Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
SWUTC/00/472840-00075-1		

4. Title and Subtitle	5. Report Date
The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data	May 2000
	6. Performing Organization Code
7. Author(s) Valerie Briggs, C. Michael Walton	8. Performing Organization Report No. Research Report 472840-00075
9. Performing Organization Name and Address Center for Transportation Research University of Texas at Austin 3208 Red River, Suite 200 Austin, Texas 78705-2650	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. DTRS95-G0006
12. Sponsoring Agency Name and Address Southwest Region University Transportation Center Texas Transportation Institute The Texas A&M University System College Station, Texas 77843-3135	13. Type of Report and Period Covered
	14. Sponsoring Agency Code

15. Supplementary Notes

Supported by a grant from the U.S. Department of Transportation, University Transportation Centers Program

16. Abstract

The purpose of this report is to develop appropriate guidelines and institutional models for the management of sensitive data collected through intelligent transportation systems (ITS). This task is performed through the examination of current regulations, policies, and practices regarding sensitive ITS data and through receipt and characterization of input from data users and stakeholders. ITS applications and technologies that raise privacy concerns are defined as those that potentially enable the identification or singling out of a specific vehicle or occupant. Both current and emerging technologies that have this capability are identified. An in-depth analysis of electronic clearance and electronic toll collection systems, ITS applications with established track records in dealing with privacy issues, reveals appropriate practices and identifies potential stumbling blocks in the collection, storage and distribution of sensitive data. Recommendations of data handling practices are made based on these findings. Potential secondary users and uses of sensitive ITS data are identified through a survey of professionals in the ITS industry. This is followed by a discussion of forums for sharing data without compromising data confidentiality. The conclusion establishes public and private roles and responsibilities for data handling and identifies opportunities for partnerships.

17. Key Words	18. Distribution Statement
Archived Data User Service (ADUS), Privacy, Electronic Toll Collection, Electronic Clearance, Legal Issues, ITS, Partnerships, Public-Private	No Restrictions. This document is available to the public through NTIS: National Technical Information Service 5285 Port Royal Road Springfield, Virginia 22161

19. Security Classif.(of this report)	20. Security Classif.(of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	183	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data

by

Valerie Annette Briggs
C. Michael Walton

Research Report SWUTC/00/472840-00075-1

Combined final report for the following two SWUTC projects:
Trends and Issues in Public Private Partnerships – 472840-00075
&
The Implications of Data Usage and Privacy of ITS – 167810

Southwest Regional University Transportation Center
Center for Transportation Research
The University of Texas at Austin
Austin, Texas 78712

MAY 2000

DISCLAIMER

ACKNOWLEDGMENT

Support for this report was provided by a grant from the U.S. Department of Transportation, University Transportation Centers Program to the Southwest Region University Transportation Center.

EXECUTIVE SUMMARY

Intelligent transportation systems (ITS) have the ability to collect vast amounts of information pertaining to transportation. This includes potentially sensitive information about specific individuals and businesses. With this capability comes the responsibility to use this information for socially acceptable purposes and to protect individuals' and businesses' private information. ITS data often have value to multiple public sector and private sector groups. Thus, in order to derive maximum benefit from ITS data, system managers must find ways to safeguard private information without compromising the potential value of those data. Policies pertaining to data usage and dissemination to outside organizations are important to ensure that data are not used inappropriately.

This report examines current regulations, policies, and practices pertaining to sensitive ITS data in order to develop guidelines and institutional models for the management of these data. The primary findings are as follows:

- U.S. and state laws do not adequately address privacy issues in ITS. ITS implementing organizations have the primary responsibility for protecting user privacy. ITS America's Privacy Principles may serve as a guide to organizations in this effort.
- Privacy protection must be balanced with the value of sharing or using ITS data for multiple purposes. Data sharing arrangements must build in privacy protections.
- Public perceptions and levels of trust are important determinants in the success of ITS data collectors and service providers.
- Both the public and private sector can provide adequate privacy protection for ITS services in most cases. However, each sector has different areas of strengths and weaknesses.
- Data infomediaries can mitigate risks associated with dissemination of sensitive information, assemble data from multiple sources, and provide these data in usable forms. Infomediaries can be public or private and should reflect the type of data collected and the purpose for which the data will be used.

ABSTRACT

The purpose of this report is to develop appropriate guidelines and institutional models for the management of sensitive data collected through intelligent transportation systems (ITS). This task is performed through the examination of current regulations, policies, and practices regarding sensitive ITS data and through receipt and characterization of input from data users and stakeholders. ITS applications and technologies that raise privacy concerns are defined as those that potentially enable the identification or singling out of a specific vehicle or occupant. Both current and emerging technologies that have this capability are identified. An in-depth analysis of electronic clearance and electronic toll collection systems, ITS applications with established track records in dealing with privacy issues, reveals appropriate practices and identifies potential stumbling blocks in the collection, storage and distribution of sensitive data. Recommendations of data handling practices are made based on these findings. Potential secondary users and uses of sensitive ITS data are identified through a survey of professionals in the ITS industry. This is followed by a discussion of forums for sharing data without compromising data confidentiality. The conclusion establishes public and private roles and responsibilities for data handling and identifies opportunities for partnerships.

Table of Contents

List of Tables

Chapter 1. Introduction

Intelligent transportation systems (ITS) have the ability to collect vast amounts of information pertaining to transportation. This includes potentially sensitive information about specific individuals and businesses. With this capability comes the responsibility to use this information for socially acceptable purposes and to protecting individuals' and businesses' private information. ITS data often have value to multiple public sector and private sector groups. Thus, in order to derive maximum benefit from ITS data, system managers must find ways to safeguard private information without compromising the potential value of those data. Policies pertaining to data usage and dissemination to outside organizations are important to ensure that data are not used inappropriately.

While there has been significant research into ITS data collection mechanisms, there has been relatively little study of how sensitive information is being stored, disseminated, and used and the policies that govern these activities. The purpose of this thesis is to address this shortcoming by examining current policies and practices regarding sensitive ITS data and characterizing input from data users and stakeholders in order to develop appropriate guidelines and models for the management of sensitive ITS data. Particular attention is given to the privacy implications related to sharing information between the public and private sectors and the potential role of public-private partnerships in data management.

OBJECTIVES

This research has the following objectives:

- Define privacy concerns related to ITS technologies;
- Identify potentially privacy invasive ITS technologies and applications;
- Document existing regulations, policies, and guidelines addressing the issues of privacy considerations and rights to information collected in ITS processes;
- Discuss current practices in the collection, storage, and dissemination of sensitive information collected in ITS processes;
- Determine potential uses of sensitive data collected via ITS;

- Outline organizational models for the treatment of sensitive data; and
- Recommend public and private roles and responsibilities in the treatment of data and opportunities for partnership.

BACKGROUND

ITS technologies enable the collection, processing, and storage of transportation related data. These data are valuable to both the public and the private sectors. The public sector uses transportation data in its roles as manager of the transportation infrastructure and protector of public safety. The data have both real-time value, in that it can be used to detect and react to problems in the transportation network, and long-term value for determining system performance and for planning. Today the public sector uses ITS data for management, administration, operations, and regulatory purposes. These include detecting incidents and automatically dispatching emergency response units, adjusting traffic signals in real time to the flow of traffic, informing travelers of traffic conditions, automatically collecting toll and fare payments, electronically checking for regulatory compliance of commercial vehicles, and much more. The same data are valuable to private companies that add value and repackage data for direct sales and for product and service enhancements. For instance, some companies use ITS data to provide traveler information and traffic reports to the public via the internet, radio, cable television, and personal devices such as pagers and watches. Profits are made through advertising or from fees or subscriptions. [1]

ITS involve two forms of data. There are data collected and stored for use in ITS processes. For example, commercial vehicle licensing, permitting, and safety records are stored for use in electronic clearance at inspection stations. Personal financial information is stored for use in electronic toll collection systems. The second type of data are those collected by the ITS system, including traffic counts, accident records, usage statistics, and video images.

Several issues arise over the collection and storage of these data. First, there is the issue of protection and privacy of data. The data collector must be able to ensure that personal and proprietary data are safe from sabotage or improper use.[2] This involves such security mechanisms as data encryption and access protection.[3] Second, there is a

question of what data should be collected and how it should be used. While ITS enable the collection of many types of data, some forms could infringe on public rights or involve the collector in litigation. For instance, some individuals and trucking industry personnel fear that ITS may be used to track their vehicle's movements without their permission.[4] Additionally, video data used for traffic monitoring are often sought for use in accident litigation. Therefore, ITS generally do not record video data, so the collector does not become entangled in outside litigation.[5]

In light of these issues, there are questions about what groups should be allowed to collect or have access to certain types of data. Those groups with access to data must be able to ensure that it is properly stored and used. Depending on the nature of the data and established precedence, it is sometimes the public sector that is more trusted with data and sometimes the private sector. For example, criminal records are entrusted to the public sector, whereas financial records are the domain of the private sector. When data are transferred between one organization and another or shared among organizations, the practices of one group could potentially affect the credibility of others. Thus, partnership arrangements are affected by data policies. Furthermore, ITS data have value. Determining the value of the data and who should pay for their collection and use, the general public or specific beneficiaries, have significant implications for public-private partnerships and business structures of organizations that provide ITS.

Thus, perceptions and policies related to data value, privacy, and use can significantly impact ITS. They determine appropriate roles for the public and private sectors as well as the potential for partnerships. Different approaches are taken to these issues in ITS programs across the country, resulting in a number of different institutional models. Studying these models can lead to insights for emerging and future ITS efforts.

METHODOLOGY

Research was conducted through a literature search and through interviews with key personnel in the ITS industry. A literature review was conducted to assess (1) issues of concern to privacy advocate groups about ITS data collection and information management practices and (2) U.S. and state privacy laws, court decisions, and transportation industry guidelines that may affect these practices. In particular, articles

discussing privacy issues and laws, guidelines and reports published by ITS America and the U.S. Department of Transportation (DOT), and written policies of individual organizations, were included in the study.

Telephone interviews were conducted with over 60 professionals in the ITS industry to determine (1) current practices in the collection and management of sensitive information within the ITS community, (2) potential uses and users of sensitive information obtained through ITS, and (3) appropriate practices for distributing or sharing information. The majority of interviews were conducted as part of one of three surveys. Survey A was administered to operators of electronic toll collection systems to determine information management practices and policies. Survey B was a similar survey directed at electronic clearance organizations. The third survey, survey C, was conducted of key personnel in the ITS industry and leaders in the Archived Data User Services activities to predict potential markets for information derived through ITS, evaluate current privacy practices, and assess methods of distributing and sharing information. Participants in survey C included personnel from

- university-based research institutes,
- transportation consulting firms,
- private vendors of transportation services and products,
- associations representing the telecommunications, trucking, and ITS industries,
- the U.S. Department of Transportation, and
- state departments of transportation.

A similar set of questions was administered to participants in each of the three survey groups. Copies of the three survey questionnaires are included in appendices A, B, and C. Additional questions were asked of certain vendors of transportation services and products to assess their interest in using sensitive information collected through ITS or new technologies that have implications for privacy. Some were also asked about their companies' information privacy policies. Appendix D contains a complete list of survey and interview participants.

DEFINITION OF TERMS

Some discussion of terminology is warranted to clarify wording used in the report and to define technical terms.

The term *sensitive information* is used throughout the report to refer to information that some individuals or businesses consider private and may not want to disclose to the public. The terms *personal information*, *confidential information*, and *proprietary information* have similar meanings and are used interchangeably in the report.

Intelligent transportation systems (ITS) comprise a number of technologies, including information processing, communications, control, and electronics, that can be applied to vehicles and transportation infrastructure to improve efficiency, safety, and ease of travel in the movement of passengers and goods. Applications of ITS are formally referred to as user services. ITS user services and technologies are defined as they are discussed within the text of the report.

ITS for Commercial Vehicle Operations (ITS/CVO) refer to a category of ITS user services that are applied to commercial vehicle transportation to improve safety and efficiency. Commercial vehicles include trucks, buses, emergency vehicles, maintenance and construction vehicles, and other heavy vehicles.

The *National ITS Architecture* provides a common structure for the design of ITS nationwide. It provides guidance to ensure compatibility and interoperability of multiple ITS products and services. The Architecture is maintained by the Federal Highway Administration and is updated periodically.

The *Archived Data User Service (ADUS)* is an element of the National ITS Architecture that provides a framework in which transportation information collected by ITS can be archived and made available to a wide variety of stakeholders.

The *Intermodal Surface Transportation Efficiency Act (ISTEA)* is the federal legislation passed in 1991 that outlined surface transportation policy and programs through 1998.

ORGANIZATION OF THE REPORT

Chapter 2 lays the foundation for a discussion of privacy issues in ITS. Its purpose is to convey who privacy advocates are, what they are concerned about, and what specific technologies concern them or may potentially concern them. The first section introduces and defines issues that are of primary concern to privacy advocates. This is followed by a section that characterizes privacy advocates as both individuals and businesses and cites studies on privacy concerns of the general public. Finally, specific ITS technologies and applications that have implications for privacy are discussed.

Chapter 3 discusses legal and institutional mechanisms that address privacy issues in ITS. Its purpose is to familiarize the reader with what controls currently exist on the collection and use of sensitive information and what impact these controls have. The first section outlines federal and state legislation and court cases deemed as relevant to ITS. The institutional framework section discusses other mechanisms that are commonly used to address privacy concerns. A conclusions section indicates how these controls are being implemented within the ITS community and the shortcomings of these controls. It also recommends a standard of practice for ITS owners and operators.

Chapter 4 provides a detailed profile of electronic clearance systems and electronic toll collection systems, with the goal of communicating what privacy issues have arisen and how they are being addressed in real world applications. A conclusion section presents findings and lessons learned for application to other ITS technologies.

Chapter 5 examines potential needs for and ability to use sensitive information collected via ITS. It first reviews material created for the Archived Data User Service within the National ITS Architecture to identify potential uses and recommended archiving practices for sensitive information. The next section discusses potential uses of sensitive information as identified through a survey of ITS professionals. This is followed by a presentation of forums for sharing and distribution of ITS data. Three hypothetical "models" are identified, and several real world examples are discussed. A conclusions section summarizes the chapter findings and provides a comparison of the models presented.

The final chapter integrates the findings of the previous chapters. It outlines recommendations for organizations collecting sensitive information via ITS or providing

ITS services. It also discusses appropriate roles for the public and private sectors and opportunities for partnerships.

Notes

[1] Smart Trek, *Smart Trek, The Path to Intelligent Travel*, Seattle, Washington (brochure.)
[2] Wright, Tom, "Eyes on the Road, Privacy and ITS," *Traffic Technology International*, (Autumn 1995), pp. 88-93.
[3] U.S. Department of Transportation, Intelligent Transportation Systems Joint Program Office, *Protecting Our Transportation System: An Information Security Awareness Overview*, by Keith Biesecker and Barbara Staples (Washington, D.C., November 1997).
[4] Wright, Tom, "Eyes on the Road."
[55] Texas Department of Transportation, *ITS Data Management System: Year One Activities*, by Shawn M. Turner, et al. (Austin, Texas, August 1997), p. 16.

Chapter 2. Privacy Issues in ITS

Potential privacy issues are raised whenever an ITS application enables the identification or singling out of a specific vehicle or occupant. Applications that do not have this capability raise few, if any, privacy concerns. The extent to which ITS applications may evoke privacy concerns depends on a number of different factors related to what information is collected, how it is stored, and how it is used.

The most important issue with regard to the collection of data is whether ITS have the ability to collect personal information and what this information entails. For instance, does the technology allow the identification of a vehicle? Is this vehicle identification linked to other information, such as the vehicle's owner? Does the technology create a visual identification, such as a video image or photograph? Can the occupants of a vehicle be identified? Does the technology allow for the tracking of a vehicle's movements? Is the collection of information continuous or episodic? Can the same information be collected manually or by an observer, and is this done in practice? Another important privacy issue is whether the individual realizes what information is being collected about him and whether he has any control over the collection of this information. For instance, do notices identify areas that are under surveillance? Can an individual choose whether to participate in an ITS program that collects personal information? Does the individual have the ability to turn off or on a surveillance device within his vehicle?

The generation of records containing personal information is of even greater concern to privacy advocate, because it allows for the retrieval and use of the record's contents for as long as the record exists. Besides the fundamental concern about the contents of a record, several other issues regarding record-keeping also have privacy implications. Privacy advocates want to ensure that records kept are accurate, that individuals know what information is stored about them and that they have the ability to access and correct this information. The length of time a record is stored is a critical issue as well as how easy or difficult it is to access the information. For instance, information placed on the internet for public viewing is likely to elicit a much stronger response from privacy advocates than the same information stored in an archive that is

difficult to access, even if the information is still in the public domain. Along the same line, the configuration of the storage medium is important. For example, is the storage medium, presumably a computer system, centralized or decentralized? Is it networked with other systems? Is it possible to link personal records to those collected in other capacities, such as law enforcement? Who can access the records, both internal and external to the organization? What types of technical and non-technical security mechanisms are in place to prevent tampering with the data or undesired access?

Privacy advocates are also concerned with how collected data are used. Is information used only for the purpose for which it is collected, and is this purpose stated and understood? Is any information collected that is not relevant to the stated purpose? Does the purpose benefit the person about whom the information is collected? What controls govern the ability to use information for secondary purposes or distribute it to outside organizations? For instance, can information be used for other purposes without the express permission of the individual? Do outside organizations have access to the information? What procedures are necessary for law enforcement to access data?[6]

The answers to these questions determine to a large extent what kind of privacy concerns will be raised by an ITS application. It is also important to note that the system design can have important ramifications for privacy. A system can be designed to be privacy sensitive or not. A number of these issues merit further explanation and discussion.

CRITICAL PRIVACY ISSUES

The following critically important privacy issues have been identified in literature and through interviews with individuals and user groups involved with ITS technologies that collect sensitive information.

Anonymous Data Collection

The collection of anonymous information raises few privacy concerns. Therefore, privacy advocates push for the adoption of anonymous data collection systems wherever possible.[7] Data can be made anonymous to varying degrees and at different stages in the process of collecting and storing information. For instance, ITS that use vehicle probes to collect information about traffic flows require the identification of individual vehicles.

However, no information about the vehicle or driver is required. Therefore, many operators devise ways to distribute transponders or other tracking devices anonymously so that there is no record linking an individual to a transponder. Thus, the system becomes anonymous. For applications that do require the use of individualized information, transformation of data later in the process may be possible. For example, some electronic clearance systems periodically purge records of individual transactions and keep only aggregate data. New technologies, such as digital cash, are making it possible to maintain accounts anonymously even for applications that have traditionally required the collection and retention of personal information.[8] Regardless of the application, privacy advocates promote the use of anonymous data at the earliest possible stage of the data collection process.

Aggregate Data Versus Anonymous Data

Aggregating data is one method of making data anonymous. However, there is a distinction between aggregate data and anonymous data. Anonymous data do not identify the specific individual or vehicle about which information is collected. Aggregate data refer to a grouping of data about multiple individuals from which no one individual can be identified. Aggregate data raise even fewer privacy concerns than simply anonymous data. In some applications, anonymous data can still reveal important information that some would deem inappropriate. For instance, detailed information about the activities of a shipper could be very valuable to other shippers even if the identity of the shipper is not known. A shipper would not want this information released. However, aggregate shipping information about many shippers, many commodities and over many routes would not be considered nearly as sensitive.[9] In much of the privacy legislation, aggregate data are treated differently and afforded greater freedom of use than other types of data.

Visual Images

ITS applications that involve visual images often create greater privacy concerns than those that simply identify vehicles. Individuals do not like to feel that they are being watched. These concerns become even greater when visual images enable the identification of a vehicle's occupants. There is fear that if records are kept of such

images, they may be accessed by law enforcement officers, employers, family members or anyone else interested in knowing where a person was and whom they were with at a certain point in time.[10] Applications involving visual surveillance, particularly for traffic law enforcement, have been slow to develop within the United States due to these fears. Principles and standards of operation have been developed by advocacy groups, such as the Security Industry Association and specific operators of technologies involving visual imaging to provide guidelines for appropriate usage of these technologies.

Secondary Uses of Data

Much of the anxiety over the ability to link personal information records stems from concerns about how these information records will be used. Privacy advocates are concerned that their personal information may be distributed and used for purposes they did not approve. They are concerned that the uncontrolled use of these data may burden them, such as in the case of "junk mail," or harm them in some way by restricting their freedoms, holding them to higher standards of law enforcement, or enabling pricing and service discriminations.[11] The privacy community advocates that data be used only for the primary purpose for which they are collected, and many privacy laws address the topic of secondary data uses. Much of this paper is devoted to a discussion of secondary uses of ITS data.

Law Enforcement Access to Data

Secondary uses of data by law enforcement is of special concern to some privacy advocates. There is fear that law enforcement officials may seek to use ITS data for traffic violation enforcement purposes, such as to detect speeding or check driver hour-of-service log books for commercial vehicles. Users of ITS would then be subject to higher standards than other drivers. There is fear that enforcement will become more strict due to the relative cheapness of electronic surveillance methods compared to personal surveillance.[12]

Litigation Involving Data

The potential exists for any record created through ITS to be used in litigation. The record may be used for the benefit or detriment of the record's subject. For instance,

records from vehicle diagnostic technologies on commercial vehicles may be used in an accident case either to prove or to disprove the proper functioning of the vehicle. Records from in-vehicle tracking devices can be used to provide evidence of an individual's location to build a case for or against the individual. Toll agencies report that customer records are commonly subpoenaed for use in marital disputes.[13] The existence of such records and their easy access through subpoena worries some individuals and companies. Some groups fear that data may be misused in court, and the mere existence of additional data may place those that chose to implement ITS at higher risk of suit.[14]

Data Creep

Data creep refers to a tendency for data collected for one purpose to eventually be used for other purposes. A prime example is social security numbers, which were originally created to be confidential identification numbers used only to keep track of old age pensions. Today, social security numbers have become a universal identification number used for many purposes despite some public concerns.[15] There is also a tendency for applications or services that are at introduction voluntary to become almost obligatory over time due to wide-spread use and other services dependency upon them. Credit cards serve as a good example of such an application.

Opt-In Versus Opt-Out Conditions

Legal documents create two conditions that govern the way organizations may share personal information they collect about individuals. The first, opt-out conditions, allows organizations to sell or release individual information for any purposes unless the individual specifically requests that his information not be released. This implies that the organization that collects the information owns it and may use it or profit from it in multiple ways. Opt-out conditions place the burden of protecting personal information on the individual, who must discover what information is being collected about him and make a request that the information not be shared or used for certain purposes. Businesses are not required to inform individuals that information is being collected about them or that the individuals have a right to request that the information not be

distributed. This makes it very difficult for individuals to control access to their personal information.

The alternative is opt-in conditions, which specify that an organization may use and distribute information only with the individual's consent. Thus, the burden is placed on organizations to obtain permission to use customers' data.

Opt-in conditions are much more protective of individual privacy and are a primary goal of privacy advocates. However, opt-out conditions govern personal information collected by most organizations in the United States. Business lobbies have been very successful at convincing state and federal lawmakers that requiring opt-in conditions would create unreasonable expenses and limit business interests. For instance, the Financial Services Modernization Bill, signed into law in November 1999, allows insurance companies, brokerage houses, banks, and credit card companies to merge and share information about their customers without notifying them. Lobbying by consumer advocates groups for customer notification of proposed data sharing was rejected as being impractical for the financial services industry.[16]

However, recent attention to data privacy in the media and by government, largely in response to the internet, has increased the public's awareness and concern about how personal information is collected and used. Such public attention may shift legislation and legal rulings about personal information use to be more protective of individual information privacy.[17]

Linking of Records

One of the greatest concerns of privacy enthusiasts is the ability of organizations to create extensive profiles of individuals' personal information. The prevalence of opt-out conditions has heralded the development of businesses based solely on collecting and selling individual information. One such business, Acxiom Corporation, for example, has a database combining public and consumer information that covers 95 percent of American households.[18] Computer networking increases the ease with which data can be exchanged or combined and makes it possible for outside groups to have direct access to computerized information. The internet is commonly used as a mechanism for collecting and distributing personal information, and much of an individual's personal information

is now available free of charge or for modest fees via the internet. Privacy advocates are concerned that information about an individual's travel behavior, collected through ITS, will be added to this mass of already available data, making possible the creation of intensely personal profiles of individual activities.[19]

Data Security

Individuals and businesses that submit their confidential information to an organization want to ensure that the information is secure from unauthorized access or alteration. Security threats, both internal and external to the data collecting organization, are real and should be guarded against. Besides threats from employees and from hackers, there is also a possibility that tracking devices could be read by unauthorized groups. Technical and non-technical information security measures may prevent many security breaches. However, it is difficult for any system to be completely secure.[20]

STAKEHOLDERS IN ITS PRIVACY ISSUES

Two groups are potentially affected by privacy issues in ITS: the general public and commercial freight carriers and shippers. The public is concerned with keeping the details of their lives free from surveillance. Individuals do not want to be restricted in their movements or activities by the concern that they are being watched.[21] They also want to be able to control who has access to information about them and how that information is used. Traditionally, some individuals have been willing to give up certain elements of their privacy to receive benefits offered by new technologies or services. However, the willingness of individuals to do this or the "price" in privacy infringement that individuals are willing to pay varies substantially. For example, ITS America cites a Columbia University study that concluded that the public may be segmented into three groups in terms of their sensitivity to privacy issues:

- 20 percent of Americans are reported as being "privacy insensitive," in that they do not think that technology threatens their own privacy and are concerned that progress in technology may be constrained by the privacy sensitivities of others;

- 55 percent are "privacy pragmatists," in that they desire the benefits that information technology creates, but are also concerned about potential harm from unauthorized and unexpected information use; and
- 25 percent are "privacy fundamentalists," in that they are concerned about all forms of information gathering, and believe that information collection and storage should be kept to an absolute minimum.[22]

Freight carriers and shippers have an additional stake in ITS privacy issues for competitive reasons. Travel routes and cargo are considered trade secrets by some in the industry.[23] ITS technologies have the capability of disclosing this information. As with individuals, members of the freight industry differ in their classification of confidential information and their willingness to concede information to receive certain benefits.

ITS proponents must address the concerns of all constituents if ITS are to gain public and user acceptance. ITS operators must be mindful of the various degrees of sensitivity that different users might have to the collection of personal or confidential information and provide appropriate choices to satisfy these users.

ITS APPLICATIONS WITH PRIVACY IMPLICATIONS

Privacy concerns are likely to be raised by any ITS application or technology that has one or both of the following characteristics:

1. It enables the identification of an individual vehicle or occupant.
2. It collects and stores proprietary information about a vehicle or individual.

A number of ITS applications meet or potentially meet the first criterion. These include, but are not limited to, the following applications and technologies:

- *Electronic clearance (EC) systems for commercial vehicles* – EC systems utilize advanced vehicle identification (AVI) technology, a database of carrier safety and credentials information, and possibly weigh-in-motion (WIM) and other technologies to enable commercial vehicles to electronically clear border crossing and inspection facilities without stopping. These are discussed in detail in chapter 4.

- *Border crossing systems for commercial vehicles* – These systems are similar to EC systems, but include additional features, such as cargo identification and customs information, to allow faster truck processing at international borders.
- *Electronic toll collection (ETC) systems* – ETC systems automatically deduct toll payments from an established user account using AVI technology to identify toll patrons.[24] These are discussed in detail in chapter 4.
- *Electronic enforcement (EE) applications* – EE applications allow automated enforcement of traffic violations, including speeding, red light running, and railroad grade crossing, by taking a picture of an offender's license plate when detection devices are triggered.[25]
- *Vehicle probe applications* – This refers to a number of technical applications used to detect and track individual vehicles through a road network for the purposes of abstracting traffic characteristics, such as travel times, or transportation data, such as trip origins and destinations, and traffic flow patterns.
- *Video surveillance applications* – Video cameras are used for a number of purposes, from wide-scale visual surveillance of traffic conditions to detailed video imaging to detect vehicle characteristics, traffic flow parameters, or vehicle queue lengths.
- *"Mayday" emergency response systems* – A variety of techniques are used to alert authorities and allow a vehicle to be located when triggered by a vehicle occupant or automatic crash detection system.
- *Smartcard applications* – Smartcards contain a computer chip capable of storing a great deal of information about the card owner that can be used for a variety of purposes, including the electronic payment of transit fares, parking fees, and tolls. The freight industry can use them to monitor information about a shipment or driver and to allow gate access to terminals.
- *Vehicle location systems* – A number of private vendors use satellite or triangulation-based technologies to provide vehicle location and other services, most commonly to commercial vehicle fleet owners. In-vehicle navigation devices also employ satellite referencing capabilities in the vehicle. The deployment of cellular

phone geolocation capabilities (described below) is expected to greatly increase the potential uses and applications associated with these technologies.[26]

- Applications that meet criterion two include most of those previously mentioned, plus several others. The following applications do not permit the identification of a vehicle or individual while enroute, but create a record that may be accessed later for potentially controversial purposes.
- *On-board safety data systems (black boxes or vehicle recorders)* – Installed by manufacturers in most commercial vehicles and some automobile engines, these devices record characteristics of the engine and vehicle for use in crash analysis. They are comparable to event recorders within the air and rail industries.[27]
- *Incident or accident logs* – Video recordings of accidents may contain sensitive information that is not appropriate for public release.[28]
- *Paratransit and rideshare request logs* – Records of individual requests for ridesharing or paratransit may enable tracing of an individual's movements.

Several of these applications and their underlying technologies merit further discussion.

Cellular Phone Geolocation

Federal legislation has mandated that cellular phone service providers deploy the technology to enable Enhanced 911 (E911), i.e. the ability to locate wireless callers of 911. Such technology would allow callers to be located not only during emergency calls, but any time a cellular phone is in use. Furthermore, the technology can provide not only latitude and longitude of a caller, but also direction and velocity of movements of callers. With over 74 million Americans now using wireless phones, often while traveling, geolocation capabilities have numerous potential uses within the transportation community.[29] The following are a few examples of potential uses.

