and Louisiana.

72. One reflection of widespread concern about the types of information which may be contained in some ITS systems is the recently enacted Drivers' Privacy Protection Act supra at note 62, which will at least to some degree restrict the availability of drivers license and motor vehicle registration records maintained by the states. But this statute does not specifically address ITS or the types of information which ITS will collect.

73. See United States Dept. of Defense v. F.L.R.A., 114 S. Ct. 1006 (1994).

74. More detail is provided in the tables in the Appendix to this article.

75. Concerns about individual choice and consent to participation in ITS might still remain, but would be significantly reduced.

76. ITS-America, an ITS industry organization which is also an authorized advisory committee to the Federal Highway Administration, has recognized the importance of ITS privacy principles. The organization is in the process of developing privacy principles for adoption by this industry group.

77. This issue regarding preemption of state privacy laws was a major factor preventing passage of proposed changes to the federal Fair Credit Reporting Act during the 103d Congress. An example of non-preemptive federal law regarding privacy can be found in the federal electronic surveillance laws which have for many years set minimum privacy standards without generally preempting state laws more protective of communications privacy.

78. Haw. Rev. Stat . s 708 - 8105, which prohibits sales of lists of credit card holders.

79. Cal. Civil Code s 1748.12. This state statute requires that "If the credit card issuer discloses marketing information concerning a cardholder to any person, the credit card issuer shall provide a written notice to the cardholder that clearly and conspicuously describes the cardholder's right to prohibit the disclosure to marketers of goods of marketing information concerning the cardholder which discloses the cardholder's identity." Cal. Civ. Code s 1748.12(c).

80. A degree of uniformity among the states with regard to ITS privacy safeguards might be facilitated by adoption of uniform state laws. Unfortunately, the fact that only eleven states have adopted the 1955 Uniform Motor Vehicle Certificate of Title and Anti-theft Act over almost four decades is some evidence that the drafting of a uniform law in the surface transportation area may not necessarily result in actual uniformity of privacy laws among the states. Model ITS privacy legislation is another possibility. But states and localities would have to be persuaded to adopt such model laws or codes in identical or nearly identical form.

APPENDIX

Table A
State Constitutional Privacy Provisions Potentially Applicable to ITS

State	Express Privacy Guarantee	Implied Privacy Right	SEARCH AND SEIZURE		
			Restriction	Plain View Doctrine	Open Fields Doctrine
Alabama			Yes	Follows	Follows
Alaska	Yes*	Yes	Yes	Only provides probable cause for search warrant	Follows
Arizona	Yes		Yes	Follows	Follows
Arkansas		Yes	Yes	Follows	Follows
California	Yes*		Yes	Follows	Follows
Colorado			Yes	Follows	Follows
Connecticut			Yes	Follows	Follows
Delaware			Yes	Follows	Follows (includes roads)
District of Columbia			Yes	Follows	Follows
Florida	Yes		Yes	Follows	Follows
Georgia			Yes	Follows	Follows
Hawaii	Yes*	Yes	Yes	Follows No enhancement	Follows
Idaho			Yes	Follows	Follows
Illinois	Yes*		Yes	Follows	Follows
Indiana			Yes	Follows No enhancement	Follows
Iowa		Perhaps	Yes	Follows	Follows
Kansas			Yes	Follows	Follows
Kentucky			Yes	Follows Enhancement OK	Follows
Louisiana	Yes*		Yes	Follows	Follows
Maine			Yes	Follows	Follows
Maryland			Yes	Follows	Follows
Massachusetts			Yes	Follows	Follows
Michigan			Yes	Follows	Follows
Minnesota			Yes	Follows	Follows

* Indicates state constitutional privacy rights against non-governmental interferences with privacy, as well as invasions of privacy by government.