- Accessed in anonymous form, cellular phone "probe" data can provide information to traffic managers about the speed of travel on all links in a traffic

network. This would allow greater coverage at potentially lower costs than current single-point detection technologies.

- Improved traffic data may support enhanced traffic information services, dynamic route guidance, and other personalized services.
- Automatic vehicle location for municipal and commercial vehicles will be possible using an inexpensive wireless beacon.
- Electronic payments, including electronic toll collection and other point of service applications, may potentially be billed directly to cell phones.
- Automatic crash notification can be facilitated through wireless phones.[30]

The privacy implications of such technology are obvious; for example, cellular phone service providers will have the ability to track users any time a phone is in use. Many of the potential services described could be provided through the cellular phone company under controlled environments. However, the potential also exists for such technology to be abused. The Wireless Communications and Public Safety Act of 1999 (discussed in chapter 3) provides some stipulations to protect user privacy, and at this time it is unclear whether the act even allows for E911 technologies to be used as traffic vehicle probes. However, the transportation and wireless communities are both advocating such uses, and it is probable that they will be allowed in the future. This is an issue that is being followed closely by the privacy community as well.[31]

Vehicle Probe Applications

Vehicle probe applications do not inherently allow the identification of individual vehicles or owners. Most are based on the premise of tracking vehicles anonymously. However, in some applications it would be possible to identify probes through matches with other databases. The likelihood of this possibility depends largely on the type of technology employed. Three potential technologies for vehicle probe tracking are described below.

Automatic Vehicle Identification (AVI). The most common technology in use today for vehicle probe tracking is AVI. Vehicles are equipped with transponders, which can be detected by roadside readers. Identical codes are matched from various readers to

determine vehicle trajectories and desired characteristics. Systems commonly scramble transponder codes after a given time period so that they may not be traced to the transponder owner. Systems either utilize transponders employed for other purposes, such as automatic tolling, or randomly distribute transponders on a voluntary basis. In either circumstance, the organization operating the system seldom knows identities of the transponder owners. In such a system, the possibility of identifying a vehicle owner are rare. However, it might be possible if vehicles are tracked to locations that are accessed only by a few vehicles or fleets.[32] Other ITS applications that use AVI and have multiple reader sites, such as electronic clearance (EC) and electronic toll collection (ETC), could potentially track and identify vehicles. However, usually operators of these systems do not track vehicles as a matter of principle and to avoid public perception problems.[33]

Video License Plate Reading. While still in the testing and development stage, this technology enables the electronic detection of license plate codes. These too can be matched across multiple reader sites to detect travel patterns of individual vehicles. Two characteristics of this technology concern road user groups. First, the reading of license plate numbers can be done without the consent or knowledge of travelers. With AVI, the traveler must consent to putting a transponder on his vehicle with an awareness that the vehicle could potentially be tracked. With license plate reading, the traveler is not afforded this protection. Second, license plate numbers are often easily traceable to vehicle owners through various databases. Although privacy protections can be built into license plate reading probe systems, much as they are in AVI systems, it is possible to imagine many uses of this technology that could be privacy invasive.[34]

Global Positioning Systems (GPS). GPS use satellite referencing to provide the longitude and latitude of a portable GPS unit. A vehicle equipped with GPS can be located anywhere along its route of travel. The GPS reading can then be transmitted to a collection center. This type of probe could potentially provide travel time statistics anywhere on a traffic network. However, the application relies on equipping an adequate number of vehicles with the technology to provide reliable statistics. Vehicles equipped with the technology can then be tracked.[35]

Cellular Phone Geolocation. As discussed above, cell phone geolocation could potentially provide a valuable set of vehicle probes that could provide traffic data across

an entire transportation network. This technology would enable much more extensive area coverage than AVI or license plate reading systems because it does not depend on independent reader stations. There are already a multitude of potential probes, unlike GPS systems. Although these factors create great potential for the technology, they also foster significant privacy implications. Probes could be potentially identifiable through the billing records maintained by the wireless service provider and could be tracked anywhere the cellular user travels. It would be incumbent on the cellular phone provider to implement privacy controls.[36]

CONCLUDING COMMENTS

This chapter has presented the fundamental privacy concerns associated with ITS and has defined potentially privacy invasive technologies as any that have the ability to single out a specific vehicle or occupant. ITS applications having this potential have also been identified. The applications presented are not inherently privacy invasive. When handled in controlled and privacy protective environments, they pose little threat to individuals or businesses. However, they create data that have the potential to be misused. Operators of these applications must be aware of this and set up appropriate mechanisms to avoid the misuse of data. ITS implementers are often faced with the challenge of balancing privacy protections with potential benefits that could be derived from the data. The remainder of this paper discusses this balance from various perspectives and presents techniques for protecting user privacy, while still allowing access to data for appropriate and beneficial purposes.

Notes

[6] Belair, Robert R., Alan F. Westin, and John J. Mullenholz, *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, contract no. DTFH61-93-C-00087 (Washington, D.C.: U.S. Department of Transportation, Dec. 1993).
[7] Ibid.
[8] Agre, Philip E., "Looking Down the Road: Transport Informatics and the New Landscape of Privacy Issues," *CPSR Newsletter*, vol. 13, no. 3 (1995), pp. 15-20, available from http://dlis.gseis.ucla.edu/people/pagre/its-cpsr.htm.
[9]Gelman, Robert, "Privacy and Electronic Clearance Systems," *Transportation Quarterly*, vol. 51, no. 4 (Fall 1997).
[10] Belair, Robert R., et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*.
[11] Holdener, Douglas J. "Electronic Toll Collection Information: Is personal Privacy Protected?" *Compendium: Graduate Student Papers on Advanced Surface Transportation Systems*, Southwest Region, University Transportation Center Research Report # SWUTC/96/72840-00003-1, Texas Transportation Institute, Texas A&M University System, August 1996, p. D-6.
[12] Belair, Robert R., et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*.
[13] Telephone interview by Valerie Briggs with Steve Pustelnyk, Manager of Communications and Marketing, Orlando-Orange County Toll Authority, Orlando, Florida, November 4, 1999.
[14] Ibid.
[15]Gelman, Robert, "Privacy and Electronic Clearance Systems," p. 63.
[16] Clausing, Jeri, "Revised Banking Legislation Raises Concerns About Privacy," *The New York Times on the Web* (October 25, 1999), available from http://nytimes.com/search/daily.
[17] Telephone interview by Valerie Briggs with Mark Johnson, Director of Legislative Affairs, ITS America, Washington, D.C., October 5, 1999.
[18] "The Surveillance Society," *The Economist* (May 1, 1999), p. 21.
[19] Wright, Tom, "Eyes on the Road, Privacy and ITS," *Traffic Technology International* (Autumn 1995), pp. 88-93.
[20] U.S. Department of Transportation, Intelligent Transportation Systems Joint Program Office, *Protecting Our Transportation System: An Information Security Awareness Overview*, by Keith Biesecker and Barbara Staples (Washington, D.C., November 1997).
[21] Belair, Robert R., et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*.
[22] Ogden, K.W., "Privacy and Electronic Toll Collection in Australia," (paper presented to the 6th World Congress on Intelligent Transportation Systems, Toronto, Canada, November 1999).
[23] Telephone interview by Valerie Briggs with Kevin Holland, Manager, Technology Policy, American Trucking Association, January 3, 2000.
[24] *An ETTM Primer for Transportation and Toll Officials*, ATMS Committee and ETTM Task Force, Intelligent Transportation Society of America.
[25] Polk, Amy E., "Electronic Enforcement of Traffic Laws," *ITS Quarterly*, Summer 1998, p. 17.
[26] "FCC Briefing Paper on the Use of Wireless Phones as Data Probes in Traffic Management, Travel Information and Other ITS Applications," provided by Mark Johnson, Director of Legislative Affairs, ITS America, Washington, D.C., October 12, 1999.
[27] Holland, Kevin, "Black Boxes, Satellites & Safety: Q&A," *Truckline*, American Trucking Association web site, September 17, 1999, available from http://www.truckline.com/infocenter/topics/tech/black_boxes_faq.thml.
[28] Telephone interview by Valerie Briggs with Rich Margiotta, Senior Associate, Cambridge Systematics, November 17, 1999.
[29] "FCC Briefing Paper on the Use of Wireless Phones as Data Probes in Traffic Management, Travel Information and Other ITS Applications," provided by Mark Johnson, Director of Legislative Affairs, ITS America, Washington, D.C., October 12, 1999.
[30] Ibid.
[31] Telephone interview by Valerie Briggs with Mark Johnson, Director of Legislative Affairs, ITS America, Washington, D.C., October 5, 1999.

[32] Telephone interview by Valerie Briggs with Mike Vickich, Systems Analyst, Texas Transportation Institute, College Station, Texas, October 10, 1999.
[33] Telephone interview by Valerie Briggs with Steve Pustelnyk, Manager of Communications and Marketing, Orlando-Orange County Toll Authority, Orlando, Florida, November 4, 1999; and electronic mail correspondence from Beth Rider, Director of Business Operations, Lockheed Martin Information Management Systems, to Valerie Briggs, January 26, 2000.
[34] Telephone interview by Valerie Briggs with Dave Barry, Director of ITS Programs and Research, National Private Truck Council, December 13, 1999.
[35] Telephone interview by Valerie Briggs with Michael Dennis, Director of Telematics, ITS America, Washington, D.C., November 16, 1999.
[36] Telephone interview by Valerie Briggs with Mark Johnson, Director of Legislative Affairs, ITS America, Washington, D.C., October 5, 1999.

Chapter 3. Legal and Institutional Framework for ITS Privacy Issues

The privacy concerns of individuals are often at odds with certain government and business interests. Likewise, the privacy concerns of the trucking industry can be at odds with certain government interests. Mechanisms, whether legal or institutional, are necessary to provide balance between business and government interests and the privacy interests of constituents. This chapter discusses some of these mechanisms as they apply to ITS. The first section outlines federal and state legislation relating to ITS privacy. This is followed by an examination of institutional mechanisms for privacy protection in ITS, including internal policies and contracts. Policies by ITS America and the Federal Motor Carrier Safety Administration relating to data privacy are discussed.

LEGAL FRAMEWORK FOR ITS PRIVACY ISSUES

The United States does not have an overarching information privacy law that applies uniformly to businesses and government agencies. While federal and state laws address the treatment of personal information within government agencies, information privacy protection within the private sector is left largely to business self-regulation through the voluntary application of codes of fair information practices. These codes do not create enforceable legal rights. Legal provisions for privacy exist largely in a patchwork of state statutes and court rulings.[37] This section outlines the legal framework for privacy issues in ITS and discusses the federal and state laws expected to have the greatest impact on how ITS collect and handle data.

The right of privacy is not expressly written in the U.S. Constitution. However, it has been upheld as a Constitutional right in numerous court opinions.

These opinions have defined the right of privacy as encompassing three fundamental principles:

- Autonomy – An interest in being free to engage in certain intimate or private activities, free from governmental regulation.

- Intrusion – An interest in being free from surveillance in situations in which an individual has a reasonable expectation of privacy. This interest encompasses the interest in preserving anonymity.
- Informational Privacy – An interest in controlling, or at least participating in, decisions about the collection, quality, use, and dissemination of personal information.38

A number of ITS applications have the potential to violate two of these interests, namely, intrusion and information privacy. Concerns about intrusion may arise for ITS systems that use surveillance, including the use of video for traffic monitoring or traffic law enforcement purposes. The electronic tracking of vehicles is also a form of surveillance that could violate the intrusion interest. Information privacy is a concern for any application that collects information about individuals or businesses (such as trucking companies) that could be deemed proprietary. Information about individual travel behavior is considered by many to be proprietary, as are address and financial data collected by many ITS organizations for customer billing purposes. This chapter discusses laws and court cases that address these privacy interests and may be applicable to ITS.

Fourth Amendment

The Constitutional prohibition against unreasonable searches and seizures established in the Fourth Amendment to the U.S. Constitution provides the basis for most federal privacy laws with potential application to ITS.[39] Specifically, the Fourth Amendment requires government authorities to obtain a valid judicial warrant prior to the execution of a search. Furthermore, any evidence obtained by government officials in violation of the Fourth Amendment may not be used during criminal trials.[40]

This branch of privacy law is interpreted according to whether the person objecting to a search or seizure has a reasonable expectation of privacy. For the most part, courts have ruled that occupants of automobiles traveling on public roads do not have the same expectation of privacy as they would inside a home or office, and, therefore, search criteria for automobiles are much less stringent than for other personal

spaces. The identification, surveillance and even tracking of a vehicle traveling on public streets is not considered a violation of Fourth Amendment rights regardless of whether manual or electronic means are employed. It should be noted, however, that some state courts have upheld more restrictive measures of law enforcement uses of electronic tracking devices on vehicles.[41]

Electronic Communications Privacy Act of 1986 and 1994 Communications Assistance for Law Enforcement Act

The literature takes dissenting views as to the importance to ITS of the Electronic Communications Privacy Act (ECPA) of 1986 and its amendment, the 1994 Communications Assistance for Law Enforcement Act (CALEA). These statutes regulate the interception of wire and wireless oral and electronic communications and require law enforcement officials to obtain a warrant and follow certain procedures before and after initiating electronic surveillance.[42]

Proponents believe that these laws will enhance safeguards for the privacy of ITS users by protecting ITS communications against interception by law enforcement and eavesdroppers.[43] However, the statutes have numerous shortcomings for this purpose. First of all, only the interception of the *contents* of a communication are restricted.[44] Often the primary ITS interest is not the content of a communication but the fact that a communication takes place, which may indicate the location and identity of a vehicle. Moreover, ECPA explicitly excludes the coverage of mobile tracking devices,[45] thus leaving unprotected a significant portion of ITS applications. Finally, the provision of the 1994 Act requiring law enforcement to obtain a warrant to access transactional data associated with on-line communications systems is less restrictive than some privacy advocates desire. Instead of requiring "probable cause," warrants may be based on the intermediate level standards of "'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."[46] The intent of the standard, as defined by the U.S. House of Representatives Report, is "to guard against 'fishing expeditions' by law enforcement."[47] While much debate has ensued over these statutes, their true impact will not be known until the Federal Communications Commission

(FCC) establishes clear rules for the interpretation of CALEA, a process that remains in progress.

Telecommunications Act of 1996

The Telecommunications Act of 1996 is one of the most important pieces of legislation for ITS both for its direct relevance to ITS applications involving telecommunications and for the precedent it sets for the ITS industry. The critical part of the Act for ITS is Title VII, Section 702, "Privacy of Customer Information," which creates a new Section 222 within the Communications Act of 1934 (see Appendix E for complete text).

The legislation has a number of important elements. First of all, it gives telecommunications carriers responsibility for protecting the confidentiality of customer proprietary information and forbids them from using this information for any purposes other than for providing the specific service for which the information was collected. This includes uses for marketing purposes. Carriers may not use, disclose, or provide access to individual customer proprietary information without approval of the customer.[48] These provisions create opt-in conditions for use of individual customer information. However, the Act's treatment of aggregate customer information is different. It does not place limitations on the use or disclosure of aggregate data except that carriers must do so "on reasonable and nondiscriminatory terms and conditions." The Act refers to individual customer information as "Customer Proprietary Network Information" (CPNI), which it defines as

> (A) information that relates to the quantity, technical configuration, type destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer or a carrier.[49]

A federal appeals court overturned part of the legislation related to telecommunications carriers' use of CPNI to market to their customers in August 1999. In the *case U.S. West, Inc. v. Federal Communications Commission and United States of*

America, the 10th U.S. Circuit Court of Appeals ruled that U.S. West and other communications companies have the constitutional right to use information gathered about customers to try to sell them additional services.[50] The Court contended that the FCC's interpretation of Section 222 (47 U.S.C. 222) adopted in the CPNI Order (63 Fed. Reg. 20.326) are "impermissible because they violate the First and Fifth Amendments of the United States Constitution."[51]

Although the direct ramifications of the Act on ITS applications are not clearly defined, it does have important implications for ITS. The Telecommunications Act applies only to telecommunications carriers. It is debatable whether various ITS applications fall under the definition of "telecommunications carriers." However, many ITS services collect information that is similar in nature to information defined as customer proprietary network information collected by telecommunications carries. Thus, it can be argued that ITS services should follow the same standards and be afforded the same protections, such as the right to use and distribute aggregate data, as telecommunications carriers.

Wireless Communications and Public Safety Act of 1999

The Wireless Communications and Public Safety Act of 1999 deals with a number of issues critical to ITS and has important privacy implications. The Act establishes provisions to allow wireless phones to be located in cases of emergencies and provides protections on the use of this location information. The ITS community hopes that the Act will also open the door for cell phones to be used as anonymous, aggregate probes for traffic management purposes.

Specifically, the Act calls on the Federal Communications Commission and state and local governments to move toward establishing coordinated E911 capabilities. This would allow emergency operators to locate callers dialing 911 from wireless phones, a process that is standard for wireline phones. The Act also provides privacy protection for the call location information of users of wireless phones.[52] It amends Section 222, established in the Telecommunications Act of 1996, to prohibit the unauthorized disclosure or use of call location information except to designated emergency service providers and the caller's immediate family members for the express purpose of

responding to an emergency (see Appendix F for text of Section 5, "Authority to Provide Customer Information").[53]

Thus, the Act is a boon to the emergency response and incident management aspects of ITS. In addition, it is possible that the Act opens the door for the use of aggregate customer location information, which might allow cellular devices to be used as traffic data probes. The new provisions concerning the use of customer location information are part of Section 222, which expressly allows freedom of use and distribution of aggregate customer information. However, location information is not included in the definition of CPNI and, therefore, some may argue that it does not fall within the realm of information that may be used and distributed in aggregate form.[54]

Privacy Act of 1974 and Freedom of Information Act

Federal information privacy laws, including the Privacy Act of 1974 and the Freedom of Information Act (FOIA), apply only to information maintained by the federal government. Thus, they do not apply to records maintained by state and local governments or private organizations, which account for the majority of ITS operators. However, the laws are important in that they provide models for numerous state statutes governing the handling of personal information by state and local government agencies and the private sector.[55]

The Privacy Act of 1974 regulates the collection, retention, use, and disclosure of personal information by federal government agencies. It upholds the federal government's ability to collect and retain personal data that serve legitimate governmental interests, but establishes rules for these practices. Although the Privacy Act allows agencies to collect personal information from third-party sources if direct collection from the individual is impractical, it "urges" agencies to use direct collection methods. Before using personal information, agencies must have in place procedures to assure that the information is accurate, timely, relevant, and complete. Additionally, individuals are given the right to access information held about them and the ability to correct or amend their records, with the exception of some records compiled for special purposes, such as law enforcement. The Privacy Act also stipulates control of access to personal information both within and outside the collecting agency. However, release of

personal information on a non-consensual basis is permitted for most governmental purposes.[56]

The federal Freedom of Information Act entitles the public to access, by request, any records held by federal agencies. FOIA has certain exemptions, including one for information, that, if disclosed, would be likely to result in a "clearly unwarranted invasion of privacy."[57] In interpreting FOIA, the U.S. Supreme Court has instructed agencies to weigh the public's interest in disclosure against the potential for an invasion of privacy, and recently has held that the disclosure of any personal information is presumed to violate privacy interests.[58] It is unclear whether information collected through ITS is included in the law's definition of personal information because it is not expressly listed.[59] However, FOIA may provide some protection of personal information that is collected through ITS as long as it is held by a federal agency. All states have adopted legislation similar to FOIA that pertain to information held by state and local government agencies.[60]

Business trade secrets are protected from public disclosure under FOIA. However, not all confidential business information are considered trade secrets. Other confidential business information may be protected depending on its competitive sensitivity and whether the information was submitted to the government voluntarily or under compulsion. These factors are determined on a case-by-case basis.[61]

State Privacy Laws

Most ITS applications fall within the realm of state privacy laws, which regulate the collection of information by state and local governments as well as the private sector. State privacy laws vary significantly among states in their degree of protection and are often more fragmented than federal law. This variability means that no uniform set of standards for appropriate practices of ITS operators with regard to privacy may be applied across states. Instead, operators must evaluate their practices according to the specific laws that govern their jurisdiction or organization. It also poses challenges for the development of nationally uniform ITS programs.[62]

Types of state privacy laws potentially applicable to ITS include state constitutional privacy laws, state statutory privacy laws, and state common law privacy

torts. A handful of states specifically guarantee a right to privacy within their state constitutions. A number of others contain an implied privacy right. Such provisions generally signal greater intensity of privacy protections in these states and could provide challenges to some ITS applications, especially law enforcement applications.[63]

Every state constitution contains a prohibition of unreasonable searches and seizures. Like the U.S. Constitution, however, state court interpretations of what constitutes a reasonable expectation of privacy for such applications vary significantly. Some states have forbid the use of electronic vehicle tracking technology by law enforcement as a violation of privacy, while other state courts have specifically held that the same use of this technology does not invade privacy.[64]

About half of all states have statutes similar to the federal Privacy Act that regulate the collection, retention, use and dissemination of personal information held in state records.[65] The remainder of states do not have comprehensive privacy statutes, but instead have numerous statues governing specific types of personal records. These statutes generally impose regulations on the private sector as well as government entities. Like the federal law, often these statutes include modest limits on the collection of personal information, standards for the accuracy and completeness of information, confidentiality and data security standards, and data rights standards allowing individuals to access and correct their personal records.[66]

Every state has adopted a public records act similar to the federal Freedom of Information Act. All of these statutes include an exemption that provides protection against the disclosure of personally identifiable information. However, many state statutes do not provide the same degree of privacy protection as under the federal law, nor do they require nondisclosure of ITS information about individuals. Thus, it is possible that personal information, including ITS data, held in government files in these states could be publicly accessible.[67]

Over forty states have adopted common law/tort actions that "create a duty not to publicly disclose private facts in cases where the disclosure would be highly offensive to a reasonable person and is not of legitimate concern to the public."[68] However, scholars agree that it would be very difficult for a plaintiff to successfully prosecute an

information privacy tort claim. Therefore, common law privacy claims are not likely to have much impact on the data practices of ITS operators.[69]

INSTITUTIONAL FRAMEWORK FOR ITS PRIVACY ISSUES

Information privacy protection within the American business community is left to reliance upon voluntary measures and market solutions. The idea is that consumers will chose to support businesses that provide adequate protection of their privacy. Two techniques are frequently used to protect consumer privacy. Many industries have adopted voluntary codes of fair information and privacy principles based on five basic tenants: openness, individual access and correction, collection limitation, finality, and security. However, these codes are not legally enforceable. Businesses can also use contracts to create legally binding agreements with their customers that address privacy provisions.

Fair Information and Privacy Principles

Recognizing the importance of protecting the privacy of ITS users, the Intelligent Transportation Society of America has drafted the *Intelligent Transportation Systems Fair Information and Privacy Principles* and the *Fair Information Principles for ITS/CVO*. These principles are intended to assist transportation professionals and policy makers in developing their own fair information and privacy guidelines for ITS systems. They were developed through the input of a wide range of stakeholders from the ITS community. The complete text of these principles are in Appendices G and H.

Federal Motor Carrier Safety Administration Policy Regarding Federal Access to Privately Held Information

Government regulators' ability to access privately held data collected through ITS has been a point of controversy between government authorities and some in the motor carrier industry. Some motor carriers have alleged that the ability of government regulators to subpoena information collected through carrier-owned ITS creates a disincentive for investment in ITS. Regulators contend that electronic records should be treated no differently than paper records, and regulators should be able access these records under the same constraints as for paper records. The case Arctic Express, Inc. vs. United States of America focused significant national attention on this issue. The U.S.

Sixth Circuit Court of Appeals upheld an earlier District Court ruling affirming the Federal Highway Administration's ability to subpoena electronic information collected through ITS and maintained by the company "in the ordinary course of business."[70]

Subsequent to the case, the Federal Motor Carrier Safety Administration issued internal enforcement guidelines to its field personnel regarding the collection of data obtained through carrier-owned ITS. The policy includes provision that enforcement personnel must issue a warning to violators and allow adequate time for corrections to be made before ITS data may be subpoenaed. In addition, enforcement personnel may only access data that is relevant to enforcement of driver hour of service restrictions.[71] This topic remains one of debate.

CONCLUDING COMMENTS

The U.S. legal environment does not provide clear cut guidance for privacy issues in ITS. U.S. law, in general, establishes little protection for individual or business privacy interests. The Privacy Act, the Freedom of Information Act, and similar state laws establish some provisions for information collected and maintained by government agencies. However, within the private sector, privacy issues have been left largely to business self regulation with execution through contracts. Those laws that do exist concerning consumer privacy tend to favor business interests over individual interests in the collection of information.[72] Furthermore, no existing laws apply directly to ITS. Those involved with ITS must look to laws addressing other industries for guidelines.

These factors lead to a difficulty of determining a standard of practice for ITS implementers to follow. ITS America has attempted to create a standard with its Privacy Principles. Although these rely on voluntary implementation and are not legally binding, they were created and have been approved by a wide range of stakeholders in ITS. Therefore, they represent the best standard currently available for the treatment of privacy issues in ITS and are the basis for much of the discussion in the remainder of this document.

Notes

[37] "Data Dogfights," *The Economist* (January 9, 1999), p. 18.
[38] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 4.
[39] Glancy, "Privacy and Intelligent Transportation Technology," *Santa Clara Computer and High Technology Law Journal*, vol. 11, no. 1 (March 1995), p. 172.
[40] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 18.
[41] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, pp. 18-25, and Glancy, "Privacy and Intelligent Transportation Technology," p. 172.
[42] Glancy, "Privacy and Intelligent Transportation Technology," p. 173.
[43] Ibid.
[44] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 27.
[45] Ibid.
[46] Pub. L. No. 103-414, 108 Stat. 4279 § 207 (1994), amending 18 U.S.C. 2703(d); as quoted from Glancy, "Privacy and Intelligent Transportation Technology," pp. 173-174.
[47] H.R. Rep. No. 827, 103d Cong., 2d Sess., at 31-32 (1994); as quoted from Glancy, "Privacy and Intelligent Transportation Technology," p. 174.
[48] U.S. Congress, Enrolled Bill, *Telecommunications Act of 1996*, 104th Cong., 2nd sess., 1996, S. 652, Sec. 702, available from: http://thomas.loc.gov.
[49] Ibid.
[50] McPhee, Mike, "Court: Firms Can Target Phone Users," *The Denver Post Online* (August 20, 1999), available from: http://www.denverpost.com/business/biz0820d.htm.
[51] *U.S. West Inc. v. Federal Communications Commission*, 98-9518 (U.S. App., 10th Cir. 1999)
[52] "President Clinton Signs into Law National 911 Bill," *Access ITS*, ITS America, [www.itsa.org/legislative.html], October 29, 1999.
[53] U.S. Congress, Enrolled Bill, *Wireless Communications and Public Safety Act of 1999*, 106th Cong., 1st sess., 1999, S. 800, Sec. 5, available from [http://thomas.loc.gov/].
[54] Memorandum from Mark Johnson, Director of Legislative Affairs and Legal Counsel, ITS America, to John Collins, President, ITS America, Washington, D.C., September 14, 1999.
[55] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 32.
[56] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, pp. 32-33.
[57] 5 U.S.C. § 552(b) (6); as quoted from Belair, et. al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 33.
[58] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 33.
[59] Holdener, Douglas J. "Electronic Toll Collection Information: Is personal Privacy Protected?" *Compendium: Graduate Student Papers on Advanced Surface Transportation Systems*, Southwest Region, University Transportation Center Research Report # SWUTC/96/72840-00003-1, Texas Transportation Institute, Texas A&M University System, August 1996, pp. D-8 – D-9.
[60] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 33.
[61] Gelman, Robert, "Privacy and Electronic Clearance Systems," *Transportation Quarterly*, vol. 51, no. 4 (Fall 1997), pp. 65, 67.
[62] Glancy, "Privacy and Intelligent Transportation Technology," p. 177.
[63] Ibid., pp. 177-203.
[64] Ibid., p. 178.
[65] Alpert, Sheri A, "Privacy and Intelligent Highways: Finding the Right of Way," *Santa Clara Computer and High Technology Law Journal*, vol. 11, no. 1 (1995), pp. 97-118.
[66] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, pp. 33-34.
[67] Ibid., p. 34; and Glancy, "Privacy and Intelligent Transportation Technology," p. 179.
[68] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, pp. 34-35.
[69] Ibid.; and Glancy, "Privacy and Intelligent Transportation Technology," pp. 179-180.
[70] *Arctic Express, Inc. vs. United States of America*, 96-4095 (U.S. 6th Ct. App., 1997).
[71] Telephone interview by Valerie Briggs with David Lehrman, Legal Counsel, Federal Motor Carrier Safety Administration, Washington, D.C., February 4, 2000.

[72] Interview by Valerie Briggs with Craig Roberts, Director of Policy and Partnerships, ITS America, Washington, D.C., June 11, 1999.

Chapter 4. The Collection of Sensitive Information

Privacy concerns related to ITS are not new. ITS developers and operators have been addressing privacy concerns since the inception of ITS programs. Many ITS operators established procedures regarding data privacy long before formal policies and guidelines were developed. Some of these organizations now have over 10 years of experience in handling sensitive information. Significant lessons can be learned from their experiences that may be applied to other ITS technologies.

The electronic toll collection and electronic clearance system operators have been addressing privacy concerns for over 10 years. Both applications have been the subjects of public privacy debates and have had to overcome opposition to gain public acceptance. Both communities continue to be sensitive to user privacy issues and to readdress internal policies and practices with regard to data privacy over time.

Lessons can be learned from their experiences that may be transferable to other ITS data collection efforts. This chapter provides an extensive profile of experiences in electronic toll collection and electronic clearance. The conclusion to the chapter presents findings and lessons learned for wide-scale application.

ELECTRONIC TOLL COLLECTION

Electronic toll collection (ETC) systems are providing faster travel, reducing congestion and improving collection efficiency on toll and turnpike facilities across the United States. ETC usage continues to rise steadily as toll facility operators and users realize the benefits of ETC. The following description of ETC and electronic toll transactions draws largely from Douglas Holdener's account of ETC.[73]

ETC allows participating vehicles equipped with electronic transponders, or tags, to avoid stopping to pay tolls. Instead, the electronic transponder communicates via radio frequency or microwave to a roadside computer. The tagged vehicle is identified as an electronic toll collection system user, and the toll amount is debited from the user's account.

ETC systems use automatic vehicle identification (AVI) technology for communicating between the tagged vehicles and a system computer. Roadside equipment consists of

1. a transceiver to transmit and receive information to and from the tag;
2. a lane controller that coordinates the activities of all other lane equipment and creates the transaction used to charge the customer's toll account; and
3. a primary processing computer, which accesses account information and processes transactions. [74]

The in-vehicle equipment is the electronic transponder (tag), which maintains the user's identification (ID) number and other information, depending upon the type of tag technology. Three basic electronic transponder technologies exist: Type I, read-only tags; Type II, read/write tags; and Type III, intelligent tags.[75] Read-only tags store few data, such as the user's ID number, whereas read/write tags can maintain unique variable data, such as entry/exit points of the toll facility and account balance information.[76] Intelligent, or smart, tags are microprocessor-based and have much more memory than either Type I or Type II transponders; these tags have the ability to calculate tolls and maintain the user's account.[77] The presence of the electronic transponder may be detected by a roadside or overhead sensor or antenna even when the tagged vehicle is traveling at a high speed.

Many ETC systems also use some form of automatic vehicle classification (AVC) technology to determine the vehicle type so that the proper toll can be charged. Various sensors are employed to detect such characteristics as the number of axles and/or tires of a vehicle, dimensions (e.g., height, length, wheel-base, height over first axle) of a vehicle, and weight of a vehicle. A processing unit then assigns a classification to the vehicle.[78]

Video enforcement systems (VES) are another common feature of ETC systems. VES capture images of the license plates of vehicles that use the facility without a valid tag so that the vehicle owners can be identified and notified that a toll is due. Advanced technologies such as digital imaging and license plate recognition can read and record a license plate number from the image, obviating the need for manual intervention.[79]

Field performance evaluations of AVI technology used for ETC purposes have indicated reliability within the range of 89.7 to 98.4 percent.[80] While conventional toll

collection methods have a reliability range of 93 to 98 percent, ETC is equally reliable and allows for more efficient processing of toll-paying vehicles, which reduces fuel consumption, vehicular emissions, and driver frustration.

Automating the toll collection process can offer significant increases in toll plaza lane capacity. A study to estimate the average capacity of different toll plaza lane configurations was conducted by the Florida Turnpike, New Jersey Turnpike, and Dallas North Tollway. From this study, the average capacity of dedicated ETC lanes, or lanes that cater only to tagged vehicles, was reported at 1200 vehicles per hour.[81] A manually operated lane allowed an average of 350 vehicles per hour, and an automatic, coin insertion toll plaza lane allowed an average of 500 vehicles per hour.

Electronic Toll Transactions

ETC users are typically required to maintain a certain minimum balance in their ETC accounts with the responsible toll collection agency. When the tagged vehicle passes through the toll plaza, a unique ID code is detected by the roadside computer; the ID numbers are associated with individual users' accounts, or toll records.[82] The necessary toll is debited from the user's account. If the user's account balance drops below the minimum balance, the toll collection agency will either automatically replenish the account balance by charging the user's credit card or notify the user to replenish the account balance with a cash or personal check payment. Users may be notified through the mail, by a smart tag liquid crystal display (LCD), or by an electronic message sign as they pass through the toll plaza. Users have the option of deciding the type of account balance replenishment method they prefer.

In order to maintain the integrity of the ETC system, a toll collection agency must maintain user accounts in a centralized system. These accounts are identifiable by the users' personal and vehicular information, and the accounts allow the agency to accurately debit tolls from their users and conduct audits. The commonly used Type I and Type II transponder technologies do not have sufficient on-board memory to conduct toll transactions or maintain user accounts, necessitating a centralized account database.[83]

Electronic Toll Collection Systems

Currently, at least 20 ETC systems are being operated by 27 different agencies or organizations on approximately 100 toll and turnpike facilities in the United States. The organization that owns the toll facility is responsible for the ETC system.[84] These are most commonly toll, turnpike, or expressway authorities that are agents of state or county governments. Government cooperatives, such as the Regional Consortium in New England, and a few private companies, including the California Private Transportation Corporation and the Toll Road Investment Partnership II, also operate toll facilities utilizing ETC.

Transponders and other equipment are purchased from one of several vendors. Toll authorities may have entire ETC systems built and provided turnkey or hire a systems integrator to integrate new components with existing toll technologies. Toll authorities retain ownership of transponders and effectively rent them to ETC customers. Customer service center functions, which include enrolling customers, managing customer accounts, issuing tags, and processing violations, may be performed by the operating agency or contracted to a private firm. Private operating organizations abide by procedures established by the toll agency. Thus, the toll agency controls the handling of data, although it may or may not perform operations.[85]

In some cases several toll authorities operate systems with the same name, such as E-ZPass in New England and Fastrak in California. These authorities utilize compatible technologies and have interoperability agreements allowing users registered with any one organization to use the entire network. This allows seamless travel for the user, although each authority operates independently with its own procedures.

Privacy Issues in Electronic Toll Collection

The primary privacy concerns associated with ETC revolve around its ability to identify vehicles and track and record their movements. ETC databases contain proprietary personal and financial information as well as data about individual travel behavior. Privacy advocates fear that outside parties may gain access to the data collected and use it for unintended purposes not approved by customers. Secondary uses of particular concern include speeding detection by law enforcement and marketing

efforts from outside organizations. Some individuals are also concerned with their potential loss of anonymity and the ability of others to detect where they are or are not at a particular instance in time.[86] The ability to use these records in litigation is a concern to privacy advocates and to toll agencies, which fear that they will have to answer to a large number of subpoenas.

Electronic Toll Collection Survey Results

The applications and customer contracts of 12 ETC agencies in the United States were examined and compared. Nine of these agencies participated in the ETC survey. Respondents included eight public and one private ETC operators. Two ETC organizations represent consortia of multiple public agencies. Table 1 lists the name of each ETC agency studied and indicates those participating in the survey. It also states the facility location, whether the agency is a public or private organization, and the year ETC operations began. Operating statistics, including the number of active accounts, the number of active transponders, whether the system utilizes AVC and VES, the type of tag used, and whether customer service center operations are performed in house or contracted out, are indicated in Table 2.

Table 1. ETC Survey Respondents

	System Name	Operating Agency	Location	Organization Type	Began Operations†
1	E-Pass*	Orlando-Orange County Expressway Authority	Orlando, Florida	Public	2/95
2	E-ZPass*	New York Thruway Authority (NYTA)	New York State	Public	4/95
3	E-ZPass	Regional Consortium, Interagency Group (RC)	New Jersey, Delaware	Public Consortium	11/98
4	EZ Tag*	Harris County Toll Road Authority	Houston, Texas	Public	10/92
5	FastLane	Massachusetts Turnpike Authority	Massachusetts	Public	10/98
6	FasTrak*	California Private Transportation Company (CPTA)	91 Expressway	Private	12/95
7	FasTrak*	San Diego Association of Governments (SanDAG)	I-15 Corridor	Public	3/98
8	FasTrak*	Transportation Corridors Agency (TCA)	Southern California	Public Consortium	1/95
9	I-Pass	Illinois State Toll Highway Authority	Illinois	Public	1/98
10	K-Tag*	Kansas Turnpike Authority	Kansas	Public	10/95
11	PikePass*	Oklahoma Transportation Authority	Oklahoma	Public	1/91
12	TollTag*	North Texas Tollway Authority	Dallas, Texas	Public	7/89

*Indicates participation in the ETC survey
† Source: ETTM On the Web, available from http://www.ettm.com. All other information received through surveys conducted by Valerie Briggs, November 1999 through January 2000.

Table 2. ETC Agency Operating Characteristics

	System Name	Active Accounts	Active Tags	AVC*	VES*	Tag Type*	Customer Service Center Operations*
1	E-Pass	138,000	208,000	yes	yes	read/write	In-House
2	E-Zpass (NYTA)	452,000	803,000	no	yes	read/write	In-House
3	E-Zpass (RC)	81,000*	154,000*	yes	yes	read/write	Contracted
4	EZ Tag	271,000	512,000	yes	yes	read only	In-House
5	FastLane	133,000*	210,000*	yes	yes	read/write	Contracted
6	FasTrak (CPTA)	100,000	130,000	no	yes	read/write	In-House
7	FasTrak (SanDAG)	7,150	10,185	no	no	read/write	Contracted
8	FasTrak (TCA)	155,000	270,000	yes	yes	read/write	Contracted
9	I-Pass	250,000	275,000	yes	yes	read/write	In-House
10	K-Tag	50,000	112,000	yes	no	read/write	In-House
11	PikePass	230,000	430,000	no	yes	read only	Contracted
12	TollTag	196,000	289,000	yes	yes	read only	In-House

* Source: ETTM On the Web, available from http://www.ettm.com. All other information received through surveys conducted by Valerie Briggs, November 1999 through January 2000.

Information Collection. Account records are maintained for each ETC customer for billing purposes. The account records include records of toll transactions and personal information used for billing. All personal information is supplied by the user through an application. Although applications vary slightly among ETC agencies, three basic types of information generally are requested: contact, vehicle, and financial information.

All 12 ETC agencies require customer name, home address, and day and evening telephone numbers. Several agencies also optionally request additional contact information, including business address (1), e-mail address (7), fax number (6), cell phone number (1), and pager number (1). The number of agencies requesting this information is indicated in parenthesis.

Social security and drivers' license numbers are required on some but not all applications, as indicated in Table 3. These forms of identification have aroused privacy concerns in the past because they are connected to a number of proprietary data,

including personal tax, driving, and credit records. However, their uses have become commonplace today. ETC agencies use drivers' license numbers as a means of locating the customer should other contact information change. K-Pass is the only program that requires a social security number, and claims that it is necessary since the program does not require customers to maintain a positive account balance. The Kansas Turnpike Authority runs credit reports for all individuals using the post-payment plan with the cash/check option, since this equates to extending customer credit. It also requires credit references and bankruptcy history for these customers.

Several other agencies request social security numbers on their applications, but report that this information is optional. Agencies requesting social security numbers claim that they are used only to perform credit checks should a customer's account become delinquent. PikePass reported that it would like to collect customer social security numbers, but is prevented by an Oklahoma state statute that limits the use of social security numbers by state agencies. One agency also asks for the applicant's mother's maiden name, which it uses as a security mechanism in case the customer forgets his PIN number.

Table 3. Driver's License and Social Security Number Requests on ETC Applications

System Name	Driver's License Number	Social Security Number
E-Pass	Yes	No
E-Zpass (NYTA)	No	No
E-Zpass (RC)	No	No
EZ Tag	Yes	Optional
FastLane	No	No
FasTrak (CPTA)	No	No
FasTrak (SanDAG)	Yes	No
FasTrak (TCA)	No	Optional
I-Pass	Yes	No
K-Tag	Yes	Yes
PikePass	No	No
TollTag	Yes	No

Source: ETC agency surveys conducted by Valerie Briggs, November 1999 through January 2000.

In a survey of electronic toll agencies conducted in 1996, three out of seven agencies, or 43 percent, required social security numbers on their applications.[87] In this survey, only 25 percent of ETC organizations include social security number on their applications. Several organizations that requested social security numbers in 1996 no longer do so. More agencies are finding that this information is not necessary for their operations and, consequently, are not collecting it. Requests for drivers' license numbers were similar for the 1996 study and this study. However, the fact that over half the organizations examined do not require this information may indicate that it is not necessary for the operation of ETC systems. Thus, some ETC agencies may be collecting more information than is necessary.

Signatures are required on most applications in order to create a legally binding contract between the agency and customer. However, several ETC agencies allow on-line registration, which does not require signatures. Instead, the customer must click a check-box indicating agreement to the agency's terms and the truthfulness of information provided.

Vehicle information is requested in order to verify that the correct vehicle is using the tag in disputed cases or in cases of lost or stolen tags. It can be used to calculate tolls on facilities that charge variable rates depending on the vehicle type. For systems that employ AVC systems, it can provide a check for the vehicle classification. K-Tag is the only ETC agency surveyed that does not request any vehicle information. All others request the license plate number and state, and the make, model, and year of each vehicle enrolled. Vehicle color (7), number of axles (2), number of tires (2), and vehicle type as selected from a list (2) are also requested by several of the 12 agencies studied, as indicated in parenthesis.

All responding agencies provide multiple payment options, including cash or check. However, by far the most commonly used is automatic credit card billing. This requires the agency to keep records of customer credit card numbers. PikePass requires a credit card number for backup even for cash or check accounts. Some agencies will also automatically deduct charges from customer bank accounts, which requires the customers' bank account numbers. Most agencies require prepayment of tolls by periodically billing the customer when the money in his account drops below a minimum amount. K-Tag and FastLane have plans for post-payment of charges. Table 4 indicates the information requested by each agency based on their payment options.

Table 4. Financial Information Requests on ETC Applications

System Name	Credit Card Number	Bank Account Number
E-Pass	Optional	No
E-Zpass (NYTA)	Optional	No
E-Zpass (RC)	Optional	No
EZ Tag	Optional	Optional
FastLane	Optional	Optional
FasTrak (CPTA)	Optional	No
FasTrak (SanDAG)	Optional	No
FasTrak (TCA)	Optional	No
I-Pass	Optional	No
K-Tag	Optional	No
PikePass	Yes	Optional
TollTag	Optional	No

Source: ETC agency surveys conducted by Valerie Briggs, November 1999 through January 2000.

Toll transaction histories are also recorded in conjunction with customer accounts. When a tag passes a toll plaza, a transaction record is created that includes the date, time, location (toll plaza and lane number), and amount of the toll. Programs with AVC systems also record number of axles. ETC agencies' databases have the ability to access customer transaction histories through an account number. This enables billing statements to be created that include transaction histories.

Speed Data. Opponents of early ETC systems feared that they would enable speed tracking, which would be used for speeding enforcement. Although all systems are technically capable of calculating vehicle speeds, most do not include algorithms to automatically track vehicle speeds. Thus, speeds are not calculated or recorded. In addition, all agencies have policies against using ETC data for speed enforcement purposes and do not allow law enforcement access to the data. However, speed data can be valuable for other purposes, and some agencies are now collecting it in various forms.

Several systems (E-Pass, K-Tag, FasTrak-TCA, E-ZPass-NYTA) record the speeds of ETC customers as they travel *through* toll plazas and record these in customer

account records. This is an effort to decrease the destruction of toll agency property and reduce safety hazards from vehicles that do not adequately decrease speeds as they travel through toll plazas. The agencies can issue warnings in the account statements and discontinue ETC privileges for offenders. However, the agencies do not have authority to issue tickets based on the speed records.

In December 1999, the I-Pass system announced a new software application that calculates speed statistics of vehicles traveling between toll plazas. The application functions as a vehicle probe system, identifying identical pairs of tag readings and calculating travel times and speeds. Once pairs are identified, tag IDs are encrypted so the user can not be identified. Speeds and travel times are used only for real-time applications and discarded after 120 minutes. The application is part of an advanced traffic management and traveler information system that the Illinois State Toll Highway Authority is developing as a service to its customers. However, negative media attention was focused on the announcement, and, at the time of this report's publication, the agency had not decided how to proceed with the new technology.[88]

A number of factors could explain why the collection of anonymous link speed data evoked public perception problems but the collection of localized individual speed data for semi-enforcement purposes did not. One theory is that the public may better understand the rationale behind the collection of speeding data for discouraging speeding through toll plazas. The collection of link speed data for traveler information purposes may seem amorphous and unnecessary to some ETC members. On the other hand, the Illinois project could simple have received negative media interpretation.

Information Storage. Six of the seven agencies responding to this part of the survey report that records are kept of the application information indefinitely, even after an account is closed. One organization reports that application information is maintained for five years after an account is closed, as required by state laws, and then deleted.

Each lane of a toll collection system, whether manual, coin-operated, or electronic, creates a data record for each transaction that includes date, time, location (plaza and lane), fee (if variable), and sometimes vehicle classification. For ETC, a transponder number is also recorded, which is used to link to the customer account. These data streams can be aggregated into numerous traffic and revenue statistics. Most

ETC organizations use relational databases. Two of the older systems use flat file databases but have plans to upgrade their systems. Both types can compile various statistical reports as long as records are maintained live within the database. Transaction records are periodically purged from most databases, but permanently stored on some type of archiving medium. After archiving data, a recovery process must be performed before information can be accessed or queries made. Agencies have different practices in terms of what aggregate statistics are generated and reported and how long records are maintained live within the database. The following sections provide greater details about individual agencies' information storage practices.

E-Pass. The Orlando-Orange County Expressway Authority maintains live transaction records for 180 days before archiving on magnetic tape. A CD back-up of customer statements is also made. Aggregate lane statistics are recorded per hour, day, month and year. These statistics include total vehicle counts as well as breakdowns by toll classification (from axle counts) and payment method. Aggregate statistics are kept electronically for approximately two years. Other aggregate statistical information is reported on an as-needed basis in response to requests by research and planning organizations. The data on speeds through toll plazas are part of the individual transaction records that are purged every 180 days.

E-ZPass (NYTA). Transaction records are maintained live on the New York Thruway Authority's database for three months beyond the billing month. They are then archived on magnetic tapes. Aggregate statistical reports are generated on an as-needed basis.

EZ Tag. The Harris County Toll Authority stores live records for one year. Back-up files are made on magnetic tape and maintained off-site. The Authority currently uses a VMS based flat-file system, but is planning to upgrade the system.

FasTrak (SanDAG). Transaction records are maintained live on the database for 180 days before being archived. Archived files may still be accessed and reported.

FasTrak (CPTC). The California Private Transportation Company maintains records or transactions live for at least six months, and possibly longer, depending on database space. Records are then archived to an unspecified medium. The CPTA does generate some aggregate statistical reports. However, since CPTA is a private

organization, these are not public records. In particular, the CPTA does not release revenue statistics. Only the information provided in the CPTA's annual report to the California Department of Transportation becomes public record.

FasTrak (TCA). The Transportation Corridors Agency maintains live transaction records for 90 days and then archives records to magnetic tapes. The agency reports aggregate statistics by week on its web site. These include total weekly transactions, percent increase from the previous week, average daily transactions, average weekly transactions, percent of transactions using ETC during the peak hour, and percent increase from the week ending December 1, 1996. Monthly toll transaction and revenue totals are also presented.

K-Tag. Transaction records are maintained live on the Kansas Turnpike Authority's database for two years, after which they are archived to magnetic tape. Aggregate statistics are generated for monthly financial reports and annual reports. These include revenue statistics and vehicle count statistics by vehicle class. Hourly and daily vehicle count statistics are generated for special studies but are not recorded on a regular basis.

PikePass. The Oklahoma Transportation Authority maintains live transaction records for three months before archiving to magnetic tape. Although the database is currently a flat file system, the authority regularly generates statistics on revenue, traffic flows, lane usage, violations, and flow densities. The authority plans to upgrade its database system in the near future.

Toll Tag. The North Texas Tollway Authority maintains transaction records live on its database for two years. Floppy disk back-ups are kept as archives. Aggregate lane statistics are recorded on a daily basis and maintained electronically for about seven years. These include total traffic counts, breakdowns by payment method and vehicle classification (from axle counts), non-revenue generating vehicles (emergency, transit, etc.), and violation statistics. Monthly reports are generated from these statistics.

The survey reveals that transaction records are maintained live for periods of three months to two years, as indicated in Table 5. After this time period, records are archived and kept indefinitely. Magnetic tape is the most common archiving medium, used by eight out of nine agencies surveyed.

Table 5. Length of Time ETC Agencies Maintain Live Transaction Records

Time Period	**3 mo.**	**6 mo.**	**1 yr.**	**2 yr.**
No. of Agencies (out of 9)	3	3	1	2

Source: ETC agency surveys conducted by Valerie Briggs, November 1999 through January 2000.

Information Security. Information security measures are necessary to ensure the integrity and confidentiality of data. ETC agencies claim that they take information security very seriously and have multiple measures in place to protect data. All ETC organizations report that their customer databases are considered proprietary to their agency and that external access is prevented through firewalls or local networks. In addition, internal access to customer account information is limited to selected employees on a need-to-know basis. Access control through passwords, logging of changes made to the database, and encryption of data during transmission are common features of all the systems in the survey. Two of the nine responding agencies require key cards to enter the facility where customer account information is stored, and one monitors employees in this area with surveillance cameras. This agency also performs daily quality control checks by reviewing 10 percent of the changes made to the database.

Routine calls for customer information are handled by customer service representatives. At least five of the agencies perform criminal screening and drug tests on these employees. All agencies report training customer service representatives on the handling and release of sensitive information. It is the policy of all organizations to provide customer information only to individuals listed on the account. All agencies report having procedures in place to ensure the identities of callers before providing information. These procedures are considered proprietary in some organizations. Among the others, these procedures range from requiring callers to supply addresses and phone numbers to specifying account numbers or personal identification numbers (PINs). Systems that allow customers to access account information over the internet use data encryption methods and require customer PINs for accessing data. Several agencies indicated a tightening of these security measures over the past few years. However, it should be noted that addresses and phone numbers are readily accessible public

information. Therefore, using these as a security mechanism could allow unauthorized individuals to access account information.

Secondary Data Uses. ETC agencies, for the most part, are protective of data and allow few secondary uses of data with the exception of aggregate statistical data. Aggregate statistics of toll facility usage and revenue generation are considered public information by all public toll agencies. Most organizations publish aggregate statistics (as indicated above) in monthly and annual reports, which are publicly available.

Marketing. Customer contact information is used for no purposes other than toll agency communications with customers in most ETC organizations. No agency will provide address lists to outside organizations. Only the CPTA, which is a private entity, will include external advertisements within its customer correspondence. A couple of public toll agencies and the CPTA do market co-promotions with other businesses through their mailings. An example of such a co-promotion between CPTA and the American Automobile Association (AAA) is that AAA gives $5 off AAA membership fees and $8 in free tolls to CPTA customers. Most ETC agencies report that they have received numerous requests from marketing organizations for customer contact information or for the right to advertise through agency mailings. Except as noted, these requests are not granted. Several agencies contract with outside companies to do their mailings. However, these companies sign agreements stating that they will not release or use customer addresses for any other purposes.

Law Enforcement and Litigation. No ETC agency allows any law enforcement agencies to have direct access to their records. Some agencies have law enforcement divisions within their organizations, and even these divisions do not have access to customer account or transaction data. Toll agencies will supply individual customer records to law enforcement agencies when a violation occurs involving an ETC customer or upon the customer's consent (such as in cases of vehicle or transponder thefts). Most agencies indicate a willingness to cooperate with law enforcement for purposes deemed appropriate by the agency. Two have provided customer information to aid murder investigations. Two regularly work with law enforcement on accident investigations, helping to identify potential witnesses or providing images from traffic monitoring

cameras. Just two of the agencies surveyed report that they will only give information to law enforcement under court order.

Regardless of agency policy, toll agencies are required by law to provide any information requested through a subpoena. All but one agency indicate that they periodically receive subpoenas for information, but not so many as to be considered a burden on the organization. Most subpoenas are for violation enforcement purposes or for marital disputes.

Planning and Research. All agencies use transaction data for the purposes of internal planning and traffic studies of the toll facilities. Most agencies indicate a willingness to cooperate with research studies performed by government organizations or for the public good. Three agencies of the nine regularly provide material to university researchers. In doing so, they do not provide any individual identifiers. One agency reported that it would only provide aggregate statistics to researchers and planners.

Interviewed personnel expressed the following opinions regarding the use of ETC data for research and planning purposes:

- It must be used for the public good.
- It should only be provided to government organizations.
- It should not be sold for third party uses.
- It should not be used for profit making enterprises.

Several agencies expressed concern about staff time required to compile and provide data.

Only one agency had a complete aversion to providing any material to outside organizations for research or planning purposes, stating that it would be a violation of the agency's customer agreement that states that information will be used only for electronic toll collection purposes. The agency feared that such sharing may discourage ETC use. The individual interviewed also indicated that controlling the types of organizations that could receive data would be impossible for a public agency. If data were released for one purpose, it must then be provided to any organization that requests it.

Secondary Applications. Radio frequency (RF) transponders can be used for a variety of purposes besides ETC. They are used to pay parking fees, provide entry to controlled access facilities, study traffic flows, track freight shipments, and for many other purposes. Tags issued by toll agencies could potentially be used in other ways. Toll agencies recognize this, and several now support activities that use ETC transponders for alternative purposes. Some of these purposes are provided to the customer as optional services to which the customer consents, others are uses of which the customer may not be aware. However, none of the uses requires ETC customer information to be divulged to outside parties.

The E-ZPass and FasTrak systems comprise multiple toll operating agencies with interoperable ETC systems, so a customer of any one agency may use the entire system with only one account. Billing is done through the agency that maintains the customer account and generally only tag numbers are shared with other agencies. Thus, proprietary customer account information is not shared except in cases of violations. However, most E-ZPass and FasTrak agencies state in their customer license agreements that personal information may be shared with other organizations with which the agency has interoperability agreements.

Some toll agencies are beginning to offer additional customer services that utilize ETC transponders. Two agencies in the study are experimenting with allowing electronic parking services to be billed through ETC transponders. The services function similar to the interoperable toll systems, where billing is done through the customer's ETC account and only transponder codes are shared with electronic parking organizations. One agency hopes to extend these services to allow customers to pay for fast food and other commodities through their ETC accounts.

RF transponders are being used in several metropolitan areas to study traffic flow characteristics such as point-to-point travel speeds and individual trip making characteristics. ETC can be a source of transponders for these activities and are being utilized for these purposes in the New York and Houston metropolitan areas. Organizations other than the toll agencies are performing the traffic analysis. These organizations receive partial transponder codes from the transponder administrator, allowing them to detect transponders, but not to trace their identities. Most ETC

customers are unaware of these activities. Customer license agreements do not mention these uses. However, since the data are completely anonymous, these secondary uses are inherently no different than other forms of data collection about which road users are unaware, such as loop detectors in roadways.

Internal Policies. While most agencies have established practices relating to information collection, storage, use, and dissemination, not all of these practices are formalized in written policies. Four of the nine responding ETC agencies report that their organizations do not have formal written policies on information collection, dissemination, or use. Two organizations without formal written policies stated a desire to evaluate information requests on an individual basis and to avoid bureaucracy associated with formal policies. Existing data policies tend to vary significantly in their content and level of detail. For instance, the Transportation Corridors Agency claims that its data collection, dissemination, and storage practices are designated within a thick document that is not publicly available due to the detailed information about its information security mechanisms. On the other hand, the North Texas Tollway Authority maintains a general privacy statement. This statement and the information policy of the New York Thruway Authority are provided in Appendices I and J.

Legal Provisions Relating to Privacy. Public toll agencies are within the purview of state laws. As government agencies, they must comply with state open records laws. Most state government codes contain language authorizing toll agencies and governing their practices. These statutes rarely address information practices beyond their relation to state open records laws. Contracts between the toll agency and ETC customers also represent legal agreements that govern agency practices.

State Open Records Laws. No ETC agency has been forced to release proprietary customer information due to state public information laws. However, there is little consensus among agencies on whether personal information held by public toll agencies can potentially be accessed through state public information laws. Most of these laws mimic the federal Freedom of Information Act (FOIA). If an individual provides a written request for information held by a government agency, that information must be provided unless the agency seeks and wins an exemption from the state Attorney General.[89]

Of the eight public authorities surveyed, most believed that their records of personal information are automatically protected within the public information laws through clauses that exempt the disclosure of personal information. The Orlando-Orange County Expressway Authority is the only organization that has sought and won a specific exemption from the state open records law for personal identifying information held by the Authority. Organization representatives feel strongly that other ETC agencies should follow suit. One agency reported that it is confused on the subject and that it is examining whether an exemption is necessary to protect its ETC customers.

Customer Contracts. All toll agencies have contracts with ETC customers that establish responsibilities of both parties with regard to ETC accounts. Most contracts focus on customer responsibilities and contain few if any provisions relating to use of customer information privacy. The notable exceptions are contracts for FasTrak (TCA), EZ-Pass (RC), EZ-Pass (NYTA), and FastLane, all of which contain confidentiality or non-disclosure statements. For instance, the non-disclosure statement in the E-ZPass (NYTA) contract reads, "Customer Account information will not be disclosed to third parties without your consent except as permissible by law." However, the contract does not specify what information is subject to disclosure by law. The I-Pass contract takes the opposite approach stating, "Information contained in your I-Pass file may be subject to disclosure pursuant to law." These statements do little to clarify customer information privacy. Four agency contracts (the three FasTrak programs and FastLane) assert the agency's right to share information with other toll agencies for purposes of toll systems interoperability. Two (I-Pass and K-Tag) contain clauses authorizing the agencies to perform credit checks on customers.

Hence, while customer contracts may potentially be used as mechanisms to protect user privacy or to communicate privacy policies with customers, few toll agencies are using them for these purposes. In eight of the twelve cases studied, customer contracts do not limit or restrict how toll agencies may use customer information. Those that do are vague in terms of what information is subject to disclosure by law. However, some agencies have internal written policy statements addressing privacy of user information. While these may not constitute legally binding contracts, they do create an

expectation of privacy on behalf of the customer, which the agency may then be required to honor.

In addition, all contracts contain language stating that the agency may change the terms of the contract at any time with written notice to the customer. In all cases, use of the tag upon receipt of the notice implies customer agreement. While the intent of this clause is to allow changes in pricing or technology, it does not exclude changes to information privacy policies.