Table A Cont. - State Constitutional Privacy Provisions Potentially Applicable to ITS

State	Express Privacy Guarantee	Implied Privacy Right	SEARCH AND SEIZURE		
			Restriction	Plain View Doctrine	Open Fields Doctrine
Mississippi			Yes	Follows	
Missouri			Yes	Follows	
Montana	Yes		Yes	Follows Enhancement OK	Follows
Nebraska			Yes	Follows	Follows
Nevada			Yes	Follows	Follows
New Hampshire		Yes	Yes	Follows	Follows
New Jersey		Yes	Yes	Follows	Follows
New Mexico			Yes	Follows	Follows
New York			Yes	Follows	Follows
North Carolina			Yes	Follows	Follows
North Dakota			Yes	Follows	Follows
Ohio			Yes	Follows	Follows
Oklahoma			Yes	Follows Enhancement OK	Follows
Oregon			Yes	Follows	Follows
Pennsylvania			Yes	Follows	Follows
Rhode Island			Yes	Follows	Follows
South Carolina	Yes		Yes	Follows	
South Dakota			Yes	Follows	Follows
Tennessee			Yes	Follows	Limited
Texas			Yes	Follows	Follows
Utah			Yes	Limited	Follows
Vermont			Yes	Follows	Follows
Virginia			Yes	Follows	Follows
Washington			Yes	Follows	Follows
West Virginia	Yes		Yes	Follows	Follows
Wisconsin			Yes	Follows	Follows
Wyoming			Yes	Follows	Follows

* Indicates state constitutional privacy rights against non-governmental interferences with privacy,

as well as invasions of privacy by government.

Table B
State Surveillance Laws Potentially Applicable to ITS

State	Consti-tutional Restriction	Search & Seizure Statute	Electronic Surveillance Statute	Vehicle Searches & Seizures	Employee Monitoring Restrictions
Alabama	Yes		Yes Tracking OK		
Alaska	Yes	Yes	Yes Tracking OK	Vehicle exterior no or reduced privacy	Perhaps
Arizona	Yes		Yes Infrared OK	DUI roadblocks OK	
Arkansas	Yes		Yes		
California	Yes		Yes Tracking OK		
Colorado	Yes		Yes		
Connecticut	Yes		Yes	Restricted	Certain areas protected
Delaware	Yes				Employee Bill of Rights
District of Columbia	US Constitution				Employee Bill of Rights
Florida	Yes		Yes Tracking OK		
Georgia	Yes		Yes - Tracking requires warrant		
Hawaii	Yes		Yes		Certain areas protected
Idaho	Yes		Yes		
Illinois	Yes		Yes		
Indiana	Yes		Yes	Vehicle exterior no or reduced privacy	
Iowa	Yes		Yes		
Kansas	Yes		Yes - Includes photography	Vehicle exterior no or reduced privacy	
Kentucky	Yes		Yes - Tracking OK if consent	Vehicle exterior no or reduced privacy	
Louisiana	Yes		Yes	DWI roadblock is a seizure	
Maine	Yes		Yes	Exterior VIN inspection OK	Substance abuse testing

Table B Cont. - State Surveillance Laws Potentially Applicable to ITS

State	Consti-tutional Restriction	Search & Seizure Statute	Electronic Surveillance Statute	Vehicle Searches & Seizures	Employee Monitoring Restrictions
Maryland	Yes		Yes		
Massachusetts	Yes		Yes	Vehicle exterior no or reduced privacy	
Michigan	Yes		Yes	VIN inspection not a search	Monitoring work areas permitted
Minnesota	Yes		Yes - Tracking requires consent or warrant	Vehicle exterior no or reduced privacy	
Mississippi	Yes		Yes	Vehicle exterior no or reduced privacy	
Missouri	Yes		Yes		
Montana	Yes		Yes		Substance abuse testing
Nebraska	Yes		Yes	Statute permits stop for registration check	Yes
Nevada	Yes		Yes		
New Hampshire	Yes		Yes	Car detention is seizure	
New Jersey	Yes		Yes	Vehicle exterior no or reduced privacy	
New Mexico	Yes			VIN inspection is not a search	Yes
New York	Yes		Yes Tracking OK	Vehicle exterior no or reduced privacy	Yes
North Carolina	Yes		Yes		
North Dakota	Yes				
Ohio	Yes		Yes	Vehicle exterior no or reduced privacy	
Oklahoma	Yes		Yes Tracking OK		Yes
Oregon	Yes		Yes	Vehicle exterior no or reduced privacy	
Pennsylvania	Yes		Yes - Tracking OK on public roads	Vehicle exterior no or reduced privacy	
Rhode Island	Yes		Yes	DUI roadblocks invade privacy	
South Carolina	Yes		Yes		

Table B Cont. - State Surveillance Laws Potentially Applicable to ITS

State	Consti-tutional Restriction	Search & Seizure Statute	Electronic Surveillance Statute	Vehicle Searches & Seizures	Employee Monitoring Restrictions
South Dakota	Yes		Eavesdropping includes visual surveillance	Reduced expectation of privacy in vehicles on highways	
Tennessee	Yes				
Texas	Yes			Vehicle exterior no or reduced privacy	
Utah	Yes		Yes Video surveillance OK	Vehicle exterior no or reduced privacy	
Vermont	Yes		Yes	Vehicle exterior no or reduced privacy	
Virginia	Yes		Yes	Vehicle exterior no or reduced privacy	
Washington	Yes		Yes - Electronic speed monitoring OK	Vehicle stops OK	
West Virginia	Yes		Yes	Vehicle exterior no or reduced privacy	
Wisconsin	Yes		Yes		
Wyoming	Yes		Yes - Tracking OK		

Table C
State Statutes Affecting Privacy in Government Information Systems Potentially Applicable to ITS

State	PUBLIC RECORDS		Vehicle &	Vehicle ID	PRIVACY
	Statutory Requirement	Privacy Exemption	Driver Records	Number Registration	ACT
Alabama	Open			Yes*	
Alaska	Open	Yes	Open	Yes	Yes
Arizona	Open	Yes	Open	Yes	
Arkansas	Open		Open	Yes	
California	Open	Yes	Restricted	Yes	Yes
Colorado	Open	Yes - no use for solicitation		Yes	Yes
Connecticut	Open	Yes	Open	Yes*	
Delaware	Open	Yes	Restricted	Yes	
District of Columbia	Open	Yes			
Florida	Open	Yes	Open	Yes	Yes
Georgia	Open	Yes	Confidential	Yes*	
Hawaii	Open	Yes	Traffic offenses open	Yes	Yes
Idaho	Open	Yes		Yes	Yes No sales of mailing lists
Illinois	Open		Sales of DMV records OK	Yes	Insurance Information
Indiana	Open	Yes if record confidential	Open		Yes Fair Info. Practices
Iowa	Open	Yes Limited	Open	Yes	Yes Fair Info. Practices
Kansas	Open	Perhaps - no use for commercial purposes		Yes	
Kentucky	Open	Yes	Open		
Louisiana	Open	Yes	Open	Yes	

* Indicates adoption of the Uniform Motor Vehicle Certificate of Title and Anti-theft Act (1955).

Table C Cont. - State Statutes Affecting Privacy in Government Information Systems Potentially Applicable to ITS

State	PUBLIC RECORDS		Vehicle &	Vehicle ID	PRIVACY
	Statutory Requirement	Privacy Exemption	Driver Records	Number Registration	ACT
Maine	Open		Open	Yes*	Yes
Maryland	Open	Yes		Yes	Yes Damages for improper disclosure
Massachusetts	Open		Restricted	Yes*	Yes
Michigan	Open	Yes	Open	Yes	
Minnesota	Open	By agency classification	Restricted	Yes*	
Mississippi	Open - must identify interest	Yes	Show need to access	Yes*	Yes
Missouri	Open		Open	Yes	
Montana	Open	Yes	Open		Yes
Nebraska	Open		Open Copies on request	Yes	
Nevada	Open		Open	Yes	
New Hampshire	Open	Limited		Yes*	
New Jersey	Open				
New Mexico	Open				Yes
New York	Open	Yes		Yes*	Yes
North Carolina	Open				
North Dakota	Open		Open		
Ohio	Open		Open	Yes	Yes
Oklahoma	Open	Yes	Confidential		Yes
Oregon	Open	Yes	Open - on request. No sales		
Pennsylvania	Open	Yes	Closed unless consent	Yes	
Rhode Island	Open	Yes		Yes*	Yes Commercial use of public records illegal

* Indicates adoption of the Uniform Motor Vehicle Certificate of Title and Anti-theft Act (1955).