ELECTRONIC CLEARANCE

Electronic clearance (EC) automates the commercial vehicle inspection process at state weigh stations and ports of entry. It allows participating trucks that have proper credentials and are lawful to bypass inspection facilities. As a participating truck approaches an enforcement site, an in-cab transponder and AVI reader identifies the vehicle to the inspection facility computer. The computer, accessing a database of registered vehicles, verifies that the truck has proper state-mandated credentials and safety and registration requirements. The computer then sends distinct audio and visual signals back to the in-cab transponder to indicate whether the truck can pass the inspection facility or must pull-in. Bypass services are provided for some facilities in the main lines of the roadway, while others take place in-station.[90]

Roadside technologies include a series of AVI transceivers, the facility computer, and, at some sites, weigh-in-motion sensors. The first transceiver, located approximately a quarter- to a half-mile upstream of the station, detects the vehicle and sends its ID number to the weigh station computer. After verifying the truck's credentials, the computer transmits a message back to the truck's transponder via the second transceiver telling the truck to bypass or pull in to the station. A compliance transceiver then validates the bypass. Some stations also utilize high-speed weigh-in-motion sensors embedded in the roadway near the first detector that measure various weight and configuration characteristics of the truck for automatic vehicle classification and compliance purposes.

Benefits from EC accrue to both the trucking industry and the state. Bypassing trucks save time by not having to stop at inspection stations. As the percent of bypassing

trucks increases, non-bypassing trucks also save time due to shorter queue lengths at inspection facilities. A simulation study estimates time savings for non-equipped trucks to be up to 8 minutes per inspection station when approximately 60 percent of trucks are equipped for EC.[91] State agencies derive potential benefits from reduced operating costs and increased inspection efficiency; authorities are able to concentrate resources on those vehicles that pose the greatest safety risks. Evaluations of the HELP/Crescent operational test of integrated electronic screening technologies estimate benefit-cost (B/C) ratios of 0 to 12:1, with an average of 4.8:1, for government agencies implementing various elements of EC. Benefits are derived from reductions in tax evasions, damages due to overweight loads, and hazardous materials incidents, as well as lower government operating costs.[92] Another study estimated a B/C ratio of 7.2:1 for EC based on data from the state of Colorado.[93]

Electronic Clearance Systems

Two systems for EC currently exist in the United States: PrePass® and Norpass. PrePass® is a privately financed EC service run by a non-profit partnership between motor carriers and government agencies known as Heavy Vehicle Electronic License Plate, Incorporated (HELP, Inc.). The PrePass® system is financed through fees assessed to participating motor carriers per station bypass (approximately $1 per bypass). A private system operator, Lockheed Martin Information Management Systems (LMIMS), developed and operates the PrePass® system under formal agreement with HELP, Inc. The system operator also provides venture capital for development and implementation of the system. Thus, states pay only a membership fee to participate in HELP, Inc.'s governance. HELP, Inc.'s staff and Board of Directors, comprising one government and one motor carrier industry representative from each member state, identify potential service offerings, develop service standards, and oversee the performance of the system operator.[94]

All data collected through the PrePass® system are owned and controlled by HELP, Inc. Motor carriers participate in PrePass® by registering through HELP, Inc. After HELP, Inc. verifies carriers' credentials and safety information based on predetermined specifications for each state, carrier information is maintained within a

database owned by HELP, Inc. and used for the purpose of determining bypass status. State agencies cannot access this database, but are provided monthly reports of aggregate bypass statistics. Participating carriers receive monthly billing reports detailing bypass activities made by their vehicles.[95]

NORPASS (NorthAmerican Preclearance and Safety System) is also a public/private partnership between member states, the motor carrier industry, and TransCore, the system administrator. However, it is primarily publicly funded. Its membership comprises seven states that previously participated in two separate operational tests of EC technologies. Member states agree to build compatible and fully interoperable EC systems, allowing trucks to use a single application and transponder for bypasses in all states. The EC system technology is called Lynx. The states contract with TransCore to provide organizational and administrative support and serve as the transponder administrator, responsible for enrolling carriers into the program, verifying and updating carrier information, and maintaining a database of enrolled vehicles. A governing body that includes a Board of Governors and a Board of Directors, with one state and one motor carrier representative from each member jurisdiction, oversees and directs the program. Each state finances, owns, and operates its own EC technology. Thus, each state controls the recording and use of data collected through its EC system. Participating carriers are assessed an annual fee of $45 per transponder but pay no bypass charges.[96]

Privacy Issues in Electronic Clearance

Electronic clearance automates an existing state regulatory process. Therefore, it does not create new databases of proprietary information as does ETC; the information that is collected and stored through EC is the same as through existing manual processes. However, EC allows for greater reliability in information collection than manual processes. EC makes a record every time an equipped truck passes an inspection station, while in manual inspection processes not all trucks are inspected at every station. The greater reliability of EC creates privacy concerns associated with the ability to track vehicles and with data creep and secondary uses of information. The trucking industry fears that government agencies will use EC records to audit driver hour-of-service logs

and weight-distance tax records and for speeding enforcement. Thus, trucks using EC might be held to higher standards than others. Furthermore, convenient data collection methods may instigate the spread of unpopular weight distance taxation and lead to government mandates for transponder equipage of all trucks, which would be expensive for the industry.[97]

Many trucking companies, especially those in the for-hire industry, are also concerned with protecting the secrecy of their routes and movements. In an industry with low margins, competitive advantage can be gained by positioning assets to best serve potential freight flow markets. Thus, routes and vehicle positions are considered trade secrets of considerable value to many in the industry. There is some concern that competitors may be able to gain access to EC records, potentially divulging these trade secrets.[98]

Electronic Clearance Survey Results

Telephone interviews and electronic mail surveys were performed with key personnel from the PrePass® and NORPASS programs. Because NORPASS is a decentralized program with operations controlled within individual states, personnel from five NORPASS member states (Florida, Kentucky, Oregon, Utah, Washington) were interviewed as well as members of the NORPASS governing body and from TransCore. PrePass® surveys involved HELP, Inc. staff and personnel from LMIMS. Information about the two systems' membership and carrier participation levels is outlined in Table 6.

Table 6. Electronic Clearance Systems

	NORPASS	**PrePass®**
Organization Type	Public/Private Partnership	Public/Private Partnership
Primary Funding Source	Public	Private
Information Ownership	States	HELP, Inc.
Participating States	Florida, Georgia, Idaho, Kentucky, Utah, Washington[a]	Alabama, Arizona, Arkansas, California, Colorado, Illinois, Indiana, Mississippi, Montana, Nebraska, New Mexico, Oklahoma, Tennessee, West Virginia, Wyoming[b]
Active Accounts	1,100[c]	3,000[d]
Active Transponders	10,000[c]	110,600[d]

[a] NORPASS web site, accessed December 12, 1999, available from: http://www.norpass.com.
[b] PrePass® web site, accessed December 12, 1999, available from: http://www.prepass.com.
[c] Provided by John O'Connor, Service Center Director for Lynx/NORPASS, TransCore, December 14, 1999.
[d] Provided by Beth Rider, Director of Business Operations, Lockheed Martin Information Management Systems, January 26, 2000.

Information Collection and Storage. EC systems collect two types of information: screening information about carriers and trucks from which bypass status is determined and records of bypasses or inspections. The credentials and safety information required for PrePass® and NORPASS enrollment is the same information required for manual inspection processes.

PrePass®. Motor carrier enrollment procedures and requisite carrier information are described in HELP, Inc.'s PrePass® Enrollment Policy (Appendix K). PrePass® customer service representatives verify credential and safety information from applicants through the carrier's base state and determine bypass status in each member state depending on its individual requirements. An account is created for each carrier within the PrePass® database, which contains the following information: enrollment information (company name, billing and shipping addresses, phone number, and contact name), credential and truck information and corresponding status, status of transponders in a carrier's inventory, and bypass status per state. Credential and safety information is

reviewed and updated quarterly as long as the account remains open. Closed accounts are archived.

A bypass record is created and stored within the PrePass® database each time an enrolled truck passes an equipped inspection facility. Bypass records indicate the data, time, PrePass® site, PrePass® state, truck classification, lane, signal given (red or green), and weight for each equipped vehicle in a carrier's fleet. These records are used to generate monthly billing statements based on the carrier's fleet's bypass activities. Bypass records are purged after three months. Only aggregate statistics on daily bypass activities per site and per carrier are retained.

LMIMS maintains the PrePass® database. States do not have access to the database or to records of individual bypasses. States receive annual reports of vehicle enrollment and aggregate bypass activities at their sites from LMIMS. States also receive vehicle weight data from any weigh-in-motion technology installed at their sites.[99]

NORPASS. NORPASS's information technology system is twofold, involving individual states' motor carrier databases and a centralized database of NORPASS-enrolled carriers maintain by TransCore. TransCore's database contains credentials and safety information and per-state bypass status for each enrolled carrier and vehicle. These records are verified and updated approximately quarterly. Vehicles are approved for bypass after TransCore screens applications and final bypass approval is received from each state.

There is no standard protocol for linking member states' databases with TransCore's database of enrolled carriers. In Oregon, information from the TransCore database is downloaded directly into the state motor carrier database. In Florida, Georgia, and Kentucky, information from TransCore is fed to the inspection facility equipment as opposed to the state database. Idaho inputs carrier data into its own database from the NORPASS applications. Efforts are underway to standardize procedures among the NORPASS states.[100]

The majority of information collected through the Lynx system resides in member states' motor carrier databases. Roadside event data are generated during a bypass from sensors and equipment in the roadway and screening data. The information collected depends on the equipment and configuration of the particular sight and varies

significantly among states and facilities. These data may include bypass date and time, vehicle length, vehicle height, vehicle speed, vehicle axle weights, vehicle axle separations, random pull levels (i.e., percent of time vehicles are called into a station for manual inspection), weight thresholds, licensed carry weight, transponder number, and electronic clearance violations.[101] Simpler systems may just record data, time, and location of bypass, transponder unit number, carrier name, and U.S. DOT number (a registration requirement).[102]

The five NORPASS states interviewed reported different practices with regard to recording and storing Lynx data. The Florida State Patrol currently makes no record of electronic clearance bypasses, but is working to update its system so that it will retain bypass records. In Washington, Oregon, Utah, and Kentucky, Lynx bypass records are stored within the same database as manual inspection records. Oregon personnel report that bypass records do not vary in form from manual inspection records and that the two are indistinguishable within the database. The other three states' databases indicate whether the inspection was made manually or through Lynx.

Data storage time periods also vary among states. Washington keeps records live within the database for one year before archiving data indefinitely. Kentucky and Utah maintain live records for three years. Oregon maintains all records within its database indefinitely.

There is no centralized database of Lynx bypass activities across all states. TransCore service center personnel can view bypass records of some states, but can not access them or generate reports. TransCore relies on reports from states to determine total bypass statistics.

Information Security. All organizations claim to limit access to databases through user passwords and firewalls. Some state systems and LMIMS report using additional security mechanisms such as tracking of changes made to the database, employee background checks and training, and others.

Secondary Data Uses and Applications. Two of the primary factors that differentiate PrePass® and NORPASS are the level of state access to data and the ability of states to use data for secondary purposes. Because states in NORPASS own and operate their Lynx systems and the data generated, states control the use of data. With

PrePass®, LMIMS controls data access under the direction of the HELP, Inc. Board of Directors. HELP, Inc. staff claim that control of data through an independent, non-government entity was a requirement of motor carriers for participation in the HELP/Crescent federal operational test from which PrePass®' developed.[103] TransCore will serve as a third-party data administrator upon request of a NORPASS state, but has not received requests to do so. One of the motivations for NORPASS and its constituent programs was to allow states to control their own data.

PrePass®. HELP, Inc.'s Board of Directors established and approved an Event Data Retention Policy (Appendix L). Carrier-specific data are used only for purposes of operating the PrePass® system and are not provided to jurisdictions or outside parties without the permission of the individual carrier. HELP, Inc. will provide carriers information about their own records, but will not release information from other carriers' records. HELP, Inc. does not release carrier contact information or allow outside organizations to advertise products through PrePass® mailouts. However, HELP, Inc. does intend to develop and market add-on products to the PrePass® service. These would likely feature secondary uses of PrePass® transponders for such purposes as accessing facilities. These activities would be operated by LMIMS and would not require divulging customer information to outside organizations without the carrier's consent. Several outside vendors have approached HELP, Inc. about co-promotional activities, for instance, providing reduced insurance rates for PrePass® participants. HELP, Inc. staff indicate a willingness to participate in some of these activities but none had been implemented at the time of publication of this report.

HELP, Inc. has not established interoperability agreements with any other EC or ETC systems. However, it has developed a resolution outlining the conditions that it would use to guide decisions about systems interoperability (Appendix M). Among provisions of this resolution are requirements that other parties "must agree to protect data privacy and to fully disclose all specific uses of event data collected from carrier transponders" and that transponder identifiers will be shared only by request of the carriers.

NORPASS. Uses of bypass data vary by state within the NORPASS system. Utah and Florida personnel report that Lynx data are being used for no purposes other than to

allow electronic clearance. Washington State DOT uses bypass records to generate aggregate statistical reports. These may be used in the future in the state's pavement management program and possibly for other planning functions. Oregon and Kentucky both use Lynx data to audit driver hour-of-service logs and weight distance tax records that carriers submit. The states claim that this is not a breech of the ITS America Privacy Principles because the electronic event records are used no differently than manually collected records. Both states report requiring inspections of all trucks at every station; consequently, trucks using EC are not held to any higher standards than other vehicles.

In addition, one NORPASS state is considering the use of EC data for research and planning purposes. Kentucky has agreed to allow Reebie Associates to access EC records in an anonymous fashion. Reebie Associates is a consulting firm that produces an extensive multi-modal goods movement database used by government planning organizations and the freight industry. The company has been working with proprietary freight data for over 10 years. Although no actions have been taken to implement the transaction, possible arrangements have been discussed. The most likely scenario is that Reebie would assign a commodity code to each vehicle enrolled in the Kentucky EC program. These codes would be entered into Kentucky's EC database. Statistics would be generated based on the assigned commodity codes, which Reebie could then access. Thus, bypass records would be aggregated by commodity code for Reebie's use.

Several barriers exist to the implementation of the data exchange. Funding has not been provided for program support from Kentucky Transportation Center staff. There could be difficulties assigning commodity codes to fleets that carrier multiple commodities. Currently, only five percent of trucks traveling on Kentucky's highways are using EC. Therefore, officials doubt whether the information gained from the system would add significant value to Reebie's activities. However, officials are optimistic about the future potential for such applications as EC expands and is used by a greater number of trucks.[104]

Internal Policies. As described previously, HELP, Inc. maintains formal policies on carrier enrollment and data retention and a resolution on interoperability. These are attached in appendices K, L, and M.

The following statement represents NORPASS's data privacy policy:

> NORPASS jurisdictions will not use or distribute data and information available through electronic clearance operations in any manner that differs from current use of such data and information now gathered through manual means.[105]

Legal Provisions Relating to Privacy. All information held by state agencies is subject to state open records laws. However, NORPASS state representatives claim that individual carrier bypass records are not public information and that internal policies protect data from being released to outside parties. Most states report that they have never received requests for carrier data. Kentucky and Oregon have both received requests from carriers for information about their own fleet records. Usually these have been granted. Kentucky is the only NORPASS state that reports that it has received subpoenas for roadside event data.

HELP, Inc. does not have to comply with open records laws by virtue of its status as a private entity. According to LMIMS personnel, PrePass® data have never been subpoenaed.

CONCLUSIONS

Summary of ETC Survey Results

Information Collection

- Collection of individually identifiable information is limited to that which is necessary for customer billing and information security purposes. However, the collection of driver's license and social security numbers by some agencies may be unnecessary.
- Customers supply all personal, vehicular, and financial information. No additional information is collected about the customer except where credit checks are performed on delinquent accounts or for the purposes of extending customer credit.
- Anonymous and cash options are provided by most ETC organizations.
- Collection of anonymous link-speed data caused public outcry, whereas collection of individual speeds through toll plazas for issuing warnings has been publicly accepted.

Information Storage

- Customer account and transaction records are archived indefinitely and are accessible in most cases.
- Magnetic tape is the most common archiving medium.

Information Security

- All ETC systems employ technical security measures to protect electronic records from unauthorized changes or access.
- All ETC organizations use procedures to ensure that data are released only to authorized customers. However, these procedures may not be adequate in cases where public information is used to identify the customer.

Secondary Data Uses

- No agencies will release customer contact information for marketing purposes and most will not distribute advertisements from outside organizations.
- Law enforcement does not have direct access to ETC records. ETC data are never used for enforcement of speed limits. However, many ETC agencies will share customer data with law enforcement for serious criminal investigations and accident investigations without a subpoena.
- Agencies must release any information requested by subpoena.
- Willingness to provide information for outside research and planning is conditioned on the public value of the proposed activity, staff time required to participate, and whether the release of the requested data violates customer contracts or might endanger public trust. Current practice is to provide only non-identifiable data, or aggregate statistics.
- Use of ETC transponders for other purposes is acceptable as long as customers can remain anonymous and the activity does not require the ETC agency to release personal information.

Internal Policies

- Only about half of ETC agencies have formal written data policies. The others choose to review requests for information on an individual basis.

Legal Provisions

- ETC agencies have not had to release proprietary customer data under state government open records laws, and most believe that customer information is protected by existing exemptions for personal information. One agency sought a specific exemption for ETC information.
- All ETC organizations have customer contracts. Most do not address data confidentiality.

Summary of EC Survey Results

Information Collection

- EC creates a record of vehicles at every inspection facility, whereas manual inspections in most states do not. Therefore, EC could enable vehicle tracking while most manual inspections could not.
- Credentials and safety information collected about the carrier to determine bypass status is the same information as required for manual inspection processes.
- The content of bypass records varies depending on the equipment implemented at each site.

Information Storage

- HELP, Inc. centralizes EC records from all facilities in one database maintained by LMIMS. HELP, Inc. member states can not access individual carrier bypass records.
- NORPASS bypass records are distributed among member states' databases. Many NORPASS states combine EC and manual inspection records in the same database.
- HELP, Inc. discards bypass records after completion of the billing cycle (approximately 3 months).
- NORPASS states maintain bypass records at least one year.

Information Security

- All NORPASS states and LMIMS use technical measures to prevent outside access to their databases.

Secondary Data Uses

- PrePass® information is used only for EC. Carrier specific information is not released to any outside parties or to member states. Member states receive aggregate EC statistics and weight information.
- Some NORPASS states use EC and manual inspection records for auditing driver hour-of-service logs and weight-distance tax records.
- Kentucky has agreed to share bypass records in anonymous form with Reebie Associates for use in their freight flow database. No actions had been taken at time of publication.

Internal Policies

- Both systems outline practices related to data privacy in formal written policies.

Legal Provisions

- HELP, Inc is exempt from state and federal FOIA requirements.
- NORPASS states have never received requests for information except from carriers wanting access to their own records. Most believe that bypass records are protected from public disclosure by existing exemptions in open records laws.

Findings

The analysis of ETC and EC policies was performed to determine findings that may be applied to other technologies. This section describes these lessons learned.

Influence of Public Perception. Both ETC and EC organizations use public perception as a guide to their practices more so than laws or recommendations by ITS America. The success and ultimate benefits of ETC and EC systems depend on wide-scale use of the technology by their target groups. In general, system operators do not want to take any actions that might endanger this use. Thus, decisions about data use and access tend to be driven by operating organizations' interpretations of their customers' desires. HELP, Inc. is a prime example. States are not allowed to access individual carrier electronic clearance records for their own facilities because some in the motor carrier industry have insisted that they would not participate in an EC system in which states had this ability. This is causing agencies to take more conservative approaches to data sharing than required by law or voluntary privacy principles. For instance, many ETC organizations are reluctant to provide anonymous data for external research and

planning purposes for fear that these activities will be misinterpreted and denounced by the public. Thus, self-regulation has been largely successful for these ITS applications.

The media can have a significant influence on how the public perceives an ITS activity. This is apparent from the controversy surrounding the Illinois State Toll Highway Authority's attempt to use link speed data calculated from the ETC system to provide travel time information. The media construed this activity as a breech of privacy as opposed to the provision of a beneficial public service, and was successful in forestalling implementation of the program.

The Illinois example also illustrates the conflict between fully disclosing all uses of information and not wanting to elicit unwarranted public fears. Many organizations expressed a preference to "maintain a low profile" for some secondary data uses, such as using anonymous data for planning purposes or transponders as data probes. ITS America's privacy principles permit the secondary use of anonymous data without customer notification, but require notification for secondary uses of personally identifiable information. On the other hand, the "Fair Information Principles for ITS/CVO" state that all uses of data should be publicly disclosed. Therefore, EC organizations should make public any intended uses of data for planning, enforcement auditing, or other purposes and allow trucking industry customers to determine whether they want to participate.

Value of Customer Choices and Voluntarism. The provision of customer choices and the voluntary nature of the EC and ETC programs are critical for gaining public acceptance. All but one of the EC and ETC programs are voluntary, meaning that vehicles can travel along the same roads and pay tolls or be inspected by alternative means. The trucking industry has made it clear that voluntary participation is key to the industry's cooperation with EC. Oregon's attempt to make transponder equipage mandatory on trucks was brought to a halt by trucking industry opposition.[106] Furthermore, the Royal Automobile Club of Victoria, Australia, found that 11 percent of respondents to a survey about a proposed entirely electronic toll facility asserted that they would want an anonymous travel option at all costs to themselves, even if they might be charged in cases of equipment malfunctioning.[107]

The voluntary nature of programs provides a market incentive for operators to address user privacy issues. Some potential ITS users feel that having to vie for a customer base helps keep ITS operators honest about information uses. The trucking industry in particular fears that mandatory participation in ITS programs might lead to abuses of data.[108]

The other reason for voluntarism is that it allows potential customers to choose the option, anonymous or non-anonymous, that best suits their desires. Users of ETC and EC choose to entrust their proprietary information to system operators in return for certain benefits. However, as indicated by the Royal Automobile Club study, some individuals and presumably businesses value the privacy of their information more so than the benefits derived from the electronic systems. Making programs voluntary and providing choices, such as cash or credit card payment options in toll systems, allows all constituents to access systems via their preferred method.

Use of Opt-In Versus Opt-Out Approaches for Data Usage. ETC and EC organizations tend to operate under opt-in approaches despite the fact that they are not legally or contractually bound to do so. The voluntary nature of participation in the programs means that customers opt-in, agreeing to have certain information collected about them to be used for specific purposes. Once collected, individual information is not used for secondary purposes without the customer's permission. There are no laws that specify this treatment of data, nor do most agencies' customer contracts indicate how data will used. Therefore, agencies are not legally bound to use opt-in approaches. The lack of legal specification of opt-in approaches means that agencies are not required to use opt-in approaches should situations arise in which it is inconvenient or unfavorable to receive customer consent. The exchange of EC data between the Kentucky Transportation Center and Reebie could be such a case, depending on how it is handled. An opt-in approach would require the Kentucky Transportation Center to obtain customers' consent before providing a customer list to Reebie for assignment of commodity codes.

Separation of Functions. Experiences in ETC and EC suggest that there is a basis for providing institutional separations between multiple functions for ITS technologies or data. HELP, Inc. is a manifestation of this concept. An independent

organization was created to ensure that data collected through EC was used only for this purpose. NORPASS does not abide by this principle. Although there could be many reasons, PrePass® has significantly greater carrier participation than NORPASS. Other examples also point to the value of institutional separation of functions. The Illinois State Toll Highway Authority faced public opposition to its calculation of link speed data through the ETC system to provide travel time information. However, the Texas Transportation Institute (TTI) performs the same function using E-Pass transponders for the entire Houston metro area and has had no problems with public perception. The primary difference between the two programs is that, in Houston, the vehicle tracking and speed calculations are performed by a separate entity that does not collect individual identification information.

Public perception is the key reason for institutionally separating functions. The Illinois traffic monitoring program is technically very similar to TTI's, and privacy protections have been built in to ensure that vehicles are not identified through their toll records. However, institutional separation is more visible than internal privacy protection mechanisms and is therefore more publicly acceptable.

Treatment of Data by Public and Private Organizations. Different theories exist about whether the public or private sector is more capable of protecting proprietary data. Some point to federal and state FOIA requirements as barriers to the public sector's ability to protect data. They also fear that publicly held data will be used for enforcement purposes. On the other hand, proponents of the public sector cite its fundamental purpose of serving the public as a benefit and argue that the profit motives of the private sector may lead to selling of data. The findings of this research indicate that organizational goals and operating characteristics of an ITS service provider are better determinants of data treatment than simply whether the organization is a public or private entity. The following subsections discuss in greater detail issues related to public and private ITS data collection.

Protection of Data Under FOIA Requirements. While it is unclear whether EC and ETC data held by public entities are currently safe from public access under FOIA requirements, public agencies can take actions to protect proprietary data from FOIA requests. Agencies can request rulings from their attorneys general to determine whether

data are protected from release under current FOIA exemptions. If not, they can follow the path of the Orlando-Orange County Expressway Authority and request special exemptions from their state legislatures. In general, FOIA requirements are not intended to release personal information about individuals, but instead to provide transparency of public actions. Therefore, it is reasonable to expect that proprietary information collected through ITS can be protected from release through FOIA.[109]

Use of Data for Law Enforcement. There is truth to the argument that publicly held ITS data is more likely to be used for enforcement purposes or accessed by law enforcement. However, none of the public ITS agencies studied allow data to be used for speeding enforcement purposes or freely accessed by law enforcement. The use of ETC data by law enforcement has been for such purposes as apprehending serious criminals and accident investigations. These uses have not received public opposition and usually the data could have been obtained by subpoena. Those NORPASS states that use EC data for enforcement purposes beyond inspections make this fact publicly known and implement controls to ensure that EC users are not held to a higher standard than other trucks. Therefore, these organizations are within the bounds of ITS America's Privacy Principles.

Sale of Data and Use of Data for Marketing. According to this analysis, the private sector does appear to have greater incentive to sell or use personal data for external marketing purposes. Often public agencies are restricted in how they can collect revenue by their authorizing charters or other regulation, while the private sector is not. However, contracts made with users and fear of compromising public trust prevent uses of data for marketing purposes to a large extent. None of the organizations studied, public or private, sell or release customer information to outside groups. One private organization allows advertisements to be included in its mailouts. This could be considered a secondary use of contact information for marketing. However, it is commonly performed by many other private industries, such as banking and credit card companies, as well.

Sharing of Data for Research and Planning Purposes. Willingness to provide data for research or planning purposes received mixed responses from both public and private organizations. Purpose of the research or planning activity and terms of the data

sharing agreement were important to both public and private organizations. All organizations wanted to be sure that data confidentiality would be maintained and that the activity would in no way interfere with their core business activities. Both sectors were concerned with staffing time required to prepare data for release.

One primary difference expressed between public and private organizations was their expectations for compensation. Most public agencies indicated that they would not require payment for data beyond possible compensation for assembly costs. Private organizations stated that they would charge for any data access beyond that which is already publicly released.

Notes

[73] Holdener, Douglas J. "Electronic Toll Collection Information: Is Personal Privacy Protected?" *Compendium: Graduate Student Papers on Advanced Surface Transportation Systems*, Southwest Region, University Transportation Center Research Report # SWUTC/96/72840-00003-1, Texas Transportation Institute, Texas A&M University System (College Station, Texas, August 1996), pp. D-3 – D-4.
[74] Zhang, Wen et al., *A Primer on Electronic Toll Collection Technologies* Preprint. Tranportation Research Board, 74th Annual Meeting (Washington, D.C., January 1995).
[75] Zhang, Wen et. al., *A Primer on Electronic Toll Collection Technologies*; and *An ETTM Primer for Transportation and Toll Officials*, ATMS Committee and ETTM Task Force, Intelligent Transportation Society of America (Washington, D.C., March 1995).
[76] Pietrzyk, Michael C. and Edward A. Mierzejewski, "Electronic Toll Collection Systems: The Future is Now," *TR News*, No. 175 (November – December 1994).
[77] *An ETTM Primer for Transportation and Toll Officials.*
[78] "Automatic Vehicle Classification," *ETTM On The Web* (updated April 25, 1997), available from: http://www.ettm.com.
[79] "Video Enforcement Systems," *ETTM On The Web* (updated April 10, 1997), available from: http://www.ettm.com.
[80] Pietrzyk, Michael C. and Edward A. Mierzejewski, "Electronic Toll Collection Systems: The Future is Now."
[81] Ibid.
[82] *An ETTM Primer for Transportation and Toll Officials.*
[83] Pietrzyk, Michael C. and Edward A. Mierzejewski, "Electronic Toll Collection Systems: The Future is Now."
[84] *ETTM On the Web* (accessed December 14, 1999) available from http://www.ettm.com.
[85] Ibid.
[86] Holdener, Douglas J. "Electronic Toll Collection Information: Is Personal Privacy Protected?" pp. D-6 – D-7.
[87] Ibid., p. D-10.
[88] Telephone Interview by Valerie Briggs with Neil McDonald, Director of Operations, Illinois State Toll Highway Authority, January 3, 2000.
[89] Telephone Interview by Valerie Briggs with Bob Andrews, Community Relations Officer, Texas Department of Transportation, Austin, Texas, January 24, 2000.
[90] "Strategic Business Plan" (draft), HELP, Inc., (Phoenix, Arizona, July 6 1998), p. 4.
[91] Glassco, R., et al., "Studies of Potential Intelligent Transportation Systems Benefits Using Traffic Simulation Modeling: Volume 2," Mitretek Systems, MTR 1997-31 (June 1997), from "Intelligent Transportation Systems Benefits: 1999 Update," electronic report, U.S. Department of Transportation, available from http://www.mitretek.org/its/benicost.nsf/.
[92] "The Crescent Project: An Evaluation of an Element of the HELP Program," The Crescent Evaluation Team, Executive Summary and Appendix A (February 1994), from "Intelligent Transportation Systems Benefits: 1999 Update," electronic report, U.S. Department of Transportation, available from http://www.mitretek.org/its/benicost.nsf/.
[93] Study of Commercial Vehicle Operations and Institutional Barriers, Appendix F, Booz, Allen & Hamilton, McLean, Virginia (November 1994), from "Intelligent Transportation Systems Benefits: 1999 Update," electronic report, U.S. Department of Transportation, available from http://www.mitretek.org/its/benicost.nsf/.
[94] "Heavy Vehicle Electronic License Plate, Incorporated," PrePass® web site (accessed December 1999), available from http://www.prepass.com/help.htm.
[95] Telephone Interview by Valerie Briggs with Gail Peters, Administrator, HELP, Inc., Phoenix, Arizona, March 30, 1999.
[96] Telephone interview by Valerie Briggs with John O'Connor, Service Center Director for Lynx/NORPASS, TransCore, December 8, 1999.

[97] Briggs, V., T. Delk and C.M. Walton, *Public-Private Partnerships for Providing ITS: Case Studies in Transportation and Other Industries*, Southwest Region, University Transportation Center Research Report # SWUTC/99/472840-00067-1, Center for Transportation Research, The University of Texas at Austin, January 1999.
[98] Telephone interview by Valerie Briggs with Kevin Holland, Manager, Technology Policy, American Trucking Association, January 3, 2000.
[99] Telephone interview by Valerie Briggs with Jim Gentner, Vice President, HELP, Inc., Phoenix, Arizona, December 20, 1999.
[100] Telephone interview by Valerie Briggs with John O'Connor, Service Center Director for Lynx/NORPASS, TransCore, December 8, 1999.
[101] Electronic mail correspondence from Douglas Deckert, Systems Architect for CVISN, Washington State Patrol, to Valerie Briggs, December 14, 1999.
[102] Telephone Interview by Valerie Briggs with Jeff Bibb, Assistant Director, Department of Vehicle Regulation, Kentucky Transportation Cabinet, January 13, 2000.
[103] Telephone interview by Valerie Briggs with Jim Gentner, Vice President, HELP, Inc., Phoenix, Arizona, December 20, 1999.
[104] Telephone Interview by Valerie Briggs with Joe Crabtree, Director, Kentucky Transportation Center, January 21, 2000.
[105] Electronic mail correspondence from Gene Bergoffen, Executive Vice President, NORPASS to Valerie Briggs, January 24, 2000.
[106] Telephone interview by Valerie Briggs with Kevin Holland, Manager, Technology Policy, American Trucking Association, January 3, 2000.
[107] Ogden, K.W., "Privacy and Electronic Toll Collection in Austrailia," *6th World Congress on Intelligent Transportation Systems* (Toronto, Canada, November 1999).
[108] Ibid.
[109] Telephone interview by Valerie Briggs with Bob Andrews, Community Relations Officer, Texas Department of Transportation, Austin, Texas, January 24, 2000.

Chapter 5. The Use of Sensitive ITS Data

Data generated through ITS applications often have multiple potential uses and users. Both real-time and archived data may have value to various groups. Users include public and private sector organizations and individuals. Transportation operators, planners, and users of transportation systems for public or commercial purposes all value better transportation information. In addition, all businesses served through the physical transportation system may benefit from better data. Thus, the potential market for data is very large.

The ITS market is far from mature. Additional applications, services and markets for information are expected to evolve as the implementation of basic ITS infrastructure expands. Classifying this market and determining how to serve it is a difficult task, however. Much of the public emphasis on ITS prior to the late 1990s, with the development of the Archived Data User Service (ADUS) within the National ITS Architecture, was on applications for real-time operations. However, ADUS, along with related workshops and reports, has brought attention to potential uses of archived data for research, planning, and other purposes. ITS-generated data are now being recognized as a valuable resource to replace or augment traditional labor-intensive data collection methods.

The private sector is also interested in archived ITS data. Having a better understanding of traffic flows and characteristics will improve traffic information services and may aid companies in the development of dynamic route guidance systems. Real estate developers, insurance companies, product marketers, and shippers and distributors of goods could also benefit from better information about travel patterns. Reports from in-vehicle diagnostic systems may help manufacturers design better vehicles. The possibilities are limitless. Market studies and experimentation have been conducted to try to assess private markets for ITS services and generated information, but predicting all potential applications and markets is virtually impossible.

Privacy concerns become especially relevant to discussions of archiving and secondary uses of data. While information used in real time has the potential to be invasive to individual privacy, records of information concern privacy advocates the

most. Records may potentially be accessed by multiple parties for various purposes without the knowledge or consent of the individual entity about whom the record is made. While some of these purposes may be acceptable to the individual, others may not. It is important for individuals to understand these potential uses of information collected about them and have choices about whether to participate. It is the responsibility of the information collecting agency to protect the privacy of individuals by controlling access to sensitive data, appropriately sanitizing records, and obtaining customer consent for all uses of individually identifiable data.

While this may sound straightforward, many complications arise. For many planning and market research applications, disaggregated data are preferred to aggregated data, and the ability to attach characteristics to individual records is also desired. Many of these projects could provide substantial public benefit. Thus, a need arises to establish forums by which data may be accessed in appropriate forms for legitimate purposes without compromising the privacy expectations of individuals.

This chapter first discusses uses of sensitive data collected through ITS. The basis for this discussion is material produced for the National ITS Architecture Archived Data User Service and interviews with selected ITS professionals and operators. The final part of the chapter presents potential forums and tools by which sensitive data may be shared among agencies. Several potential models for data sharing are explained, and existing case study examples are provided.

USES OF ARCHIVED ITS DATA

The ADUS architecture provides a framework in which transportation information collected by ITS could be made available to a wide variety of stakeholders for data analysis and exploration.[110] The impetus for the creation of ADUS was a growing recognition among stakeholders of the value of archived ITS data for multiple purposes. A series of workshops and studies preceding the development of ADUS were dedicated to the topics of identifying data needs of various stakeholder groups to serve as a guide to ADUS.[111] The results of these workshops were compiled into an addendum to the ITS program plan and a set of user service requirements before being included in Version 3.0 of the National ITS Architecture.[112] Table 7, indicates stakeholder groups

with a potential interest in archived ITS data, as identified through the “ITS as a Data Resource” activities conducted in 1998.

The ADUS material goes on to define potential uses of various ITS data sources and suggested archiving procedures for the data. The material includes two detailed tables; the first defines potential uses of specific data elements collected through various ITS sources, and the second describes recommended archiving procedures for these elements. The majority of ITS data elements do not have significant privacy implications in that they can not be linked to a specific individual or vehicle. However, some ITS data elements have the potential to elicit privacy concerns, depending on how the data are collected and handled. The portions of the tables from the ADUS material that might have privacy implications are included in Tables 8 and 9 .

Table 7. Stakeholders for Data Generated by ITS

Stakeholder Group	**Primary Transportation-Related Functions**	**Example Applications**
MPO and state transportation planners	Identifying multimodal passenger transportation improvements (long-and short-range); congestion management; air quality planning; develop and maintain forecasting and simulation models	• congestion monitoring • link speeds for TDF and air quality models • AADT, K- and D-factor estimation • temporal traffic distributions • truck travel estimation by time of day • macroscopic traffic simulation • parking utilization and facility planning • HOV, paratransit, and multimodal demand estimation • congestion pricing policy
Traffic management operators	Day-to-day operations of deployed ITS (e.g., Traffic Management Centers, Incident Management Programs)	• pre-planned control strategies (ramp metering and signal timing) • highway capacity analysis • saturation flow rate determination • microscopic traffic simulation -- historical -- short-term prediction of traffic conditions • dynamic traffic assignment • incident management • congestion pricing operations • evaluation and performance monitoring
Transit operators	Day-to-day transit operations: scheduling, route delineation, fare pricing, vehicle maintenance; transit management systems; evaluation and planning	• capital planning and budgeting • corridor analysis planning • financial planning • maintenance planning • market research • operations/service planning • performance analysis planning • strategic/business planning
Air quality analysts	Regional air quality monitoring; transportation plan conformity with air quality standards and goals	• emission rate modeling • urban airshed modeling
MPO/state freight and intermodal planners	Planning for intermodal freight transfer and port facilities	• truck flow patterns (demand by origins and destinations) • HazMat and other commodity flow patterns

Stakeholder Group	Primary Transportation-Related Functions	Example Applications
Safety planners and administrators	Identifying countermeasures for general safety problems or hotspots	• safety reviews of proposed projects • high crash location analysis • generalized safety relationships for vehicle and highway design • countermeasure effectiveness (specific geometric and vehicle strategies) • safety policy effectiveness
Maintenance personnel	Planning for the rehabilitation and replacement of pavements, bridges, and roadside appurtenances; scheduling of maintenance activities	• pavement design (loadings based on ESALs) • bridge design (loadings from the "bridge formula") • pavement and bridge performance models • construction and maintenance scheduling
Commercial vehicle enforcement personnel	Accident investigations; enforcement of commercial vehicle regulations	• HazMat response and enforcement • congestion management • intermodal access • truck route designation and maintenance • truck safety mitigation • economic development
Emergency management services (local police, fire, and emergency medical)	Response to transportation incidents; accident investigations	• labor and patrol planning • route planning for emergency response • emergency response time planning • crash data collection
Transportation Researchers	Development of forecasting and simulation models and other analytic methods; improvements in data collection practices	• car-following and traffic flow theory development • urban travel activity analysis
Private sector users	Provision of traffic condition data and route guidance (Information Service Providers); Commercial trip planning to avoid congestion (carriers)	

Source: Margiotta, Richard. *ITS as a Data Resource: Preliminary Requirements for a User Service*, prepared for Federal Highway Administration, Office of Highway Information Management (Washington, D.C., April 1998), pp. 4-5.

Table 8. ITS Data Relevant for Archiving

ITS data source	Primary data elements	Features of the Data Source			Real-time uses	Possible multiple uses of ITS-generated data
		Typical collection equipment	Spatial coverage	Temporal coverage		
FREEWAY AND TOLL COLLECTION						
Visual and video surveillance data	• time • location • queue length • vehicle trajectories • vehicle classification • vehicle occupancy	•CCTV •aerial videos •image processing technology	Selected locations	Usually full-time	• coordinate traffic control response • congestion/queue identification • incident verification	• Congestion monitoring • Car-following and traffic flow theory
Vehicle counts from electronic toll collection	• time • location • vehicle counts	Electronic toll Collections Equipment	At instrumented toll lanes	Usually full-time	Automatic toll collection	• Traffic counts by time of day
VEHICLE AND PASSENGER INFORMATION						
Vehicle probe data	• vehicle ID • segment location • travel time	• probe readers and vehicle tags • GPS on Vehicles • Cellular geolocation	GPS and cellular geolocation are area-wide; readers restricted to highway locations	Usually full-time	• coordinate traffic control response • congestion/queue identification • incident detection • real-time transit vehicle schedule • adherence • electronic toll collection	• congestion monitoring • link speeds for travel forecasting models • historic transit schedule adherence • traveler response to incidents or traveler information • O/D patterns
Vehicle trajectories	• location (route) • time • speed • acceleration • headway	• AVI or GPS Equipment • Cellular geolocation • advanced video image Processing	AVI restricted to reader locations; GPS and cellular geolocation are area-wide	1-10 second intervals	Collected as part of surveillance function	• Traffic simulation model calibration for local conditions (driver type distributions) • Modal emission model calibration • Traffic flow research
TMC and Information Service Provider generated route guidance	• time/date • O/D • route segments • estimated travel time	TMC/Information Service Provider Software	Usually area-wide	Hours of TMC operation	Traveler information	• O/Ds for TDF model inputs • Interzonal travel times for TDF model calibration
TRANSIT AND RIDESHARING						
Rideshare requests	• time of day • O/D	computer-aided dispatch (CAD)	Usually areawide	Day time, usually peak periods	Dynamic rideshare matching	• travel demand estimation • transit route and service planning
INCIDENT MANAGEMENT AND SAFETY						
Incident logs	• location • begin, notification, dispatch, arrive, clear, depart times • type • extent (blockage) • HazMat • police accident report reference • cause	• CAD • computer-driven logs	Extent of Incident Management Program	Extent of Incident Management Program	Incident response and clearance	• incident response evaluations (program effectiveness) • congestion monitoring (e.g., % recurring vs. nonrecurring) • safety reviews (change in incident rates)

COMMERCIAL VEHICLE OPERATIONS						
HazMat cargo identifiers	• type • container/package • route • time	CVO systems	At reader and sensor locations	Usually full-time	• Identifying HazMat in specific incidents • routes for specific shipments	• HazMat flows • HazMat incident studies
Fleet Activity Reports	• carrier • citations • accidents • inspection results	CVO inspections	N/A	Usually summarized annually	May overlap with SAFETYNET functions	
Automatic vehicle Classification system	• vehicle classification • vehicle weight	•loop detectors •WIM equipment •video imaging •acoustic	Usually 50-100 per state; by lane	Usually full-time	Pre-screening for weight enforcement	• Truck percents by time of day for TDF and air quality models • Truck flow patterns • Pavement loadings
Border Crossing	• counts by vehicle type • cargo type • O/D	CVO systems	At reader and sensor locations	Usually full-time	Enforcement	Freight movement patterns
Cargo identification	• cargo type • O/D	CVO systems	At reader and sensor locations	Usually full-time	Border Clearance activities	Freight movement patterns
On-board safety data	• vehicle type • cumulative mileage • driver log (hrs. of service) • subsystem status (e.g., brakes)	CVO systems	At reader and sensor locations	Usually full-time	Enforcement and inspection	Special safety studies (e.g., driver fatigue, vehicle components)

Source: Margiotta, Richard. *ITS as a Data Resource: Preliminary Requirements for a User Service*, prepared for Federal Highway Administration, Office of Highway Information Management, (Washington, D.C., April 1998), pp. 10-13.

Table 9. Requirements for Archived Data from ITS for Multiple (Nonreal-Time) Uses

Primary Data Element or Record Type	**Definition**	**Units**	**Internal Data Structure and Data Reduction Cycle**	**Level of Accuracy**
Commercial vehicle cargo type	The SIC code for the type of cargo being transported.	SIC code	These data are collected by CVO systems, usually field sensors that detect the passage of individual trucks. The data should include time, location, and a vehicle identification code. Archiving data from every truck would probably not be cost effective; however, provision to permanently store a sample of data should be made.	90-95% accuracy
Commercial vehicle origin and destination	For the shipment being made by this vehicle, the first point of origin and last destination.	Prevailing location referencing system		Unknown
Intermodal container cargo type	The SIC code for the type of cargo being transported and the type of container.	SIC	Same as for commercial vehicle cargo and O/D.	90-95% accuracy
Commercial vehicle origin and destination	The first point of origin and last destination for the container.	Prevailing location referencing system		Unknown
Hazardous material cargo type	Hazard class and U.N. numbers (where appropriate) from the placard (multiple entries allowed).			95-100% accuracy
Hazardous material pre-planned shipment route	The specified route to be taken for hazardous material shipments that require such treatment.	Highway routes (as determined by the issuing agency)		Unknown
Commercial vehicle driver log	Selected locations and dates/times to determine hours of service for drivers.	Prevailing location referencing system	These data are collected from on-board safety systems that are downloaded to field sensors. Archiving data from every truck would probably not be cost-effective; however, provision to permanently store a sample of data should be made. Privacy concerns may preclude the collection of these data.	95-100% accuracy
Segment travel times and locations	The time for a probe vehicle to traverse a given roadway segment	Seconds	For permanent storage, probe information (times at given points on the highway system) should be converted to total seconds. The data should be permanently stored online as 5-minute summaries (total probes counted, average travel time). A supplemental data item for permanent storage is the segment length. The raw probe data may be stored offline if actual vehicle identification is not included.	+/-10%
Rideshare requests	The origin and destination of rideshare patrons by time of the request	Prevailing location referencing system	Data should be permanently stored by individual request.	95-100% accuracy

Source: Margiotta, Richard. *ITS as a Data Resource: Preliminary Requirements for a User Service*, prepared for Federal Highway Administration, Office of Highway Information Management (Washington, D.C., April 1998), pp. 30-34.

POTENTIAL USES OF SENSITIVE DATA COLLECTED THROUGH ITS

The ADUS material does little to define private markets for ITS data; nor does it indicate what groups might have an interest in sensitive data collected from ITS. Therefore, a survey and literature search were conducted for the purposes of determining these factors. The survey consisted of interviewing users and collectors of sensitive ITS data. The interviews focused on uses of potentially sensitive information collected through ITS. Collectors of ITS data were asked

- how data was being used internally,
- what outside groups had requested data and for what purposes, and
- for what additional purposes might data be used in the future.

These questions were included as part of the surveys conducted of ETC and EC agencies. Other organizations involved in data collection that were interviewed include university-based research organizations, consultants, private brokers of transportation information, and associations representing the telecommunications and trucking industries. Potential users of ITS data were asked to clarify how data collected through ITS could be beneficial to their activities and how ITS data compared to other sources of information. Researchers, consultants, and private brokers of transportation information were targeted for these interviews. Several "ITS experts" from ITS America, U.S. DOT and various consulting firms were also interviewed to determine their insights on the subject. A complete list of interviewees and the interview forms are in Appendices C and D.

Public Sector Freight Planning

Data elements collected from commercial vehicle operations systems constitute a significant portion of Tables 8 and 9. Any information collected about a specific motor vehicle, including cargo type, origin/destination, routes, driver logs, and safety records, is proprietary to the carrier. At the same time, this information can be very valuable for public and private freight planning efforts, as explained by John Kaliski in a document prepared for ITS America entitled "ITS Data for Freight Planning."[113]

Traditionally, freight transportation has been the domain of the private sector, and the public role has been limited to providing infrastructure funding through modal trust funds and taxing and regulating use of freight transportation systems. However, in recent decades, as the public sector came to understand the impact of freight transportation on a regional economy, state and local governments have focused more attention on planning for and managing key elements of the freight transportation system. The Intermodal Surface Transportation Efficiency Act (ISTEA) of 1991 acknowledged the importance of freight movement and required consideration of freight and goods movement in state and metropolitan transportation plans.

However, there are significant deficiencies in data available for freight planning efforts. The following excerpt from Kaliski's document describes these deficiencies:

- Congestion Management – State DOTs and Metropolitan Planning Organizations (MPOs) generally have adequate data – road maps, traffic counts, accident records, traffic engineering studies, etc. – to identify congestion bottlenecks and analyze their causes. What usually is missing for freight planning purposes is information about the number of trucks and types of commodities delayed by traffic congestion.
- Intermodal Access – State DOTs and MPOs generally have simple inventories of the major intermodal facilities in their jurisdiction, but often lack time-series data on the truck movements into and out of these facilities. They also may lack information on specific access problems, such as intersections and exit ramps that are too small for today's larger trucks; low bridges that force trucks to make long detours; and noise and safety problems when trucks must travel through neighborhoods.
- Truck Route Designation and Maintenance – State DOTs and MPOs typically have modest data on truck volumes and patterns. With the exception of a few specialized port agencies, however, state DOTs and MPOs have little knowledge of industry supply chains and distribution networks. Data are limited with respect to commodity flows, particularly for interstate or international traffic. Consequently, planners have little sense of the freight trip as a whole – its origin, modes of travel, routes, transfer points, destination, and reliability.

- Safety Mitigation – State DOTs and MPOs typically have inventories of rail-grade crossings and low-clearance bridges, and they may have collected data on intersections with high frequencies of truck-related crashes. They often lack data on the types of trucks that are involved in accidents, or the cost to industry from accident impacts and countermeasures.
- Economic Development – Planners have high-level data on the employment or revenue of the trucking industry, but little information is available about the value of freight flowing into or out of most metropolitan areas, shipment costs, and the time sensitivity of deliveries. Without these data, it is difficult to gauge the impact of congestion on business logistics practices and overall regional economic growth.[114]

Kaliski also describes how ITS technologies can be used to fill in some of these voids. His findings are summarized in Table 10.

Kaliski indicates that some of the most valuable tools for freight planning are vehicle tracking capabilities and information from carrier-owned fleet management technologies. However, use of such capabilities would be highly contentious within the freight industry. Kaliski suggests that information derived from the freight industry should be supplied on a voluntary basis and used only in aggregate form.[115] However, a framework would be necessary for collecting, aggregating and distributing this information.

Table 10. Freight Planning Applications of ITS Technologies.

Technology	**ITS Use**	**Freight Planning Opportunities**
Traffic surveillance technologies (loop detectors, infrared sensors, acoustic sensors, radar, CCTV)	Collect information about the status of traffic stream (counts, speeds, incidents)	Provide real-time data on truck travel times and speeds at specific points Provide detail on types of trucks and commodities
Automatic Vehicle Classification (AVC)	Vehicle counts and classifications	Inventory the type and volume of trucks using particular roadways
Dedicated Short-Range Communication (DSRC)/Automatic Vehicle Identification (AVI)/Automatic Equipment Identification (AEI)	Electronic toll collection Electronic roadside screening International border clearance Container identification Traffic management	Estimate travel times and speeds on certain corridors or around particular sites Estimate travel time reliability Estimate truck and container flows at intermodal facilities Suggest broad O/D patterns
Smart Cards	Gate access at terminals Driver licensing Electronic toll collection Electronic fuel purchasing	Determine the weight of trucks using particular roadways Assess potential pavement damage
Weigh-in-motion (WIM)	Truck weighings Electronic roadside screening	Determine the weight of trucks using particular roadways Assess potential pavement damage
Vehicle Tracking and Navigation Systems	Locate vehicles and cargo Estimate time of arrival Optimize routing and dispatching	Assess travel times and delivery reliability Estimate impact of congestion on business logistics practices

Source: Kaliski, John, "ITS Data for Freight Planning," prepared for ITS America, Washington, D.C., January 9, 1998.

Private Sector Freight Planning

The public sector is not the only user of freight data. The freight industry itself also values information about shipments, commodity flows, travel times, congestion, facility accessibility, and more. This information is the basis for many important business decisions about facility locations, shipment routes, service areas, rates and more. Primary customers of Reebie Associates, a firm that specializes in gathering and integrating freight shipment information, are private shippers, carriers, and industries that provide services and supplies to the freight industry. Thus, it appears that there is a substantial private market for freight information.

Transportation Demand Modeling

Transportation demand models are based on trip-making characteristics of individual travelers. Important characteristics often include number of trips made per day, time of day of travel, purpose of trips, mode choice, and distance of travel. This type of information is traditionally gleaned from travel surveys and trip making diaries completed by individual households. ITS tracking applications, such as cell phone geolocation, could potentially reduce the need for such surveys. However, this would require the tracking of individual probes over long periods of time, potentially revealing where the individuals live and work. The Wireless Communications and Public Safety Act of 1999 does not currently permit the location of a cellular user to be identified except for emergency purposes without the customer's consent.

Similar planning activities could be envisioned with license plate reading technology. For instance, to determine the origins of vehicles traveling on a certain roadway segment or entering a commercial establishment, vehicle license plates can be read and then cross-referenced with a vehicle registration database to determine the owner's home address. While privacy advocates may not object to such activities for public planning purposes, the potential for such a system to be used for other purposes, such as marketing, are great. This is an area that may merit future consideration by lawmakers.

Accident Investigation and Safety Analysis

Both the safety research and accident investigation communities are eager to have access to ITS video images of accidents and incidents for investigation purposes. Although the ADUS material recommends logging of certain parameters associated with accidents and incidents, it does not include video images. Traffic management centers (TMCs) typically do not save video images for fear that they will be overwhelmed with subpoenas for the data and that the images may open them up to litigation. However, steps could be taken to develop a forum for archiving data that would allow safety researchers to access the information they are interested in without risk to the TMC.

Traveler Information Products

ITS America's Advanced Traveler Information Systems committee has identified the travel "data gap" as a critical issue affecting rapid deployment of traveler information services.[116] In other words, sufficient traffic information does not exist in most areas to provide valuable traveler information to customers. As indicated previously, the ability to use cellular phones as traffic probes could do much to overcome this problem. Only aggregate information from many probes would be necessary to obtain basic traffic information for much of a transportation network.[117] Such a use would lead to few privacy concerns.

There is also the potential for cellular phones to be used for individualized transportation services. For instance, customized traffic information based on a vehicle's location could be provided to individuals calling a traveler information service. Dynamic route guidance may also be possible. A vehicle's location, along with up-to-the-minute traffic conditions, could be transmitted to an in-vehicle navigation system that would process this information and propose the most efficient route for a traveler. Services that rely on locating individual cell phone users require customer consent by law. Voluntary use of such services could be considered customer consent as long as the customer is aware that his location is being pinpointed. In addition, standards should be set about what part of this information is archived.

Product Marketing

Product marketers are interested in information about consumer activity in order to target marketing efforts. Most of the ETC organizations surveyed reported that they frequently receive requests from marketers to advertise directly to ETC customers. Marketers know that ETC customers are likely to frequently travel on and around toll facilities. Vehicle tracking capabilities, such as cell phone geolocation and license plate reading, could provide marketers with a wealth of information about where individual consumers travel, how far they are willing to travel for certain products, and so forth. Devices that provide two-way communication between a vehicle and an outside facility and enable the vehicle's location to be determined provide a platform for targeted marketing. It can safely be assumed that marketing firms would be willing to pay for any

valuable information about consumer behavior and for the right to advertise to consumers.

Unless prohibited by state laws from tracking vehicles or from accessing vehicle registration databases, marketers could presumably perform independent studies using vehicle license plate readers. As previously mentioned, this is an area that may merit future consideration by lawmakers.

On the other hand, access to information obtained through cellular phone geolocation could be controlled through cellular phone companies. While aggregate information derived from cellular geolocation can be released by the cellular provider, information about individual users can not legally be released without the customer's consent. It is possible to imagine services that would provide something to the customer, such as traffic information, in exchange for rights to use the customer's location information.

Commercial Real Estate Development

Commercial real estate developers are interested in much the same information as product marketers. They want to understand consumers' travel behavior in order to make informed business location decisions. Developers may also benefit from information about traffic volumes and congestion. Many of these needs can be met with aggregate data. Therefore, it is conceivable that developers may be able to work with cellular service providers to obtain the information they desire. Alternatively, public information about traffic flows generated by TMCs may provide the real estate industry with valuable information. It can be assumed that real estate developers would be willing to pay for information that could not be obtained from public sources.

FORUMS FOR ARCHIVING AND DISTRIBUTING SENSITIVE INFORMATION

The previous section makes clear that there are legitimate uses of sensitive data collected through ITS for both public and private sector applications. At the same time, it is important that privacy concerns be considered in decisions about how this information be collected, archived and distributed. In some cases, legal actions may be warranted. In other cases, institutional mechanisms can be designed to provide an acceptable level of privacy. Organizations should abide by ITS America's Privacy Principles in determining

data practices. The findings in chapters 4 and 6 of this document also provide guidance to ITS data collectors for establishing data handling practices. However, these guidelines do little to address the legitimate external uses and potential secondary markets for these data. Data collectors should be aware of these needs and, where appropriate, provide forums through which data can be accessed.

Potential forums may be through the data collecting agency itself, or may involve an outside "information broker." Information brokers, known as infomediaries in the computer world, would gather data from multiple sources, sanitize the data to alleviate any individually identifiable information, and make the data available to interested parties. These infomediaries may be either public or private entities. Brokers of transportation information already exist. Firms such as Reebie Associates, SmartRoute Systems, and ETAK collect, transform, and distribute transportation information. University research organizations are also fulfilling this role, as demonstrated by the Texas Transportation Institute's DataLink project. Regional transportation organizations, such as TRANSCOM in the New York City metropolitan area, may serve as infomediaries of ITS data within their region.[118] It is also conceivable to imagine a state or federal archive of ITS data. Brokering of ITS information may be done through an existing entity in conjunction with current activities or may invoke new business segments.

This section discusses potential forums for the distribution of ITS data. The first subsection describes licensing agreements, contracts that allow organizations to share proprietary information under controlled conditions and for legitimate purposes. This is followed by a presentation of various models for data distribution, along with case study examples.

Licensing Agreements

Conflicts between the desires of researchers for unsanitized data and promises made to keep data confidential are not new to ITS. Federal statistical agencies and research organizations have been collecting confidential data for many years. They allow researchers to access these data, under highly controlled conditions, through the use of

data licensing. Data licensing involves the signing of a formal contract between the data providing organization and a research team.
License agreements have the responsibility of ensuring that

- the data file is used only by a small group of designated file users, and
- the data are kept confidential as required by the licensing agreement as well as applicable laws and promises made to survey respondents.[119]

An established structure is necessary for the implementation of data licensing. This structure must include

- drawing up a legally binding contract by the data providing organization;
- implementation of methods for secure handling of the data by the data receiving organization; and
- establishment of enforcement procedures.[120]

Although the data licensing procedures described here refer to data collected by pubic institutions, licensing is an equally viable alternative for the release of business establishment files.

Personnel from the U.S. Census Bureau recently undertook a study of licensing agreements used by six government agencies and two university-based research organizations. They found a number of common elements among the forms examined.

- *Demonstration of the need for the data.* The principal researcher must demonstrate that the data are required for research, i.e., public use data are not adequate. The goals of the research that requires these non-public data must be stated in the application. The licensor must approve of the research before the application process can proceed.
- *Designation of the group of people that will have access to the data.* The principal researcher (PR) must supply a list of names of people who will be authorized to use the data. Those people must be informed of their responsibility not

to share the data with people outside the group. The PR must indicate the group's experience, if any, with handling other licensed datasets.

- *Legal aspects of the agreement.* The agreement specifies which people in the licensee's institution must sign the form. It also includes a statement concerning which law(s) protects the data (e.g., Privacy Act of 1974).
- *Data security and enforcement.* A data security program must be developed and implemented. The licensee's institution must allow inspections of the area where the data are used and stored. Penalties for violations of aspects of the agreement are listed on the form (e.g., denial of use of other data from licensor, fines, prison terms).
- *Restrictions on use of the data.* There is a requirement that no attempt will be made to determine the identity of respondents. The licensee cannot link the licensed data to other microdata files.
- *Restrictions on release of the research results.* Articles, reports, and statistical summaries must be reviewed by the agency before they are published or otherwise communicated. The results must adhere to the agency's disclosure limitation practices (e.g., all non-zero cells in a publicly released table must represent some minimum number of respondents).
- *Returning the data.* There is a specified limit to the duration of the license. It is often less than two years. The licensee is often required to return or destroy the original and any derived files.
- *Cost to the licensee* (not usually described in the form). Some licensors require user fees. One type is an up-front fee in the form of a security bond as surety for maintaining confidentiality. Also, the licensee must cover the cost of creating and maintaining a secure data handling environment.[121]

One problem with the use of licensing is that the burden of oversight and enforcement of the contract may be significant. Data collecting agencies must plan ahead and allocate funding for such activities where data licensing may be a possibility. Compensation for such activities from the data receiving organizations may be necessary,

especially in cases where the proposed research is not connected to the primary functions of the data collecting organization.