Table C Cont. - State Statutes Affecting Privacy in Government Information Systems Potentially Applicable to ITS

State	PUBLIC RECORDS		Vehicle & Driver Records	Vehicle ID Number Registration	PRIVACY ACT
	Statutory Requirement	Privacy Exemption			
South Carolina	Open	Yes	Confidential	Yes	
South Dakota	Open	Discretionary			
Tennessee	Open	Yes			Yes
Texas	Open		Open		
Utah	Open	Yes	Open on request		Yes
Vermont	Open	Yes	Open	Yes*	
Virginia	Open	Yes	Open	Yes	Yes
Washington	Open	Yes	Open no business solicitation		Yes
West Virginia	Open	Yes	Open on request		
Wisconsin	Open	Yes	Open	Yes	Yes Privacy Council
Wyoming	Open	Yes Narrow	Open	Yes	

* Indicates adoption of the Uniform Motor Vehicle Certificate of Title and Anti-theft Act (1955).

Table D
State Statutes Regulating Private Sector Interferences with Privacy Potentially Applicable to ITS

State	General Privacy Statute	Unauthorized Access to Computerized Data Prohibited	Consumer Credit Information	Financial Information	Employee Records
Alabama		Yes		Yes	
Alaska		Yes	Yes	Yes	Yes
Arizona		Yes	Yes	Yes	
Arkansas		Yes			Yes
California	Yes stalking statute	Yes	Yes Sale of credit card info. restricted	Yes	
Colorado	Yes stalking statute	Yes		Yes	
Connecticut		Yes		Yes Utility billing	Yes
Delaware	Yes	Yes	Yes		Yes
District of Columbia		Yes			Yes
Florida		Yes			
Georgia		Yes			
Hawaii		Yes	Yes Sale of credit card info. restricted		
Idaho	Yes stalking statute	Yes			
Illinois		Yes	Yes	Insurance Information	Yes
Indiana	Yes stalking statute	Yes			
Iowa		Yes		Yes EFT privacy	
Kansas	Yes	Yes	Yes		
Kentucky	Yes - harassing communications and stalking statute	Yes	Yes	Yes	
Louisiana	Yes stalking statute	Yes	Yes	Yes	
Maine	Yes - telephone	Yes	Yes	Yes	

Table D Cont. - State Statutes Regulating Private Sector Interferences with Privacy Potentially Applicable to ITS

State	General Privacy Statute	Unauthorized Access to Computerized Data Prohibited	Consumer Credit Information	Financial Information	Employee Records
Maryland	Yes stalking statute	Yes	Yes Willful disclosure criminal	Yes Willful disclosure criminal	
Massachusetts		Yes	Yes		Yes
Michigan	Yes stalking statute	Yes	Yes	Yes	
Minnesota	Yes stalking statute	Yes	Yes	Yes - ATM records protected	
Mississippi		Yes		Yes	
Missouri		Yes		Yes	
Montana		Yes	Yes	Yes - EFT privacy protected	
Nebraska	Yes stalking statute	Yes	Yes		
Nevada	Yes stalking statute	Yes	Yes	Yes	
New Hampshire		Yes	Yes		
New Jersey		Yes	Yes		
New Mexico	Yes	Yes		Yes	
New York	Yes	Yes	Yes		
North Carolina		Yes		Yes	Yes
North Dakota		Yes		Yes	
Ohio	Yes stalking statute	Yes	Yes	Yes	
Oklahoma		Yes	Yes	Yes	
Oregon	Yes stalking statute	Yes	Yes	Yes	
Pennsylvania	Yes stalking statute	Yes		Yes	
Rhode Island	Yes	Yes	Yes		

Table D Cont. - State Statutes Regulating Private Sector Interferences with Privacy Potentially Applicable to ITS