Models for ITS Data Distribution

Decentralized Approach. The approach that is commonly used now is for the data collecting agency to control access to data. Often this means that data are collected solely for the purpose of the collecting agency, and no outside groups are allowed access to the data. While this is in keeping with the ITS America Privacy Principles, it does not allow data to be used for other legitimate purposes. An alternative approach is for data collecting organizations to create a policy outlining a set of conditions under which data may be shared externally and with what groups. Licensing agreements and appropriate enforcement mechanisms can ensure that sensitive data remain confidential.

This approach allows some outside agencies to have access to data, while collecting organizations maintain direct control of their information. It is easier to implement relative to centralized approaches because it does not require the development of third party data distributors. It may also provide cheaper or free access to data relative to private infomediaries.

However, the approach has several disadvantages. It places a burden on the data collecting organization to develop structures for sharing information and to negotiate and enforce many individual licensing agreements. Some degree of data transformation to avoid release of all confidential information may be necessary, which would be an additional cost to the collecting organization. In addition, there is still a risk that data will be divulged by the licensee. The collecting organization may have little incentive to provide information for most outside purposes. Therefore, it may not be willing to incur the additional cost and risk involved with data sharing. Nor may it collect or store the data in a form that would be useful to other organizations. A fee could be charged to offset additional costs. However, most ITS data collectors are public agencies. The charging of fees for services by public agencies can create ethical issues. This approach also has disadvantages for organizations that want to access multiple ITS data sources. They may have to negotiate multiple contracts and merge data supplied in different forms.

Public Infomediary. An alternative approach is to establish a public infomediary at the state or national level. These public infomediaries could collect and archive ITS data from multiple public sources, filter sensitive information and make it publicly available to outside groups. Such a system would allow the integration of data from multiple sources and provide a single point of reference for ITS data. Certain government agencies, e.g., the Bureau of the Census, have established and respected practices for handling sensitive information and may have an easier time gaining public trust than private infomediaries. A derivative of this approach is for publicly funded research organizations to serve as infomediaries; such is the case with the DataLink research project at the Texas Transportation Institute.

However, there are several stumbling blocks for such an approach. First, funding must be made available to establish and operate the public infomediary. Since the benefits of the infomediary would be spread among multiple public and private groups, it is unclear where a single source of funding could be derived. Second, the infomediary would depend on public agencies voluntarily supplying their data. As in the decentralized approach, there may be little incentive and substantial risk for these organizations to do so. It is also relatively unlikely that private organizations would be willing to provide their data to the public infomediary. The trucking industry, which collects data that would be extremely valuable to some planners and researchers, is often distrustful of government motives and is wary of providing data to public entities. Other companies that provide services based on information derived through ITS have significant investments in their data collection techniques and are not likely to provide their data freely, except that which is already in the public domain. Since the ITS market is expected to be driven by the private sector, there could be significant data gaps within a public sector infomediary approach.

Private Infomediary. A private infomediary could collect and integrate data from multiple public and private sources and sell it to outside organizations in useful forms. Many of these types of organizations already exist, and a couple are profiled below. Private infomediaries are demand driven. They gather the information for which they see a market and assemble data into useful forms for those markets. Thus, infomediaries tend to specialize in specific kinds of information, such as freight data for

Reebie Associates or traffic and traveler information for SmartRoute Systems. Since information can be tailored to the needs of specific user groups, it alleviates the necessity for those groups to obtain data from multiple sources. Furthermore, a private organization may be better equipped to obtain information from other private sources, as demonstrated by Reebie's success at gathering data from the trucking industry.

The primary disadvantage of this approach is that data obtained through private infomediaries can be too expensive for many potential users. One of the primary user groups would be public sector organizations. Some in the public sector do not like the concept of buying information from a group that received information free of charge from other public agencies. However, this may create the opportunity for partnerships such as the one being discussed between Reebie Associates and the Kentucky Transportation Center, described below and in chapter 4.

One potential stumbling block to the private infomediary concept is that it may be difficult for new organizations to earn the trust of organizations from which they are collecting information. It has taken more than 10 years for Reebie Associates to reach its current level of trust with the trucking industry, and Reebie was originally backed with federal funds.[122] Data collecting organizations are more likely to entrust their proprietary information to organizations with proven track records with which they are familiar. Furthermore, established organizations have more to offer in cases where agencies provide raw data in exchange for discounts on data products or certain free services. Monopolies are likely to form in industries with such high barriers to entry. As in the case of Reebie, there may be grounds for government backing of certain private infomediary efforts to avoid the formation of monopolies and help to build public trust in these organizations.

Selected Case Studies of Transportation Data Distribution Efforts

This section provides profiles of several organizations that are currently collecting, transforming, and distributing transportation data. The Texas Transportation Institute acts as a public infomediary, while Reebie Associates and SmartRoute Systems could be classified as private infomediaries. The cases illustrate some of the characteristics identified in the models above. Although none of the cases serves as

information repositories to the extent described in the models, they provide platforms through which additional functions may be developed in the future. In addition, their experiences with data collection and research into market needs can provide insights to transportation professionals.

Texas Transportation Institute's DataLink. DataLink is an ITS data management system that arose out of the desires of Texas Transportation Institute (TTI) researchers to easily access and analyze data being collected by transportation management centers. The DataLink website explains the project's motivations and concept:

> In 1996, the TransGuide TMC in San Antonio was generating about 140+ Megabytes of data per day from inductance loop detectors on 26 miles of freeway around downtown. These TransGuide data were being compressed and archived, but the large data files were difficult to manipulate or analyze on most desktop computers. As revealed in a 1997 national survey conducted by TransLink researchers, the experience at other TMCs nationwide were similar to TransGuide. Many TMCs were archiving data collected by ITS components, but the ITS data were often inaccessible or difficult to analyze. The national survey also revealed wide variability in how and what aggregation level the data were stored.
>
> From this original need, TransLink researchers developed a concept for an ITS data management system that had the following features and/or functions:
>
> - Ability to store, access, and analyze large amounts of ITS data;
> - Easy-to-access database, with no special database software needed;
> - Intuitive graphical user interface, no programming or query language required; and
> - Provides summaries of original data as well as calculating performance measures.

> DataLink, as the ITS data management system is now called, was developed by TransLink as a prototype system for use by TTI researchers and as a "proof of concept" for examination by TxDOT. The DataLink system contains loop detector data aggregated to five-minute periods from Phase One of the TransGuide system in San Antonio. The loop detector data consists of vehicle volume, speed, and lane occupancy data collected from inductance loop detectors with nominal spacings of 0.5 mile. DataLink is updated daily with recent data, and contains continuous data dating from November 1997.
>
> The DataLink system is a large database that is accessible through a web browser. DataLink has a point-and-click interface for selecting query variables such as date, time period, data aggregation level, and roadway facility of interest. DataLink also provides flexibility in receiving query output, providing tables in the browser itself, comma-separated values through e-mail, and 2-D and 3-D graphics viewable using the free Adobe Acrobat Reader software.[123]

Currently, the DataLink system is available to a limited number of users, including those within TTI, TxDOT, and others that have expressed an interest. Because of increasing interest in DataLink, it is hoped that this prototype will be expanded and enhanced to create endless opportunities to explore ITS data.[124]

Although DataLink is designed around loop detector data, which are not considered sensitive information, a similar concept could be designed for sensitive data. However, for public release, sensitive information must be provided in anonymous form and adequately filtered and aggregated to avoid identification of individual units.

Reebie Associates. Reebie Associates (Reebie) is a consulting firm that produces an extensive multi-modal goods movement database, Transearch, used by government planning organizations, carriers, shippers, suppliers, financial firms, and logistics companies.[125] To produce Transearch, Reebie integrates information from a number of government databases with data it collects directly from trucking companies. Trucking companies supply shipment data to Reebie on a voluntary basis. In return, they receive market data that Reebie produces. The shipment data include volume, in various units,

by commodity type from origin to destination. Commonly, carriers compile a year's worth of shipment data and submit them to Reebie on diskette or CD. Records are either a compilation of each shipment or are aggregated by the carrier before submission. Reebie does not select a statistical sample of carriers, but receives information from any carrier willing to participate. Participants include many of the nation's leading truckload and less-than-truckload carriers and one major private carrier.

Reebie has been gathering data from trucking companies for over 10 years. The company attributes its success to its data confidentiality principles, the incentives it provides for carrier participation, and the fact that it does not ask for sensitive information. Reebie has written agreements with its participants specifying exactly how data will be utilized and that the company will not release data from any one carrier in any form. Rate information and shipper names are the greatest concern to carriers, according to Reebie; this information is never requested. Although route information is not collected, Reebie personnel do not think that carriers are concerned with releasing this information.[126]

Although Reebie is not currently utilizing ITS technologies, it is looking into ITS as a potential source of data in the future. The company has had discussions with Kentucky and received permission to access Kentucky's electronic clearance data in anonymous form. This is a result of arrangements made when the University of Kentucky purchased data products from Reebie. As described in chapter 4, under the proposed agreement, Reebie would receive records of electronic screenings at state inspection facilities aggregated by commodity code. Reebie acknowleges that other ITS data may also aid their activities but that it has not determined which ones.[127]

SmartRoute Systems. SmartRoute Systems, Inc. (SmartRoutes) provides information for a number of traveler information services. These include

- Route-specific, real-time traffic and transit information;
- Up-to-date weather conditions;
- Turn-by-turn street directions;
- Real-time flight arrival and departure times;

- Rental car, hotel, restaurant, and entertainment listings; and
- Personalized information services.[128]

The company collects real-time traffic and traveler information obtained through its own resources and those of its public sector partners. These sources include live video cameras, police, traffic probes, and aircraft. Information is integrated in a real-time traveler information database. SmartRoutes uses the database to provide traveler information services directly to customers and sells database access rights to other traveler information delivery systems such as radio, pagers, cable TV, and internet service providers.

The company enters into partnership arrangements with government agencies to receive information feeds from their ITS equipment and notifications from police and other public sources of information. SmartRoutes provides additional data collection and communication infrastructure to augment the information. The public partner pays SmartRoutes a monthly fee for three to five years for services it provides to the public free of charge, including a telephone information service. The company may also provide services directly to government agencies, such as the operation of variable message signs on public roadways or incident management programs. The goal is for SmartRoutes operations within a region to eventually become self-sustaining from fees charged for specialized services and revenue from the sale of information to other companies.

SmartRoutes currently does not collect any individually identifiable information, nor does it retain any data or images. Consequently, information privacy has not been a topic of concern, and the company does not have an information privacy policy. However, the company is planning to start archiving aggregate travel time information on a continuous basis. It has received previous requests for this information from market research and real estate organizations and believes that the information would also be valuable for government planning agencies. The company hopes to use cell phone geolocation as a primary means of obtaining these data. This application would still not require the company to collect individually identifiable information.

SmartRoutes is a national leader in the design, development, and deployment of ITS relating to advanced traveler information services. It is experienced in fusing data from multiple sources and in developing partnerships with public and private organization to obtain and provide data and services. The company is willing to move into new markets as it sees a need arising. SmartRoutes representatives have attended the ADUS activities, and see a market potential for some forms of archived data. Currently, the company is planning to archive only aggregate travel time information, but, should it see the market arising, the company would be poised to collect and distribute other archived data.[129]

CONCLUSIONS

There are currently significant data gaps that may be reduced through the application of ITS technologies. In addition, data collection through ITS may augment or replace more cumbersome means of data collection, such as travel surveys. Data gaps occur particularly in the areas of transportation planning and research, freight logistics, traveler information services, and commercial marketing and real estate. Although organizations in these areas may apply ITS technologies to collect data for their own purposes, there is also significant value for these applications in data that are collected for other purposes. If data collectors completely deny data access to all external organizations, they may prevent usage of data for some legitimate and beneficial purposes. However, the privacy of individuals who are the subjects of information collection must be protected. Hence the need for information sharing forums arises.

Infomediaries are most relevant when a third party is necessary to

- integrate data from multiple sources, or
- transform data to make them more useable or to protect the privacy of individual data units.

Organizations that collect data for their own purposes may not have the resources to perform data transformations for alternative purposes. However, untransformed data may not be valuable to other organizations or it may reveal proprietary information about data subjects. In these cases, a third party can screen and transform data. Data

confidentiality agreements may be necessary between the data providing organization and the third party infomediary. There are also cases in which data from multiple sources can be significantly more valuable than data from an individual source. Traffic information provides a good example. Traffic information from one source, for instance, one jurisdiction's traffic cameras and roadway sensors, provides significantly less value than traffic information about an entire metropolitan area derived from multiple sources. Infomediaries provide a valuable role in integrating data from multiple sources.

Infomediaries are most likely to develop in a stepwise fashion, collecting information relevant to a specific need. Consequently, multiple infomediaries are likely to arise to meet different needs. Over time, an infomediary may collect new forms of information to fulfill additional needs or augment existing data. These concepts are evident in the cases examined. Reebie specializes in the provision of freight commodity flow data, SmartRoutes in traveler information, and TTI in traffic flow data for research purposes. TTI's infomediary activities were instigated to provide information for its own research purposes. SmartRoutes and Reebie recognized external markets for specific data products. Both companies are now augmenting their data collection efforts and moving into new markets.

Whether information is exchanged directly from data collectors to other users or through infomediaries, data collection and archiving practices are based on known or anticipated needs. Traditionally, transportation data collection for operations has been separate from that for planning or other purposes. ITS provides the opportunity for consolidating some of these data collection efforts. However, current institutional arrangements do not necessarily support such consolidation. ADUS activities recognize the need for additional communication among potential data collectors and users. The TTI report *ITS Data Archiving: Case Study Analysis of San Antonio TransGuide Data* recommends the formation of communication feed-loops to discuss stakeholder data needs and data collectors' ability to provide data elements.[130]

Thus, infomediaries have an important role in the distribution of certain types of transportation data. Other data may be exchanged directly between information collectors and users. Better communication among data collectors and potential users will improve the flow of valuable information. Sources such as the ADUS materials and

the data needs identified through this research may also aid information collectors in determining their data collecting and archiving practices.

Notes

[110] U.S. Department of Transportation, ITS Joint Program Office, *ITS Data Archiving: Case Study Analysis of San Antonio TransGuide Data*, prepared by Texas Transportation Institute (Washington, D.C., August 1999), p. 41.
[111] Federal Highway Administration, Office of Highway Information Management, *ITS as a Data Resource, Preliminary Requirements for a User Service*, by Richard Margiotta (Washington, D.C., April 1998), pp. 4-5.
[112] U.S. Department of Transportation, ITS Joint Program Office, *ITS Data Archiving: Case Study Analysis of San Antonio TransGuide Data*, p. 41.
[113] ITS America, "ITS Data for Freight Planning," by John Kaliski, Cambridge Systematics (Cambridge, Massachusetts, January 9, 1998).
[114] Ibid., p.7-8.
[115] Ibid., p. 13.
[116] "FCC Briefing Paper on the Use of Wireless Phones as Data Probes in Traffic Management, Travel Information and Other ITS Applications," provided by Mark Johnson, Director of Legislative Affairs, ITS America (Washington, D.C., October 12, 1999).
[117] Ibid.
[118] Briggs, Valerie, "New Regional Transportation Organizations," *ITS Quarterly*, Fall 1999, pp. 35-46.
[119] U.S. Census Bureau, Statistical Research Division, "Data Licensing Agreements at U.S. Government Agencies and Research Organizations" (draft), by Paul B. Massell and Laua Zayatz (Washington, D.C., January 13, 2000).
[120] Ibid.
[121] Ibid.
[122] Telephone interview by Valerie Briggs with Paul Ciannavei, Principal, Reebie Associates, Stamford, Connecticut, January 21, 2000.
[123] "DataLink," Texas Transportation Institute web site (accessed January 25, 2000), available from: http://vixen.cs.tamu.edu/users-cgi/tlinkora/sample.cgi.
[124] Ibid.
[125] Reebie Assoicates, *U.S. Freight Market: Commercial Data and Analysis*, Stamford, Connecticut (brochure.)
[126] Telephone interview by Valerie Briggs with Paul Ciannavei, Principal , Reebie Associates, Stamford, Connecticut, January 21, 2000.
[127] Ibid.
[128] "About the Company," SmartRoute Systems web site, accessed January 20, 2000, available from http://www/smartroute.com/about.htm.
[129] Telephone interview by Valerie Briggs with Bill Twomey, SmartRoute Systems, Boston, Massachusetts, January 25, 2000.
[130] U.S. Department of Transportation, ITS Joint Program Office, *ITS Data Archiving: Case Study Analysis of San Antonio TransGuide Data*, p. 59.

Chapter 6. Results and Conclusions

This research involved a study of literature about privacy, interviews with experts in the ITS industry about data access issues and uses of sensitive information collected through ITS, a detailed examination of the data practices of two organizations that collect sensitive information through ITS, and development of models for data sharing. Findings are presented throughout the body chapters of the report and are summarized below. This chapter also presents recommendations for organizations that collect sensitive data, a discussion of roles for the public and private sectors in activities that require the collection of sensitive information, and opportunities for public-private partnerships.

SUMMARY OF RESEARCH FINDINGS

This section presents the primary research findings.

Basis for Privacy Concerns in ITS

Consideration of privacy issues in the collection of data through ITS is important for several reasons.

- Individuals and businesses want to maintain control over who has access to information about them or their activities and how it is used.
- Some confidential business information constitutes trade secrets which, if revealed, could provide competitive advantage to other businesses.
- Many ITS technologies have the ability to collect personal or confidential information about individual travelers or freight movements.
- Certain ITS services require the maintenance of records about an individual user.

Privacy Issues Relevant to ITS

ITS implementers need to understand and address the privacy concerns of their constituents in order to for ITS to be publicly accepted. A review of literature and interviews with ITS stakeholders helped to identify the following issues and concerns of ITS users and privacy advocates.

- Any ITS application that enables the identification or singling out of a specific vehicle or occupant raises potential privacy concerns.
- Information collected about individual units (travelers or freight shipments) may be made anonymous at various stages in the process of collecting and storing information. Privacy advocates recommend anonymization of data at the earliest possible point.
- Anonymous, but non-aggregate data, may still allow the identification of individual units through data characteristics. Data should be appropriately screened before release to prevent the disclosure of individually identifiable information.
- Visual images of vehicle occupants elicit greater privacy concerns than vehicle identification technologies due to the ability to detect an individual's movement and traveling companions.
- Privacy advocates are concerned that recorded data may be used for secondary purposes that may burden them with marketing, restrict their freedoms, hold them to higher standards of law enforcement, or allow other forms of discrimination.
- The secondary uses of ITS data for enforcement of traffic violations, commercial driver hour-of-service logs and commercial vehicle weight distance taxation are special concerns among certain user groups.
- Privacy advocates are concerned with the linking of records held by multiple organizations that is facilitated by computer networking and electronic data manipulation capabilities.
- Any data record may be accessed through court ordered subpoena to the potential aid or detriment of the ITS user.
- Additional uses of recorded information tend to develop over time if not controlled.
- Applications that are voluntary often become obligatory with widespread usage.
- Services that collect or distribute information about individuals can be organized to allow individuals to opt-in (i.e., give prior consent for participation) or opt-out (i.e., request not to be included). Although privacy groups advocate opt-in conditions, most business laws in the U.S. require only opt-out conditions.

- The security of data against unauthorized access is an important privacy concern.
- Various individuals and businesses differ in their level of concern about privacy issues and their willingness to reveal information in order to receive benefits derived through ITS.

ITS Applications with Privacy Implications

Two standards determine whether an ITS application or technology may elicit privacy concerns:

4. It enables the identification of an individual vehicle or occupant; or
5. It collects and stores proprietary information about a vehicle or individual.

ITS applications and technologies identified as having privacy implications include:

- Electronic clearance (EC) systems for commercial vehicles;
- Border crossing systems for commercial vehicles;
- Electronic toll collection (ETC) systems;
- Electronic enforcement (EE) applications;
- Vehicles probe applications;
- Video surveillance applications;
- “Mayday” emergency response systems;
- “Smartcard” applications;
- Vehicle location systems;
- On-board safety data system (black boxes or vehicle recorders);
- Incident or accident logs; and
- Paratransit and rideshare request logs.

Legal Privacy Protection Mechanisms

Few laws exist that could potentially protect the privacy of ITS users. The effects of those that do are summarized below.

- *The Fourth Amendment to the U.S. Constitution* – Fourth Amendment specifications of legal search and seizure procedures could affect electronic vehicle surveillance and tracking capabilities. Most court cases have ruled that occupants of vehicles traveling on public roads have little expectation of privacy and therefore the tracking and surveillance of vehicles on public streets is not considered a violation of the Fourth Amendment. Thus, the Fourth Amendment does little to limit the use of ITS.
- *The Electronic Communications Privacy Act (ECPA) of 1986 and the 1994 Communications Assistance for Law Enforcement Act (CALEA)* – The ECPA penalizes persons that intercept or disclose electronic communications without authorization, and CALEA sets standards by which law enforcement may access wire-line communications. However, the laws do not appear to apply to ITS vehicle tracking technologies.[131]
- *The Telecommunications Act of 1996* – This Act forbids telecommunications carriers' from using, disclosing, or providing access to proprietary information collected about customers for any purpose other than providing the service for which it was collected. However, a subsequent federal appeals case, *U.S. West, Inc. v. Federal Communications Commission*, ruled that carriers may use data they collect to market their own services to customers. The Act also specifies that carriers may disclose aggregate customer data on "reasonable and nondiscriminatory terms and conditions."[132] The Act applies to ITS services, such as cell phone geolocation, that may be provided through telecommunications companies. Although it does not apply to other ITS service providers, it could serve as a model to follow.
- *The Wireless Communications and Public Safety Act of 1999* – The Act establishes provisions to allow wireless phones to be located in cases of emergencies and prohibits the unauthorized disclosure or use of customer location information

except for purposes of emergency response. The ITS community hopes that it will open the door for aggregated cell phone user location information to be used for traffic monitoring purposes.

- *The Privacy Act of 1974 and the Freedom of Information Act* – The Privacy Act regulates the collection, retention, use, and disclosure of personal information held by federal government agencies. The federal Freedom of Information Act (FOIA) entitles the public to access any records held by federal agencies, but has an exemption that protects information that, if disclosed, would be likely to result in a "clearly unwarranted invasion of privacy." It is unclear whether information collected through ITS is included in this definition. All states have adopted legislation similar to FOIA. Therefore, these laws *may* provide some protection of personal information collected through ITS that is held by federal, state, or local government agencies.[133]
- *State Privacy Laws* – State privacy laws vary in their degree of privacy protection and are more fragmented than federal laws. Laws similar to the federal FOIA have been adopted in all states and to the federal Privacy Act in about half of the states, but their interpretations in state courts may vary.

Institutional Privacy Protection Mechanisms

Institutional measures play an important role in the protection of user privacy.

- Voluntary measures and market solutions largely dictate privacy protection within the American business community.
- Many industries have developed voluntary codes of fair information and privacy principles based on the following five tenets: openness, individual access and correction, collection limitation, usage control, data security. These codes are not legally enforceable.
- ITS America has drafted Fair Information and Privacy Principles for ITS and for ITS/CVO to serve as a policy guide to ITS operators.
- Contracts between ITS users and operators can serve as a means to make elements of a privacy policy legally binding.

Collection of Sensitive Information

A study of electronic clearance and electronic toll collection systems' organizational practices revealed important findings about how public and private ITS organizations treat sensitive data. A summary of the findings are included in the conclusions to chapter 4. From these findings, general inferences can be drawn that are relevant to other forms of sensitive ITS data collection.

- Public perception has a greater influence on the development of policies relating to privacy in ITS organizations than laws or formal guidelines.
- Media attention can significantly influence public perception of an ITS activity.
- Many organizations find it preferable to "maintain a low profile" about secondary uses of anonymous data.
- It may be necessary for ITS/CVO organizations to disclose all anonymous and non-anonymous data uses to comply with ITS America's Fair Information and Privacy Principles for ITS/CVO.
- Voluntary participation and options for anonymity are important for gaining user acceptance and provide a market incentive for ITS operators to address privacy issues.
- Most organizations surveyed apply opt-in approaches to secondary data uses although they are not required by law or contract to do so.
- Institutional separations between multiple functions for ITS technologies or data provide more visible privacy protection than internal policies and are consequently more publicly acceptable.
- ITS system operators believe that protection of data confidentiality is essential to their organizations' success.
- Staff time and cost required to assemble and screen data are barriers to release of information for external uses.
- Information collected may be accessed by subpoena regardless of whether the collector is a public or private entity.

- Public agencies can protect proprietary information collected through ITS from release under FOIA requests, but may need to obtain special exemptions through state legislatures or attorneys general offices.

Public and Private Treatment of Data

The analysis of EC and ETC organizations and study of literature led to the following inferences concerning the collection of data by public and private organizations.

- Public agencies must comply with government information laws and Constitutional requirements. These provide some protections for data but may also make data open to public disclosure under FOIA requirements if not exempted.
- Private organizations are subject to few legal requirements in the treatment of ITS data. Control of data through private organizations depends entirely on individual agencies' policies.
- Public organizations may be subject to regulations dictating data archiving procedures and tend to archive data for longer periods of time than private organizations.
- Publicly held data are more likely to be used for law enforcement purposes than privately held data. However, in cases studied, public opposition prevents use of data for traffic violation enforcement.
- The private sector has greater incentive to sell or use personal data for external marketing purposes. However, customer contracts can prevent these uses.
- Few restrictions exist on the sharing of data among public agencies. Most public agencies are willing to cooperate with other public agencies in the provision of data for research and planning purposes as long as data confidentiality can be maintained.
- The private sector is more likely to require payment for release of data to outside organizations.

Uses of Sensitive ITS Data

ITS generated data is starting to be recognized as a valuable resource to replace or augment traditional labor-intensive data collection methods. Additional applications, services and markets for ITS information are expected to evolve as the implementation of basic ITS infrastructure expands. Activities surrounding the development of the Archived Data User Service within the National ITS Architecture helped to define some of the potential uses of archived data. This research included surveys with ITS data collectors and users with the purpose of determining potential uses of sensitive information collected through ITS. Table 11 summarizes the findings. It specifies activities that may benefit from the use of sensitive ITS data, lists data requirements for those activities, and indicates ITS data sources and data forms that might be useful to fulfill those requirements.

Table 11. Secondary Uses of Sensitive ITS Data

Activity	**Data Requirements**	**ITS Data Source**	**Data Type***
Public Sector Freight Planning	Commodity flows – O/D patterns, modes, routes, transfer points, shipment value, time sensitivity; cost to industry of accidents; cost to industry of congestion; facility usage; access problems	Traffic surveillance technologies	An
		Automatic vehicle classification	An
		Vehicle probe applications	An
		Automatic vehicle identification	I, Ag
		Cargo identification	I, Ag
		Smart cards	I, Ag
		Vehicle tracking technologies	I, An
		Incident logs	I, An
		Electronic clearance records	I
		Border crossing records	I
Private Sector Freight Planning	Shipments, commodity flows, travel times, congestion, facility accessibility, accident rates	Traffic surveillance technologies	An
		Automatic vehicle classification	An
		Vehicle probe applications	An
		Automatic vehicle identification	I, Ag
		Cargo identification	I, Ag
		Smart cards	I, Ag
		Vehicle tracking technologies	I, An
		Incident logs	I, An
		Electronic clearance records	I, Ag
		Border crossing records	I, Ag

Activity	Data Requirements	ITS Data Source	Data Type*
Transportation Demand Modeling	Trip making characteristics of individual travelers; O/D patterns; traveler behavior and response; traffic characteristics – speed, volume, density; facility usage	Traffic surveillance technologies	An
		Vehicle probe applications	An
		Automatic vehicle identification	I, Ag
		Automatic vehicle occupancy counts	An
		Smart cards	I, Ag
		Vehicle tracking technologies	I, An
		Incident logs	I, An
		Rideshare request records	An
Accident Investigation	Information to determine cause of accident, witness identification, analysis of response	Surveillance video images	I
		Incident logs	I
		Automatic vehicle identification	I
Safety Analysis	Cause of incidents, effects of incidents, response characteristics, driver and vehicle behavior characteristics	Surveillance video images	An
		Incident logs	An
		Traffic surveillance technologies	An
		On-board safety data systems	An
Traveler Information Products	Travel times and speeds, congestion and incident information, customer identification and location	Traffic surveillance technologies	An
		Vehicle probe applications	An
		Automatic vehicle location	I
Product Marketing	Consumer travel behavior – travel distances; Characteristics of travelers for targeted marketing	Traffic surveillance technologies	An
		Automatic vehicle classification	An
		Vehicle tracking technologies	I, An
		Electronic Toll Collection Records	I
Commercial Real Estate Development	Consumer travel behavior – travel distances, O/D patterns; traffic characteristics – volume, travel times, congestion; characteristics of travelers	Traffic surveillance technologies	An
		Automatic vehicle classification	An
		Vehicle tracking technologies	I, An
		Vehicle probe applications	An

*Data Type refers to whether anonymous (An), aggregate (Ag), or individually identifiable (I) data is desired from the given data source for the specified activity.

Forums for Archiving and Distributing Sensitive Information

Many of the activities listed in Table 11 have the potential to provide significant public benefit. ITS data in aggregate or anonymous forms can often be provided for these activities without compromising user privacy. Other types of data require special protections and should only be shared under tightly controlled conditions. Management techniques and certain institutional forums may be able to mitigate the risks involved

with distributing some types of sensitive data. Potential institutional models and techniques for sharing data are described in chapter 5 and summarized below.

Licensing Agreements

License agreements are formal contracts that allow external organizations to access sensitive data for predetermined purposes and under controlled conditions. Contracts are customized to individual data applications and specify how data will be used, who will have access to the data, data security and enforcement mechanisms, restrictions on data use and release of research results, procedures for return of data, and applicable fees. Data licensing creates a burden of oversight and contract enforcement on the data providing agency that must be planned for and may require compensation from the data receiving organization.

Decentralized Approach

In the decentralized approach the data collecting agency provides data directly to external users. The collecting agency follows a policy that outlines a set of conditions under which data may be shared externally. Licensing agreements are used to bind data receiving agencies to these conditions.

Advantages

- Collecting organizations maintain direct control of their information;
- Easy to implement;
- Lowest cost alternative.

Disadvantages

- Substantial burden and cost to the data collecting agency for
    - developing structure for sharing information,
    - negotiating and enforcing individual license agreements,
    - screening and transforming data;
- Risk of data being divulged by licensee;
- Little incentive for collecting organization to provide outside access to data;
- May require data receiving organizations to seek data from multiple sources.

Public Infomediary

With the public infomediary concept, a public agency or its contractor collects and merges data from multiple sources, screens data, and makes the data available to outside users based on predetermined standards.

Advantages

- Provides a single point of reference for data;
- Allows data management, screening, and distribution by experts.

Disadvantages

- Requires public funding;
- Depends on voluntary cooperation of data collecting organization;
- Cooperation from private data collectors unlikely.

Private Infomediary

A private infomediary collects and integrates data from multiple sources and sells the data to outside organizations in useful forms.

Advantages

- Demand driven;
- Creation of customized products for specific user groups possible;
- Best ability to obtain data from private sources;
- Creates opportunities for public-private partnerships.

Disadvantages

- Cost to users of data;
- Depends on voluntary cooperation of data collecting organization;
- Formation of monopolies probable.

Conclusions about Data Sharing Forums

- Infomediaries are most relevant when a third party is necessary to
    6. integrate data from multiple sources, or
    7. transform data into more useable forms or to protect the privacy of individual data units.
- Infomediaries are most likely to develop in a stepwise fashion, collecting information relevant to a specific need and moving into new data markets over time.

- Multiple infomediaries are likely to arise to meet different data needs.
- Better communication is needed among data collectors, users, and third party infomediaries to improve information flows.

RECOMMENDATIONS FOR DATA COLLECTING ORGANIZATIONS

The agencies that collect data have ultimate control over how those data are protected and how they are used. These agencies' actions and policies have important ramifications for the subjects of the data collection and potential users of the collected data. Data collecting agencies should understand the desires of both groups as well as any laws that regulate the treatment of data. These factors must be carefully considered in agencies' actions and policies. Based on the research findings, several recommendations are made for data collecting organizations.

Build privacy protection into the organizational structure. Privacy issues should be considered from the early stages of development of an ITS program. Basic institutional decisions about whether an ITS activity should be performed by a public or a private organization affect privacy considerations, as discussed below. Appropriate actions should be taken to protect data whether they are held by a public or private agency. Technical elements should be designed with adequate information security features. Decisions about data access, use, and disclosure should be determined early. It may be difficult to implement more stringent privacy regulations later in a program's life if groups become accustomed to having access to certain types of data.

Disclose all collection and uses of individual data. Visibility of data flows is a fundamental element of privacy protection. ITS America's Privacy Principles advise that individuals should know what information is collected about them, how it is collected, what its uses are, and how it will be distributed. Most ITS data collection activities should follow opt-in conditions in which the subject chooses to participate in the activity. Where this is not feasible, individuals should be able to opt-out or request that information not be collected or used in the manner specified.

Provide user choices. Various individuals and businesses differ in their levels of concern about privacy and what information they consider proprietary. Provision of multiple options for provision of proprietary information allows individuals or businesses

to disclose only the information that they feel comfortable revealing. An anonymous participation option should be provided if the application permits. Participation in an activity that collects individual information should be voluntary unless dictated by law. Agencies that collect individual information should ensure that the subjects know about the data collection activity and have the opportunity to opt-out. Following these guidelines can foster greater public support for a data collection activity.

Collect only relevant data. ITS America's Fair Information and Privacy Principles stipulate that collection of individually identifiable information be limited to only the information that is necessary for the specified ITS service function. Collection of additional information may be desired for secondary purposes. Provision of such information by ITS customers should be optional, and customers should understand how the data will be used. An ITS organization should consider carefully the prudence of collecting such information, taking into account the organization's missions and goals.

Collect and use the least-sensitive form of information necessary. The sensitivity of information depends on its form. Individually identifiable information is the most sensitive. Aggregate data are the least sensitive. The sensitivity of anonymous but non-aggregate data depends on the ability to identify individuals due to characteristics of the data. Agencies can minimize privacy risks by collecting and using the least sensitive form of information necessary. Information that must be collected in individual units but is used in aggregate form should be aggregated early in the data collection process. Data should be collected anonymously whenever the application permits.

Provide incentives for individuals and businesses to consent to the collection and use of their personal information. Some ITS applications require the collection of individual information in order to provide a user service. Users voluntarily provide information in order to receive the service. In other cases, organizations desire individual information that could be collected through ITS. Individuals and businesses are often willing to reveal proprietary information in exchange for certain benefits. Organizations desiring individual information may chose to offer beneficial services or other incentives in exchange for the right to collect and use individual data for specific purposes. The concepts of visibility and individual consent should be followed in such cases.

Establish policies for data archiving. Data archiving has important privacy implications for users and subjects of individual information. Privacy advocates desire the purging of individual information at the earliest point possible, i.e., at the end of the billing cycle for ETC and EC. On the other hand, researchers and other data users advocate the retention of such data for later use. Data collecting agencies must balance the desires of both groups in establishing policies about archiving data. Activities and documents associated with the Archived Data User Service within the National ITS Architecture provide some guidelines for archiving information. Individual data may be given alternative identifiers and transformed into anonymous or aggregate form before archiving.

Implement appropriate internal data security mechanisms. Private information maintained by ITS organizations should be protected through technical and non-technical information security mechanisms. Databases containing private information should be proprietary to the data collecting agency only and should not be accessible through computer networks. Access to private information should be limited through technical measures such as password access control to specified personnel on a need-to-know basis. These personnel should undergo criminal background checks to identify previous fraudulent activities and should receive training about appropriate data handling. Technical measures such as logging of changes to the database, data encryption, and checksums should be implemented to protect the integrity of electronic data. Organizations should establish procedures for identifying individuals before providing individual account information. These should rely on the provision of account numbers, PINs, or passwords as opposed to publicly available information such as addresses and phone numbers. Documents available through the ITS Joint Program Office provide additional recommendations about information security.[134]

Create a formal written data policy. The data policy should address data collection, access, protection, use, and disclosure. The policy should be made publicly available with the exception of details about information security.

Establish rules, conditions, and procedures for disclosure of information. Organizations should establish protocols for release of information. They should determine in advance what types of information they are willing to release and publish

rules and conditions for release of this information. In establishing these policies, the agency should consider the needs and desires of the potential data users discussed in chapter 5 as well as the possibility of providing data to infomediaries. However, customer contracts must be honored, and individually identifiable information should not be exchanged without the customers' permission. The U.S. Statistical Policy Office, which reviews and evaluates statistical disclosure limitation methods used by federal agencies, recommends creation of a checklist to determine whether information requests may be granted. All information requests and disclosures, besides those of customers accessing their own account information, should be addressed by one office or group of employees in order to ensure consistency and correct application of procedures and protocols.

Establish boundaries for sharing information with law enforcement. Allowing law enforcement access to ITS data may decrease public support for the ITS activity. ITS America's Privacy Principles specify that information identifying individuals should not be disclosed to law enforcement absent consent or appropriate legal processes. However, aggregate data may be provided to law enforcement. ITS organizations should include specifications for law enforcement access to data within their data policies.

Use contracts to create legal agreements. Contracts create legally binding agreements between multiple entities. Therefore, contracts can be used to control data uses and create legally enforceable expectations for privacy protection. Contracts between ITS organizations and customers should address privacy issues and data handling. License agreements for sharing information among organizations should specify allowable uses and conditions for data use as well as repercussions for misuse.

Ensure that aggregate and anonymous data is sufficiently screened before release. Most privacy laws and fair information principles allow the release of aggregate and sometimes anonymous data. However, when treating data as anonymous it is important to ensure that individuals cannot be identified from the information. Often, small aggregation levels or unique characteristics (such as tracking a traveler from his home) can allow identification of an individual unit. It is important that data be screened for such occurrences before public release. Otherwise, these data should be treated as

sensitive individual information. The U.S. Statistical Policy Office has published several documents explaining screening methods for statistical disclosure used by federal statistical agencies.[135]

Take appropriate actions to protect data from disclosure under FOIA. Government agencies are subject to either state or federal FOIA requirements for information disclosure. Although exemptions exist for disclosure of personal information, it is often unclear whether ITS information is included in the definition of personal information. Agencies should seek advice from their state attorney's general office to determine whether the individually identifiable information they hold is safe from release under FOIA. If not, agencies should seek legislative action to create a special exemption for these data, as was done in Florida. If this is not possible, agencies may consider partnership arrangements that would allow data to be held by the private sector. Such a scenario is most likely to be necessary for business information, which is afforded less protections than personal information under most FOIA laws.

PUBLIC AND PRIVATE ROLES

Chapter 4 determined that both public and private sector organizations are capable of protecting the privacy of individuals and businesses in the collection of sensitive information. It concluded that organizational goals and operating characteristics of an ITS service provider are better determinants of data treatment than whether the organization is public or private. However, public and private sector organizations do tend to have different weaknesses in terms of data privacy and may be better suited to some applications than others. In particular, the private sector is more likely to sell personal information or consent to marketing of its customers by outside organizations. In the public sector, information may be subject to disclosure under FOIA and information is more likely to be used for law enforcement purposes. These weaknesses can be controlled to a large extent through agency policies and protection clauses in customer contracts. They were not exhibited in all the organizations examined in chapters 4 and 5. Disclosure of information through FOIA is the most difficult of these weaknesses for agencies to control. Agencies can take actions to protect information from release through FOIA, as described above. The investigation of FOIA requirements in chapters 3

and 4 reveal that personal information about individuals can probably be protected from disclosure. However, it is less clear whether information about businesses, including freight and trucking information, is protected from public disclosure under FOIA unless it is classified as a trade secret.[136]

Chapter 2 reveals that individuals and businesses differ in their degrees of concern about privacy. A percentage of the population is not concerned with privacy and is willing to share personal information freely. Another segment of the population are privacy fundamentalists and want to limit any collection of their personal information. The majority of the population falls in between. They weigh the risks of information disclosure against the benefits derived. Therefore, among organizations that desire to collect personal information, the most successful will be those that the population being served perceives as having the lowest risk and highest reward for information disclosure. The perception of risk may be as important as actual risk.

Individuals and the freight industry are most likely to provide personal information to organizations that they trust. Relationships between the trucking industry and government have traditionally been mistrustful due to the government's role in regulating and taxing the industry.[137] The predecessors of HELP, Inc. and NORPASS had to work to overcome this mistrust and build cooperative relationships between the two sides. HELP, Inc. found it necessary to provide services through a neutral third party rather than seek to establish trucker confidence in government service providers. Reebie, a private company, has been successful in collecting proprietary shipment information from truckers. These examples point to the conclusion that the trucking industry may be more comfortable sharing information with private infomediaries than directly with the public sector. Public organizations may be just as capable at protecting customer privacy as private organizations. However, public organizations may have to overcome more perception problems when dealing with the freight industry than private organizations. This may make it more difficult for them to receive participation rates as high as those of private organizations. There is little evidence in this report that individuals are more comfortable sharing personal information with one sector than another.

There are many reasons why certain services develop either in the public or in the private sector, and many reasons why a transportation agency may chose to provide a

function in-house or privatize it. Both sectors are capable of protecting customer privacy in the collection of sensitive information if appropriate actions are taken. However, the public sector may be at a disadvantage in collecting sensitive information from the freight industry due to perceptions of potential conflicts of interest and a history of mistrust between the industries.

OPPORTUNITIES FOR PUBLIC-PRIVATE PARTNERSHIPS

The processes discussed in this paper present many opportunities for public-private partnerships. Data collected in one sector are often valuable to the other sector. Data exchanges may constitute beneficial partnerships. The agreement between the Kentucky Transportation Center and Reebie is an example of such a partnership. The Kentucky Transportation Center receives Reebie products at a discounted rate in exchange for access to information collected by the center that Reebie values. SmartRoute Systems is another variant of such a partnership. It receives raw data from public organizations in exchange for services that the public values. Partnerships may also be formed to circumvent problems associated with data collection through the public sector, including the possibility of release of data through FOIA. HELP, Inc. exemplifies such a partnership. Public-private partnerships may also form to provide greater incentives for customers to participate in ITS services or data collection activities. For example, some public toll agencies partner with private companies to do co-promotions. The private company provides customer discounts for toll services or other incentives to entice individuals to participate in ETC. The private organization receives recognition for this service, which is a form of advertising.

RESEARCH CONCLUSIONS

Several fundamental conclusions can be drawn from this research.

- ITS implementing organizations have the primary responsibility for protecting user privacy. U.S. and state laws do not adequately address privacy issues in ITS. However, protecting user privacy is a critical element in public acceptance of ITS. Therefore, implementing organizations must address privacy issues. ITS America has established ITS Privacy Principles to aid implementers in this effort. The experiences of established ITS organizations

that collect sensitive information, such as ETC and EC agencies, can also provide valuable insights.

- ITS implementers must balance privacy protections with the value of sharing or using data for multiple purposes. ITS are capable of providing valuable data for multiple purposes. Arrangements for sharing information among different organizations or for using data for multiple purposes within the same organization should include provision for privacy protection.
- Public perceptions and levels of trust are important determinants in the success of ITS data collectors and service providers. Perceptions of privacy protection can be as critical to public acceptance as actual practices.
- Both the public and private sector can provide adequate privacy protections for ITS services in most cases. However, each sector has different areas of strengths and weaknesses.
- There is an important role for data infomediaries in collecting, transforming, and providing data for multiple uses. Infomediaries can mitigate risks associated with dissemination of sensitive information, assemble data from multiple sources, and provide these data in usable forms. Public infomediaries are most applicable when data is to be assembled from public sources for use by public sources. Private infomediaries are best suited to collecting data from or providing it to multiple public and private sources. Findings suggest that the freight and commercial vehicle communities are more willing to provide information to private sector infomediaries.

Notes

[131] Holdener, Douglas J. "Electronic Toll Collection Information: Is personal Privacy Protected?" *Compendium: Graduate Student Papers on Advanced Surface Transportation Systems*, Southwest Region, University Transportation Center Research Report # SWUTC/96/72840-00003-1, Texas Transportation Institute, Texas A&M University System (College Station, Texas, August 1996).
[132] U.S. Congress, Enrolled Bill, *Telecommunications Act of 1996*, 104th Cong., 2nd sess., 1996, S. 652, Sec. 702, available from [http://thomas.loc.gov/].
[133] Belair et al., *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, p. 33.
[134] U.S. Department of Transportation, Federal Highway Administration, ITS Joint Program Office, *Protecting Our Transportation Systems: An Information Security Awareness Overview*, prepared by Mitretek Systems (Washington, D.C., 1997); U.S. Department of Transportation, Federal Highway Administration, ITS Joint Program Office, *Intelligent Transportation Systems (ITS) Information Security Analysis*, prepared by Mitretek Systems (Washington, D.C., 1997); U.S. Department of Transportation, Volpe National Transportation Systems Center, *Maryland ITS Security Requirements Recommendations and Maryland ITS Security Implementation Recommendations*, prepared by Computer Sciences Corporation (Cambridge, Massachusetts, 1997).
[135] U.S. Statistical Policy Office, Office of Management and Budget, Executive Office of the President, "Report on Statistical Disclosure Limitation Methodology," Statistical Policy Working Paper 22 (Washington, D.C., May 1994); U.S. Statistical Policy Office, Office of Management and Budget, Executive Office of the President, "Checklist on Disclosure Potential of Proposed Data Releases," Statistical Policy Working Paper 22 (Washington, D.C., July 1999).
[136] Gelman, Robert, "Privacy and Electronic Clearance Systems," *Transportation Quarterly*, vol. 51, no. 4 (Fall 1997), pp. 65, 67.
[137] U.S. Department of Transportation, Federal Highway Administration, Volpe National Transportation Systems Center, *IVHS Institutional Issues and Case Studies: HELP/Crescent Case Study*, prepared by Science Applications International Corporation (Cambridge, Massachusetts, April 1994), pp. 11-18.

Appendix A
Electronic Toll Collection Survey

Name of Service:

Responsible Organization:

Type of organization (public, private for-profit, or private non-profit):

Respondent's name:

Respondent's title:

Data Collection and Storage:

1. What type of transponder does your system use?
2. What capabilities does this transponder have (i.e. read only, read-write, smart)?
3. How many user accounts are currently active?
4. How many transponders are currently active?
5. Please verify that the following information is requested on your application in order to enroll in your service (this data will be referred to as "enrollment data"):

Personal Information		**Vehicle Information**	
Name		License Plate No./State	
Home Address		Make	
Business Address		Model	
Home (or evening) phone		Color	
Work (or day) phone		Year	
Fax number		No. of Axles	
E-mail address		No. of Tires	
Cell phone number		Vehicle type	
Pager number			
Personal Information (Cont.)		**Financial Information**	
Social Security No.		Credit Card No.	
Driver's License No./state		Bank Account No.	
Signature			
		Security Information	
Other		Customer selected PIN	

Method of learning about program		Customer selected password	
Method of obtaining application		Mother's maiden name	
Commuting behavior			
Household Income			
Other: please specify			

6. How long is this enrollment data maintained?

7. Is any other information, such as credit records or driving records, collected about the customer?

    a. If yes, is this data integrated into a user record along with the enrollment data?

    b. If yes, how long is this information maintained?

Transaction records refer to records of toll transactions.

8. Please describe the content of transaction records stored for an individual customer (i.e., record of individual transactions in chronological order indicating time of transaction, station name, and fee).

9. How long are transaction records maintained?

10. Are transaction records for a particular customer maintained within the same account as the enrollment data?

    a. If not, how are enrollment and transaction records linked?

11. Are customer records (enrollment, personal, or transaction) combined with any other collected data (i.e., from automatic vehicle identification reader stations)?

    a. If yes, please describe.

    b. If yes, who maintains this data?

12. Is transaction data also stored in an aggregate form, stripped of personal identifiers (i.e., all electronic toll transactions at a particular collection station within a particular time)?

    a. If yes, please describe what information is stored.

    b. If yes, is aggregate data combined with any other data (i.e., from automatic vehicle identification reader stations)? If so, please describe.

    c. If yes, who maintains this data?

Information Security:

13. What technical measures are in place to ensure information security? These may include data encryption, access control through passwords, activity logs, checksums to detect alteration of data during transmission or storage, and others.

14. What non-technical measures are in place to ensure information security? These may include written policies, personnel background checks, personnel surveillance, training programs, and others.

15. Who has access to customer account information?

Information Integrity:

16. How accurate is the electronic collection system?

    a. What type of errors occur and how often?

    b. What must a customer do to correct an error?

Information Dissemination and Use:

17. Does your agency use transaction or customer data for any purposes other than ETC (i.e., for marketing, travel time estimations, or vehicle counts for planning purposes)?

    a. If yes, please describe.

18. What outside groups or individuals have requested customer data and for what purposes?

    b. Were these requests granted?

    a. If yes, how are these groups using this data?

19. Has customer information ever been subpoenaed?

ETC data may have value to:

- Law enforcement (for violation enforcement, accident investigations or criminal investigations)
- Insurance companies
- Cellular phone companies
- Government planning organizations
- Research organizations (i.e. universities, federal and state research organizations)

- Market researchers
- Fleet operators
- Others

20. What other groups (public or private) may be interested in ETC data and for what purposes?

21. What is your agency's policy on giving or selling information to these groups?

22. Does your agency view these groups as potential revenue sources?

23. Would your agency's policy change if potential revenue could be derived from these sources?

24. What would need to be done to information in order to supply it to these groups?

25. Is the ETC data your agency collects being used to its full potential? Why or why not?

26. For what other purposes may this data be used in the future (by your agency or outside groups)?

Policies and Practices:

27. Does your agency have a formal written policy on data collection, storage, dissemination, and use?

    a. If yes, is it publicly available? By what means?

28. Is the customer aware of all personal information that is collected and stored, who has access to this data, and how it is used? How?

29. How have federal legislation (i.e., the Freedom of Information Act, The Privacy Act of 1974, the Electronic Communications Privacy Act of 1986 and amendments in 1994, or language in ISTEA or TEA-21) affected the agency's data collection, storage, and dissemination practices?

30. How have state statues influenced these practices?

31. Are you familiar with ITS America's ITS Fair Information and Privacy Principles, and has your agency used them to establish policies or practices?

Appendix B
Electronic Clearance Survey

Name of Service:

Responsible Organization:

Type of organization (public, private for-profit, or private non-profit)?

Respondent's name:

Respondent's title:

Data Collection and Storage:

1. What type of transponder does your system use?

2. What capabilities does this transponder have (i.e. read only, read-write, smart)?

3. How many user accounts are currently active?

4. How many transponders are currently active?

5. Please verify that the following information is requested on your application in order to enroll in your service (this data will be referred to as "enrollment data"):

Company Information		**Interstate Information**	
Company name		ICC Number	
Billing address		U.S. DOT Number	
Shipping address			
Telephone number		**Vehicle Information**	
Fax number		Owner equipment number	
Contact names		Truck year and make	
Contacts' e-mail addresses		License plate number	
Contacts' telephone numbers		VIN	
Contacts' fax numbers		Registration Name	
Load type		IRP Account Number	
		Leased or owned truck	
		HAZMAT code	

6. Is any other information collected in the enrollment process?

7. For what purpose is each piece of enrollment data used?

8. Would the same data be collected in a manual process?

9. How long is this enrollment data maintained?

10. What other information is collected about the customer (i.e., safety records)?

    a. If yes, is this data integrated into a user record along with the enrollment data?

    b. If yes, how often is this information updated?

Transaction records refer to records of electronic bypasses.

11. Please describe the content of transaction records stored for an individual customer?

12. How long are transaction records maintained?

13. Are transaction records for a particular customer maintained within the same account as the enrollment data?

    a. If not, how are enrollment and transaction records linked?

14. Are customer records (enrollment or transaction) combined with any other collected data (i.e., from AVI reader stations not associated with inspection facilities)?

    a. If yes, please describe.

    b. If yes, who maintains this data?

15. Is transaction data also stored in an aggregate form, stripped of personal identifiers (i.e., all electronic clearance transactions at a particular station within a particular time)?

    a. If yes, please describe what information is stored.

    b. If yes, is aggregate data combined with any other data (i.e. from automatic vehicle identification reader stations)? If so, please describe.

    c. If yes, who maintains this data?

Information Security:

16. What technical measures are in place to ensure information security? These may include data encryption, access control through passwords, activity logs, checksums to detect alteration of data during transmission or storage, and others.

17. What non-technical measures are in place to ensure information security? These may include written policies, personnel background checks, personnel surveillance, training programs, and others.

18. Who has access to customer account information?

Information Integrity:

19. How accurate is the electronic clearance system?

20. What type of errors occur and how often?

21. What must a customer do to correct an error?

Information Dissemination and Use:

22. Who owns the data?

23. Does your agency use transaction or customer data for any purposes other than electronic clearance?

    a. If yes, please describe.

24. Have carriers requested data on their vehicles for purposes other than electronic clearance, such as to track the movement of their fleets?

    a. How do you deal with these requests?

25. What outside groups or individuals have requested customer data and for what purposes?

    a. Were these requests granted?

26. Has customer information ever been subpoenaed?

Electronic clearance data may have value to:

- Law enforcement (for violation enforcement, accident investigations or criminal investigations)
- Insurance companies
- Government planning organizations
- Research organizations (i.e. universities, federal and state research organizations)
- Market researchers
- Fleet operators
- Businesses serving the trucking industry

- Shippers (trucking companies' clients)
- Others

27. What other groups (public or private) may be interested in electronic clearance data and for what purposes?

28. What is your agency's policy on giving or selling information to these groups?

29. Does your agency view these groups as potential revenue sources?

30. Would your agency's policy change if potential revenue could be derived from these sources?

31. What would need to be done to information in order to supply it to these groups?

32. Is the data your agency collects being used to its full potential? Why or why not?

33. For what other purposes may this data be used in the future (by your agency or outside agencies)?

Policies and Practices:

34. Does your agency have a formal written policy on data collection, storage, dissemination, and use?

    a. If yes, is it publicly available? By what means?

35. Is the customer aware of all personal information that is collected and stored, who has access to this data, and how it is used?

36. How have federal legislation (i.e., the Freedom of Information Act, The Privacy Act of 1974, the Electronic Communications Privacy Act of 1986 and amendments in 1994, or language in ISTEA or TEA-21) affected the agency's data collection, storage, and dissemination practices?

37. How have state statues influenced these practices?

38. Are you familiar with ITS America's ITS Fair Information and Privacy Principles, and has your agency used them to establish policies or practices?

Appendix C
ITS Industry Experts Survey

1. Aggregate Data Market: Anonymous information, stripped of personal identifiers, usually does not concern privacy advocates. Electronic toll collection, electronic clearance, and vehicle probe data can be aggregated into anonymous forms. Do you foresee a secondary market for this aggregate data currently or in the future? What organizations, public and private are, or might be, interested in this data? For what purposes? Could this market provide revenue to the information collecting agency? What problems arise with the sale or distribution of this data? Is this an appropriate use of this data?

2. Non-Aggregate Data Market: There is speculation that a market exists for the personally identifiable and non-aggregate data. Do you believe that there is a market for this data and if so what organizations may be interested in it? For what purposes? Could this market provide revenue to the information collecting agency? What problems arise with the sale or distribution of this data? Is this an appropriate use of this data?

3. Law Enforcement: Is it appropriate for law enforcement officials to access individual ITS account records to aid in criminal investigations such as for repeated tollway violators, car thieves, or traffickers of illegal substances? Should law enforcement have access to these records for any other purposes? In order for law enforcement to have access to this information should there be some “due process” requirements such as a “probable cause” standard and a warrant issued by a judge.

4. Open Access: Should companies or individuals have access to individual account records for any purposes?

5. Adequacy of Protection Mechanisms: In general, do you think privacy protection mechanisms within the ITS community are adequate and appropriate? If not what actions need to be taken by whom to provide adequate user protection? What actions should data collecting agencies take to protect user privacy (i.e., should data be purged, archived without identifiers, archived only in aggregate form, etc.)

6. Public Versus Private: Do public and private organizations have differing abilities to protect user privacy? Why? Should collecting agencies have the same or differing policies for release of data to public organizations and private organizations?

Appendix D
Survey and Interview Participants

ITS Industry Expert Survey

Dave Barry, Director of ITS Programs and Research, National Private Truck Council, Alexandria, Virginia

Gene Bergoffen, Executive Vice President, NORPASS, Bethesda, Maryland

Russ Capelle, Manager of Freight Data Programs, Bureau of Transportation Statistics, U.S. Department of Transportation, Washington, D.C.

Richard Easley, President, e^2 Engineering, Reston, Virginia

Ralph Gillmann, Office of Highway Information, Federal Highway Administration, U.S. Department of Transportation, Washington, D.C.

Jack Goldstein, Sector Vice President and General Manager, Logistics and Transportation Systems Sector, Science Applications International Corporation (SAIC), McLean, Virginia

Mark Hallenbeck, Director, Washington State Transportation Center (TRAC), University of Washington, Seattle, Washington

Kevin Holland, Manager, Technology Policy, American Trucking Association, Alexandria, Virginia

Mark Johnson, Director of Legislative Affairs and Legal Counsel, ITS America, Washington, D.C.

John Kaliski, Senior Associate, Cambridge Systematics, Cambridge, Massachusetts

Steve Keppler, Director of Commercial Vehicle Programs, ITS America, Washington, D.C.

Catherine Lawson, Transportation Research Group Manager, Center for Urban Studies, Portland State University, Portland, Oregon

Rich Margiotta, Senior Associate, Cambridge Systematics, Cambridge, Massachusetts

Jane McIntire, Director of Continuing Education and Research, National Private Truck Council, Alexandria, Virginia

Rob Puentes, Director, Infrastructure Programs, ITS America, Washington, D.C.

Craig Roberts, Director, Policy and Partnerships, Intelligent Transportation Society of America (ITS America), Washington, D.C.

Hal Worral, Executive Director, Orlando-Orange County Toll Authority, Orlando, Florida

Electronic Toll Collection Survey

Mike Ashcraft, Division Director, Oklahoma Transportation Authority, Oklahoma City, Oklahoma

Frank Barbagallo, Manager of Toll Operations, Transportation Corridors Agency, Irvine, California

Erik Christiansen, EZPass Operations Manager, NY Thruway Authority, Albany, New York

Carl Compton, Accounting Systems Manager, Kansas Turnpike Authority, Topeka, Kansas

Paul Crawford, Systems Administrator, Orlando-Orange County Toll Authority, Orlando, Florida

Kevin Holbert, Systems Administrator, Harris County Toll Road Authority, Houston, Texas

Jay Gainer, Project Manager, San Diego Association of Governments, San Diego, California

Kim Kawada, Senior Regional Planner, San Diego Association of Governments, San Diego, California

Debbie Lee, Customer Service Supervisor, Oklahoma Transportation Authority, Oklahoma City, Oklahoma

Cybil McDermott, Operations Auditor, North Texas Tollway Authority, Dallas, Texas

Neil McDonald, Director of Operations, Illinois State Toll Highway Authority, Downers Grove, Illinois

Bruce Meisch, Information Services Director, Kansas Turnpike Authority, Topeka, Kansas

Randy Moore, Branch Manager of Toll Enforcement, Oklahoma Transportation Authority, Oklahoma City, Oklahoma

Steve Pustelnyk, Manager of Communications and Marketing, Orlando-Orange County Toll Authority, Orlando, Florida

Jerry Shelton, Director of Marketing, North Texas Tollway Authority, Dallas, Texas

Tammi Stanley, Marketing Specialist, California Private Transportation Company, Corona, California

Tracy Williamson, Manager of Video Enforcement, Harris County Toll Road Authority, Houston, Texas

David Wyn, E-Pass Service Center Manager, Orlando-Orange County Toll Authority, Orlando, Florida

Electronic Clearance Survey

Jeff Bibb, Assistant Director, Department of Vehicles, Kentucky Transportation Cabinet, Lexington, Kentucky

Rick Clasby, Administrator, Ports of Entry, Utah Department of Transportation, Salt Lake City, Utah

Douglas Deckert, System Architect for CVISN, Washington State Department of Transportation, Olympia, Washington

Tim Erickson, CVISN Program Manager, Washington State Department of Transportation, Olympia, Washington

David Fifer, ITS Specialist, Oregon Department of Transportation, Eugene Oregon

Alan Frew, Special Permit Manager, Motor Vehicle Division, Idaho Department of Transportation, Boise, Idaho

Jim Gentner, Vice President, HELP, Inc., Phoenix, Arizonia

John O'Connor, Service Center Director for Lynx/NORPASS, TransCore

Beth Rider, Director Business Operations, Lockheed Martin Information Management Systems

Marcell Tart, Captain, Florida State Patrol, Tallahassee, Florida

Randal Thomas, ITS Program Manager, Motor Carrier Transportation Division, Oregon Department of Transportation, Eugene, Oregon

Interviews

Bob Andrews, Community Relations Officer, Texas Department of Transportation, Austin, Texas

Paul Ciannavei, Principal, Reebie Associates, Stamford, Connecticut

Kathryn Condello, Vice President of Industry Operations, Cellular Telecom Industry Association, Washington, D.C.