State	General Privacy Statute	Unauthorized Access to Computerized Data Prohibited	Consumer Credit Information	Financial Information	Employee Records
South Carolina	Yes stalking statute	Yes		Yes	
South Dakota		Yes			
Tennessee		Yes	Yes	Yes	
Texas		Yes			
Utah		Yes		Yes	
Vermont	Yes stalking statute		Yes		
Virginia		Yes	Yes	Yes	
Washington		Yes	Yes		
West Virginia	Yes stalking statute	Yes			
Wisconsin	Yes stalking statute	Yes	Yes		Yes
Wyoming	Yes stalking statute	Yes			

Table E
Invasion of Privacy Damage Actions Potentially Applicable to ITS

State	Common Law Tort	Statutory Damage Action	Appro-priation Tort recognized	False Light Tort recognized	Intrusion Tort recognized	Public Disclosure Tort recognized
Alabama	Yes		Yes	Yes	Yes	Yes
Alaska	Yes				Yes	
Arizona	Yes			Yes		Yes
Arkansas	Yes		Yes	Yes	Yes	Yes
California	Yes	Yes	Yes	Yes	Yes	Yes
Colorado	Yes					
Connecticut	Yes		Yes	Yes	Yes	Yes
Delaware	Yes	Yes	Yes	Yes	Yes	Yes
District of Columbia	Yes		Yes	Yes	Yes	Yes
Florida	Yes	Yes	Yes	Yes	Yes	Yes
Georgia	Yes		Yes	Yes	Yes	Yes
Hawaii	Yes	Yes	Yes	Yes	Yes	Yes
Idaho	Yes		Yes	Yes	Yes	Yes
Illinois	Yes		Probably	Probably	Probably	Probably
Indiana	Yes	Yes	Yes	Yes	Yes	Yes
Iowa	Yes		Yes	Yes	Yes	Yes
Kansas	Yes	Yes	Yes	Yes	Yes	Yes
Kentucky	Yes	Yes	Yes	Yes	Yes	Yes
Louisiana	Yes		Yes	Yes	Yes	Yes
Maine	Yes - Narrow		Yes	Yes		Yes
Maryland	Yes		Yes	Yes	Yes	Yes
Massachusetts	Yes	Yes		Disapproved		
Michigan	Yes					
Minnesota	Disapproved		Disapproved	Disapproved	Disapproved	Disapproved
Mississippi	Yes		Yes	Yes	Yes	Yes

Table E Cont. - Invasion of Privacy Damage Actions Potentially Applicable to ITS

State	Common Law Tort	Statutory Damage Action	Appro-priation Tort recognized	False Light Tort recognized	Intrusion Tort recognized	Public Disclosure Tort recognized
Missouri	Yes		Yes	Perhaps not	Yes	Yes
Montana	Yes			Yes		
Nebraska	Yes - Restatement Disapproved	Yes	Yes	Yes	Yes	
Nevada	Yes		Yes	Yes	Yes	Yes
New Hampshire	Yes				Yes	
New Jersey	Yes		Yes	Yes	Yes	Yes
New Mexico	Yes		Yes	Yes	Yes	Yes
New York	Yes - Restatement Disapproved	Yes	Yes			
North Carolina	Yes		Yes	Yes	Yes	Yes
North Dakota	Restatement Disapproved					
Ohio	Yes		Yes	Perhaps not	Yes	Yes
Oklahoma	Yes	Yes	Yes	Yes	Yes	Yes
Oregon	Yes		Yes	Yes	Yes	Yes
Pennsylvania	Yes		Yes	Yes	Yes	Yes
Rhode Island		Yes	Yes	Yes	Yes	Yes
South Carolina	Yes		Yes		Yes	Yes
South Dakota	Yes		Yes	Yes	Yes	Yes
Tennessee	Yes		Yes			
Texas	Yes					Yes
Utah	Yes		Yes	Yes	Yes	Yes
Vermont	Yes		Yes		Yes	Yes
Virginia	Yes	Yes	Yes			Yes
Washington	Yes	Yes	Yes	Yes	Yes	Yes
West Virginia	Yes		Yes	Yes	Yes	Yes
Wisconsin		Yes	Yes		Yes	Yes
Wyoming	Uncertain					

"Restatement"	Refers to the four damage actions for invasion of privacy described in the Restatement, Second, of Torts, Sections 652A - 652I.

State Privacy Law Potentially Applicable to IVHS