Joe Crabtree, Director, Kentucky Transportation Center, University of Kentucky, Lexington, Kentucky

Michael Dennis, Director, Telematics, ITS America, Washington, D.C.

Chris Green, Technical Support Engineer, Etak, Inc., Menlo Park, California

Bill Ische, Electronic Toll Collection Regional Manager, Amtech, Dallas, Texas

David Lehrman, Attorney, Federal Motor Carrier Safety Administration, Washington, D.C.

Bill Twomey, Vice President of Public Sector Business, SmartRoute Systems, Inc., Boston, Massachusetts

Tricia Sulpizio, Media Relations Specialist, Qualcomm, San Diego, California

Mike Vickich, Systems Analyst, Texas Transportation Institute, College Station Texas

Laura Zayatz, Leader, Disclosure and Limitations Group, Bureau of the Census, Washington, D.C.

All surveys and interviews were conducted between November 1999 and January 2000 by Valerie Briggs.

Appendix E
Telecommunications Act of 1996 (S.652)
Title VII, Sec. 702. Privacy of Customer Information

Title II is amended by inserting after section 221 (47 U.S.C. 221) the following new section:

SEC. 222. PRIVACY OF CUSTOMER INFORMATION.

(a) IN GENERAL- Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) CONFIDENTIALITY OF CARRIER INFORMATION- A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION-

(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS- Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) DISCLOSURE ON REQUEST BY CUSTOMERS- A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) AGGREGATE CUSTOMER INFORMATION- A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of

a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) EXCEPTIONS- Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents--

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; or

(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information provide such service.

(e) SUBSCRIBER LIST INFORMATION- Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) DEFINITIONS- As used in this section:

(1) CUSTOMER PROPRIETARY NETWORK INFORMATION- The term `customer proprietary network information' means--

(A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

(2) AGGREGATE INFORMATION- The term `aggregate customer information' means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) SUBSCRIBER LIST INFORMATION- The term `subscriber list information' means any information--

(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

Source: U.S. Congress, Senate, *Telecommunications Act of 1996*, 104th Congress, 2nd Sess., 1996, S.652. SEC. 702.

Appendix F
Wireless Communications and Public Safety Act of 1999 (S.800)
SEC. 5. Authority to Provide Customer Information.

Section 222 of the Communications Act of 1934 (47 U.S.C. 222) is amended--

(1) in subsection (d)--

(A) by striking 'or' at the end of paragraph (2);

(B) by striking the period at the end of paragraph (3) and inserting a semicolon 'and'; and

(C) by adding at the end the following:

'(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d))--

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.'

(2) by redesignating subsection (f) as subsection (h) and by inserting the following after subsection (e):

'(f) AUTHORITY TO USE WIRELESS LOCATION INFORMATION- For purposes of subsection (c)(1), the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to--

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d)), other than in accordance with subsection (d)(4); or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) SUBSCRIBER LISTED AND UNLISTED INFORMATION FOR EMERGENCY SERVICES- Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide information described in subsection (i)(3)(A) (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.';

(3) by inserting 'location,' after 'destination,' in subsection (h)(1)(A) (as redesignated by paragraph (2)); and

(4) by adding at the end of subsection (h) (as redesignated), the following:

`(4) PUBLIC SAFETY ANSWERING POINT- The term `public safety answering point' means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) EMERGENCY SERVICES- The term `emergency services' means 9-1-1 emergency services and emergency notification services.

(6) EMERGENCY NOTIFICATION SERVICES- The term `emergency notification services' means services that notify the public of an emergency.

(7) EMERGENCY SUPPORT SERVICES- The term `emergency support services' means information or data base management services used in support of emergency services.'.

Source: U.S. Congress, Senate, *Wireless Communications and Public Safety Act of 1999*, 106th Cong., 1st Sess., 1999, S.800.

Appendix G
ITS America's Interim Intelligent Transportation Systems Fair Information and Privacy Principles

These fair information and privacy principles were prepared in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems (ITS). The principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

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

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

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

privacy must be respected. This requires disclosure and the opportunity for individuals to express choice.

2. **VISIBLE. Intelligent Transportation Information Systems will be built in a manner "visible" to individuals.**

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

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

4. **SECURE. Intelligent Transportation Systems will be secure.**

   ITS databases may contain information on where travelers go, the routes they use, and when they travel, and therefore must be secure. All ITS information systems will make use of data security technology and audit procedures appropriate to the sensitivity of the information. ITS systems should use technological and administrative safeguards to assure that access to personally identifiable information is available only to those that need to know it.

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

   ITS has the potential to make it possible for traffic management agencies to know where individuals travel, what routes they take, and travel duration. Therefore, ITS can increase the efficiency of traffic law enforcement by providing aggregate information necessary to target resources. States may legislate conditions under which ITS information will be made available. Absent government authority, however, ITS systems should not be used as a surveillance means for enforcing traffic laws. Although individuals are concerned about public safety, persons who

voluntarily participate in ITS programs or purchase ITS products have a reasonable expectation that they will not be "ambushed" by information they are providing.

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

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

7. ANONYMITY. Where practicable, individuals should have the ability to access Intelligent Transportation Systems on an anonymous basis.

Certain ITS applications (e.g., commercial vehicle operations or "mayday") require personally identifiable information to function. Others (e.g., automated fee payment) may be designed to enable use by individuals without identifying themselves (through anonymous debit accounts) or with identifiers for convenience (credit cards). Unless provision of identifiers is required by the ITS application, users should be provided with the opportunity to choose anonymity.

8. SECONDARY USE. Intelligent Transportation Systems information stripped of personal identifiers may be used for non-ITS applications.

American consumers want information used to create economic choice and value, but also want their interest in privacy preserved. ITS information is predictive of goods and services that interest consumers, for example, the right location for stores, hospitals and other facilities. However, personally identifiable information collected by ITS surveillance technologies is extremely sensitive. Therefore, the following practices should be followed:

- ITS information absent personal identifiers may be used for ITS and other purposes.

- Generally, data collectors should assure that ITS information provided to private organizations for secondary uses is stripped of personal identifiers.
- Individuals, however, may contract to allow use of personal identifiers for secondary use if full disclosure in the intended use is made and informed consent obtained.

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

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

Source: Intelligent Transportation Society of America, "Interim Intelligent Transportation Systems Fair Information and Privacy Principles," (Washington, D.C., August 30, 1999), available from: http://www.itsa.org.

Appendix H
ITS America's Fair Information Principles for ITS/CVO

These fair information principles were prepared in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems (ITS) for Commercial Vehicle Operations (CVO). They have been adopted by the ITS America CVO Technical Committee.

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

These principles are advisory, intended to educate and guide transportation professionals, policy-makers, and the public as they develop fair information and privacy guidelines for specific ITS/CVO projects. They are not intended to supersede existing statutes or regulations. Initiators of ITS/CVO projects are urged to publish the fair information principles that they intend to follow. Parties to ITS/CVO projects are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements.

FIP #1: Privacy

The reasonable expectation of privacy regarding access to and use of personal information should be assured. The parties must be reasonable in collecting data and protecting the confidentiality of that data.

FIP #2: Integrity

Information should be protected from improper alteration or improper destruction.

FIP #3: Quality

Information shall be accurate, up-to-date, and relevant for the purposes for which it is provided and used.

FIP #4: Minimization

Only the minimum amount of relevant information necessary for ITS applications shall be collected; data shall be retained for the minimum possible amount of time.

FIP #5: Accountability

Access to data shall be controlled and tracked; civil and criminal sanctions should be imposed for improper access, manipulation, or disclosure, as well as for knowledge of such actions by others.

FIP #6: Visibility

There shall be disclosure to the information providers of what data are being collected, how they are collected, who has access to the data, and how the data will be used.

FIP #7: Anonymity

Data shall not be collected with individual driver identifying information, to the extent possible.

FIP #8: Design

Security should be designed into systems from the beginning, at a system architecture level.

FIP #9: Technology

Data encryption and other security technologies shall be used to make data worthless to unauthorized users.

FIP #10: Use

Data collected through ITS applications should be used only for the purposes that were publicly disclosed.

FIP #11: Secondary Use

Data collected by the private sector for its own purposes through a voluntary investment in technology should not be used for enforcement purposes without the carrier's consent.

Source: Intelligent Transportation Society of America, "Fair Information and Privacy Principles for ITS/CVO," (Washington, D.C., April 22, 1999), available from: http://www.itsa.org.

Appendix I
North Texas Tollway Authority
Policies and Procedures

Subject: Privacy

Purpose: To establish policies concerning handling of private information of customers

Policy: It is the policy of the North Texas Tollway Authority that all employees of the Tolltag Store® protect the confidentiality of private information provided by customers to open and maintain Tolltag accounts.

Under no circumstances will this information be provided outside the Authority except in response to a subpoena.

Mailing lists of customers will not be provided to outside sources for any reason.

Personal information of customers will not be discussed among employees except in the course of business.

All employees will take precautions to secure documents or monitors exposing the private information of customers from the eyes of those without a need to know.

Source: "North Texas Tollway Authority Policies and Procedures," Toll Tag Office, Dallas, Texas, December 20, 1999.

Appendix J
New York State Thruway Authority
E-ZPass Account Information Policy

As the operator of an electronic toll collection system, known as E-ZPass, the Thruway Authority is the repository for data concerning the movement of electronic tags issued by the Authority or other tolling facilities to customers who choose to utilize the E-ZPass system. The universe of individuals and entities that have established E-ZPass accounts is quite diverse. Such diversity is similarly reflected in the varying methodologies that are utilized to request E-ZPass account information from the Authority.

All E-ZPass account holders, in whatever form they may be (individuals, corporate entities, public bodies, etc.), always have the ability to access their own Thruway account information and to request that such information be sent to a third party. This Policy sets forth the circumstances under which the Authority, absent a request from or the consent of the account holder, will release to third parties or on its own utilize the E-ZPass account information of its own customers or the customers of another tolling facility. The Authority is strongly committed to the concept of personal privacy, and the guiding principle behind this Policy is to protect the privacy of this information to the greatest extent possible.

When used in this Policy, the term "account information" means all information about an account holder and the vehicles utilizing that account, including but not limited to: the account holder's name, address, and any other identifying characteristics; the make, model, year and plate number of such vehicles; all photographs, microphotographs, videotapes and other recorded images of such vehicles created by E-ZPass equipment; and itemized statements of account deductions for the use of such system.

The Authority will not sell, distribute or make available in any way the names and addresses of its own customers or the customers of another tolling facility for fundraising purposes or commercial purposes not involving E-ZPass transactions.

From time to time, the Authority may make statistical information about the E-ZPass usage on the Thruway available to the public provided the information is presented in such a way that it cannot be used to identify an individual person or vehicle.

AUTHORITY USE OF E-ZPASS ACCOUNT INFORMATION

1. The Authority will utilize individual and aggregate account information concerning its own customers or the customers of another tolling facility solely for the following purposes:
   a. billing an account holder or deducting toll charges from the account holder's account;
   b. enforcement of toll collection and related regulations or violations of the account holder's customer agreement;
   c. in a judicial or administrative action or discovery proceeding to which the Authority is a party;
   d. the operation of commercial vehicle operation programs;
   e. for traffic and facility management purposes, provided such use does not identify an individual person or vehicle; and
   f. with respect to account information received from another tolling facility, as otherwise permitted by such other facility.
2. The Authority will require all contractors performing work involving access to E-ZPass account information to comply with the terms of this Policy.

Source: The New York State Thruway Authority, "E-Z Pass Account Information Policy," (Albany, New York, November 20, 1998).

Appendix K
HELP Inc.'s PrePass Enrollment Policy

Title: **PREPASS ENROLLMENT**

Policy: It is the policy of HELP, Inc. to permit motor carriers to enroll in PrePass if they meet the participation criteria of at least one participating state.

Purpose: To establish the procedures for enrolling motor carriers in PrePass.

Scope: This policy is applicable to all employees responsible for screening motor carrier application for PrePass.

Procedures:

1.0 Application

1.1 All motor carriers who desire to participate in PrePass, weigh station/port of entry bypass must complete and forward an enrollment application (for each fleet) to:

HELP PrePass Service Center
40 N. Central Avenue, Suite 2250
Phoenix, Arizona 85004

1.2 Accompanying each fleet application a carrier must provide a copy of:

1.2.1 Truck registration - IRP or intrastate

1.2.2 Fuel Tax registration - IFTA or State Fuel Tax Permit

1.2.3 Intrastate Operating Authority and /or Single State Registration System (SSRS) - if applicable

1.2.4 HAZMAT/HAZWASTE permit - if applicable

1.2.5 Agriculture permit - if applicable

1.3 Enrollment Data Retention - All application data submitted by a carrier shall be retained by the service center for as long as the carrier participates in PrePass. This data may be shared with participating PrePass states and by agreement with other electronic bypass systems.

2.0 Review

2.1 Service Center personnel will review the carrier's application and accompanying documents for completeness and will verify the current status of each document submitted. The documents will be verified with issuing state agencies:

2.1.1 Registration

2.1.1.1. IRP & Weight

Status- Must reflect current registration in at least one PrePass participating state.

Verification - Request issuing state verify account is not revoked or suspended.

2.1.1.2. Intrastate & Weight

Status - Must reflect current registration in a participating PrePass state.

Verification - Request issuing state verify registration is not revoked or suspended.

2.1.2 Fuel Tax

2.1.2.1 IFTA

Status - Must reflect current year license.

Verification - Request issuing state verify account is not revoked or suspended.

2.1.2.2 State Fuel Tax Permit (where applicable)

Status - Must reflect current year permit.

Verification - Request issuing state verify permit is not revoked or suspended.

2.1.3 Intrastate Operating Authority (If applicable)

Status - Must reflect current year authority.

Verification - Request issuing state verify authority is not revoked or suspended.

2.1.4 Single State Registration System (SSRS) (If applicable)

Status - Must reflect current registration year in at least one PrePass state where SSRS is required.

Verification - Request issuing state verify registration is not revoked or suspended.

2.1.5 Safety Rating

Status - Must meet a least one participating PrePass state's minimum safety criteria.

Verification
2.1.5.1 Interstate Carriers must have satisfactory safety rating as outlined in each PrePass state's participation criteria. Verification will be through the safety system used to establish the carrier's eligibility.

2.1.5.2 Intrastate Carriers must have satisfactory safety rating as defined by the PrePass state's participation criteria. Verification will be through the safety system used to establish the carrier's eligibility.

2.1.6 HAZMAT/HAZWASTE Permit (If applicable)

Status - (Where Applicable) Must have current year permit issued by appropriate authority.

Verification - Request issuing state agency verify permit is not revoked or suspended.

2.1.7 Agriculture Permit (If applicable)

Status - (Where Applicable) Must have current year permit issued by appropriate authority.

Verification - Request issuing state agency verify permit is not revoked or suspended.

3.0 Approval
Carriers that meet all enrollment criteria in at least one (1) participating PrePass state shall be approved for PrePass enrollment.

4.0 Transponder Activation

PrePass states may permit newly enrolled vehicles to operate in their state during the verification process so long as ALL credentials and safety documentation have been checked and copies are maintained by the PrePass service center.

Source: Heavy Vehicle Electronic License Plate, Incorporated (HELP, Inc.), "PrePass Enrollment Policy," (Phoenix, Arizona, May 15, 1998).

Appendix L
HELP Inc.'s PrePass Event Data Retention Policy

Title: **PrePass Event Data Retention**

Policy: It is the policy of HELP, Inc. to ensure that PrePass carriers are not subjected to a higher level of regulatory compliance than non-PrePass carriers. To that end, HELP, Inc. will retain carrier specific data for a defined period of time for the purpose of operating the PrePass System only. HELP Inc. intends not to provide carrier specific event data to jurisdictions without authorization of the individual carrier.

Purpose: To establish the procedures for collecting and retaining carrier event data.

Scope: This policy is applicable to everyone who will collect, retain or destroy PrePass data.

Procedures:

1.0 **Data Collection –** In the normal course of PrePass site operations, carrier data is collected and retained. This event data is retained for billing purposes and is used as the basis of: Site Activity, Pull-in Rates and Annual Bypass Activity/Vehicle Enrollment reports which are periodically provided to participating state agencies. (Copies of the summary reports used in California, are attached as examples.)

1.0 **Data Retention –** Carrier data collected during the course of PrePass site operations shall be retained for a period not to exceed 60 days beyond the end date of the period billing. This will allow for mailing times to and from the customer and accommodate most customer bill payment cycles. Billings will normally cover a calendar month period. Therefore, a carrier's January billing will reflect activity from 1 through 31 January. The data supporting an unprotested January billing will be retained until April 1st, which is a maximum of sixty (60) days beyond the billing end date of January 31. Data will be destroyed only after payment of an unprotested billing has been received by the Service Center or a protested billing has been resolved.

Source: HELP, Inc., "PrePass Event Data Retention Policy," (Phoenix, Arizona, May 15, 1998).

Appendix M
HELP Inc.'s Electronic Bypass Interoperability Agreement

RESOLUTION

WHEREAS: HELP, Inc. is a unique partnership of the private and public sectors formed to deploy Intelligent Transportation Systems.

WHEREAS: HELP, Inc. been a pioneer in developing electronic bypass services for states and the motor carrier industry.

WHEREAS: System interoperability and uniformity are important objectives that will allow states and motor carriers to obtain the maximum benefit from public and private sector investments in Intelligent Transportation Systems.

WHEREAS: HELP, Inc. fully supports the Western Association of State Highway and Transportation Official's recent resolution urging states "to develop interoperability between weigh stations/port of entry bypass systems."

THEREFORE BE IT RESOLVED THAT:

HELP, Inc. welcomes agreements with any state or system that might seek interoperability with the PrePass system. To facilitate interoperability, the HELP Board of Directors has identified six core principles that will guide our efforts to coordinate operations of the HELP PrePass system with other bypass systems.

1. Carrier participation must be voluntary.

2. Participation must be a privilege granted only to carriers meeting established enrollment criteria which includes proper credentials, current tax and insurance requirements and protection of safety, with participation being re-validated routinely.

3. Participating states must agree to protect data privacy and to fully disclose all specific uses of event data collected from carrier transponders.

4. Transponder identifiers will be shared outside the PrePass system only at the request of our carrier customers.

5. System interoperability agreements must contain provisions for fair and appropriate fees to support interoperability between PrePass and other states or systems.

6. HELP strongly supports the use of a single transponder for commercial applications, and transponders proposed for use with PrePass must be interoperable with the HELP system.

Source: HELP, Inc., "Electronic Bypass Interoperability Agreements," (Phoenix, Arizona, September 16, 1997).

Glossary

AAA – American Automobile Association

ADUS – Archived Data User Service

AVC – Automatic Vehicle Classification

AVI – Automatic Vehicle Identification

CALEA – Communications Assistance for Law Enforcement Act

CPNI – Customer Proprietary Network Information

CPTA – California Private Transportation Company

CVO – Commercial Vehicle Operations

DOT – Department of Transportation

E911 – Enhanced 911

EC – Electronic Clearance

ECPA – Electronic Communications Privacy Act

EE – Electronic Enforcement

ETC – Electronic Toll Collection

FCC – Federal Communications Commission

FOIA – Freedom of Information Act

ISTEA – Intermodal Surface Transportation Efficiency Act

ITS – Intelligent Transportation Systems

ITS/CVO – Intelligent Transportation Systems for Commercial Vehicle Operations

LCD – Liquid Crystal Display

MPO – Metropolitan Planning Organization

NYTA – New York Thruway Authority

PIN – Personal Identification Number

RC – Regional Consortium

RF – Radio Frequency

SanDAG – San Diego Association of Governments

TCA – Transportation Corridors Agency

TTI – Texas Transportation Institute

VES – Video Enforcement Systems

WIM – Weight-In-Motion

References

"About the Company," SmartRoute Systems web site (accessed January 20, 2000), available from: http://www/smartroute.com/about.htm.

Agre, Philip E., "Looking Down the Road: Transport Informatics and the New Landscape of Privacy Issues," *CPSR Newsletter*, vol. 13, no. 3 (1995), available from: http://dlis.gseis.ucla.edu/people/pagre/its-cpsr.htm.

Alpert, Sheri A, "Privacy and Intelligent Highways: Finding the Right of Way," *Santa Clara Computer and High Technology Law Journal*, vol. 11, no. 1 (1995).

An ETTM Primer for Transportation and Toll Officials, ATMS Committee and ETTM Task Force, Intelligent Transportation Society of America.

Arctic Express, Inc. vs. United States of America, 96-4095 (U.S. 6th Ct. App., 1997).

"Automatic Vehicle Classification," *ETTM On The Web* (updated April 25, 1997), available from: http://www.ettm.com.

Belair, Robert R., Alan F. Westin, and John J. Mullenholz, *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, contract no. DTFH61-93-C-00087 (Washington, D.C.: U.S. Department of Transportation, Dec. 1993).

Briggs, V., T. Delk and C.M. Walton, *Public-Private Partnerships for Providing ITS: Case Studies in Transportation and Other Industries*, Southwest Region, University Transportation Center Research Report # SWUTC/99/472840-00067-1, Center for Transportation Research, The University of Texas at Austin, January 1999.

Briggs, Valerie, "New Regional Transportation Organizations," *ITS Quarterly*, Fall 1999.

Clausing, Jeri, "Revised Banking Legislation Raises Concerns About Privacy," *The New York Times on the Web* (October 25, 1999), available from http://nytimes.com/search/daily.

"Data Dogfights," *The Economist* (January 9, 1999).

"DataLink," Texas Transportation Institute web site (accessed January 25, 2000), available from: http://vixen.cs.tamu.edu/users-cgi/tlinkora/sample.cgi.

Electronic mail correspondence from Douglas Deckert, Systems Architect for CVISN, Washington State Patrol, to Valerie Briggs, December 14, 1999.

Electronic mail correspondence from Gene Bergoffen, Executive Vice President, NORPASS to Valerie Briggs, January 24, 2000.

ETTM On the Web (accessed December 14, 1999), available from: http://www.ettm.com.

"FCC Briefing Paper on the Use of Wireless Phones as Data Probes in Traffic Management, Travel Information and Other ITS Applications," provided by Mark Johnson, Director of Legislative Affairs, ITS America, Washington, D.C., October 12, 1999.

Federal Highway Administration, Office of Highway Information Management, *ITS as a Data Resource, Preliminary Requirements for a User Service*, by Richard Margiotta (Washington, D.C., April 1998).

Glassco, R., et al., *Studies of Potential Intelligent Transportation Systems Benefits Using Traffic Simulation Modeling: Volume 2*, Mitretek Systems, MTR 1997-31 (June 1997).

Gelman, Robert, "Privacy and Electronic Clearance Systems," *Transportation Quarterly*, vol. 51, no. 4 (Fall 1997).

Glancy, "Privacy and Intelligent Transportation Technology," *Santa Clara Computer and High Technology Law Journal*, vol.. 11, no. 1 (March 1995).

"Heavy Vehicle Electronic License Plate, Incorporated," PrePass® web site (accessed December 1999), available from: http://www.prepass.com/help.htm.

Heavy Vehicle Electronic License Plate, Incorporated (HELP, Inc.), "Strategic Business Plan" (draft), (Phoenix, Arizona, July 6 1998).

HELP, Inc., *The Crescent Project: An Evaluation of an Element of the HELP Program*, prepared by The Crescent Evaluation Team (Phoenix, Arizona, February 1994).

Holdener, Douglas J. "Electronic Toll Collection Information: Is personal Privacy Protected?" *Compendium: Graduate Student Papers on Advanced Surface Transportation Systems*, Southwest Region, University Transportation Center Research Report # SWUTC/96/72840-00003-1, Texas Transportation Institute, Texas A&M University System, August 1996.

Holland, Kevin, "Black Boxes, Satellites & Safety: Q&A," *Truckline*, American Trucking Association web site, September 17, 1999, available from http://www.truckline.com/infocenter/topics/tech/black_boxes_faq.thml.

Intelligent Transportation Society of America, "ITS Data for Freight Planning," by John Kaliski, Cambridge Systematics (Cambridge, Massachusetts, January 9, 1998).

McPhee, Mike, "Court: Firms Can Target Phone Users," *The Denver Post Online* (August 20, 1999), available from: http://www.denverpost.com/business/biz0820d.htm.

Memorandum from Mark Johnson, Director of Legislative Affairs and Legal Counsel, ITS America, to John Collins, President, ITS America, Washington, D.C., September 14, 1999.

Ogden, K.W., "Privacy and Electronic Toll Collection in Austrailia," *6th World Congress on Intelligent Transportation Systems* (Toronto, Canada, November 1999).

Pietrzyk, Michael C. and Edward A. Mierzejewski, "Electronic Toll Collection Systems: The Future is Now," *TR News*, No. 175 (November – December 1994).

Polk, Amy E., "Electronic Enforcement of Traffic Laws," *ITS Quarterly*, Summer 1998.

"President Clinton Signs into Law National 911 Bill," *Access ITS*, ITS America, [www.itsa.org/legislative.html], October 29, 1999.

Reebie Assoicates, *U.S. Freight Market: Commercial Data and Analysis*, Stamford, Connecticut (brochure.)

Smart Trek, *Smart Trek, The Path to Intelligent Travel*, Seattle, Washington (brochure.)

"The Surveillance Society," *The Economist* (May 1, 1999).

Texas Department of Transportation, *ITS Data Management System: Year One Activities*, by Shawn M. Turner, et al (Austin, Texas, August 1997).

U.S. Census Bureau, Statistical Research Division, "Data Licensing Agreements at U.S. Government Agencies and Research Organizations" (draft), by Paul B. Massell and Laura Zayatz (Washington, D.C., January 13, 2000).

U.S. Congress, Enrolled Bill, *Telecommunications Act of 1996*, 104th Cong., 2nd sess., 1996, S. 652, Sec. 702, available from: http://thomas.loc.gov.

U.S. Congress, Enrolled Bill, *Wireless Communications and Public Safety Act of 1999*, 106th Cong., 1st sess., 1999, S. 800, Sec. 5, available from [http://thomas.loc.gov/].

U.S. Department of Transportation, Federal Highway Administration, Intelligent Transportation Systems Joint Program Office , "Intelligent Transportation Systems Benefits: 1999 Update," electronic report, prepared by Mitretek Systems (January 12, 2000), available from: http://www.mitretek.org/its/benicost.nsf/.

U.S. Department of Transportation, Federal Highway Administration, ITS Joint Program Office, *ITS Data Archiving: Case Study Analysis of San Antonio TransGuide Data*, prepared by Texas Transportation Institute (Washington, D.C., August 1999).

U.S. Department of Transportation, Federal Highway Administration, ITS Joint Program Office, *Intelligent Transportation Systems (ITS) Information Security Analysis*, prepared by Mitretek Systems (Washington, D.C., 1997).

U.S. Department of Transportation, Federal Highway Administration, Intelligent Transportation Systems Joint Program Office, *Protecting Our Transportation System: An Information Security Awareness Overview*, by Keith Biesecker and Barbara Staples (Washington, D.C., November 1997).

U.S. Department of Transportation, Federal Highway Administration, Intelligent Transportation Systems Joint Program Office, *Study of Commercial Vehicle Operations and Institutional Barriers*, prepared by Booz, Allen & Hamilton (Washington, D.C., November 1994).

U.S. Department of Transportation, Volpe National Transportation Systems Center, *IVHS Institutional Issues and Case Studies: HELP/Crescent Case Study*, prepared by Science Applications International Corporation (Cambridge, Massachusetts, April 1994).

U.S. Department of Transportation, Volpe National Transportation Systems Center, *Maryland ITS Security Requirements Recommendations and Maryland ITS Security Implementation Recommendations*, prepared by Computer Sciences Corporation (Cambridge, Massachusetts, 1997).

U.S. Statistical Policy Office, Office of Management and Budget, Executive Office of the President, "Report on Statistical Disclosure Limitation Methodology," Statistical Policy Working Paper 22 (Washington, D.C., May 1994);

U.S. Statistical Policy Office, Office of Management and Budget, Executive Office of the President, "Checklist on Disclosure Potential of Proposed Data Releases," Statistical Policy Working Paper 22 (Washington, D.C., July 1999).

U.S. West Inc. v. Federal Communications Commission, 98-9518 (U.S. App., 10th Cir. 1999)

"Video Enforcement Systems," *ETTM On The Web* (updated April 10, 1997), available from: http://www.ettm.com.

Wright, Tom, "Eyes on the Road, Privacy and ITS," Traffic Technology International, (Autumn 1995), pp. 88-93.

Zhang, Wen et al., *A Primer on Electronic Toll Collection Technologies* Preprint. Tranportation Research Board, 74th Annual Meeting (Washington, D.C., January 1995).

Zhang, Wen et. al., *A Primer on Electronic Toll Collection Technologies*; and *An ETTM Primer for Transportation and Toll Officials*, ATMS Committee and ETTM Task Force, Intelligent Transportation Society of America (Washington, D.C., March 1995).