1-1-2002

# A New Approach to Assessing Road User Charges

David J. Forkenbrock
*University of Iowa*

Jon G. Kuhl
*University of Iowa*

# A New Approach to Assessing Road User Charges

# A New Approach to Assessing Road User Charges

David J. Forkenbrock
Director, Public Policy Center

Jon G. Kuhl
Chair, Department of Electrical and Computer Engineering

Public Policy Center
The University of Iowa
2002

This study was funded by the Federal Highway Administration and the departments of transportation serving California, Connecticut, Iowa, Kansas, Michigan, Minnesota, Missouri, North Carolina, Ohio, Oregon, South Carolina, Texas, Utah, Washington, and Wisconsin in a pooled funding arrangement. The conclusions are the independent products of university research and do not necessarily reflect the views of the funding agencies.

# PREFACE

For many years, the mainstay of highway finance in the United States has been the motor fuel tax. This mechanism for assessing road user charges has certain advantages, perhaps the greatest of which is that the tax is roughly proportional to the distance traveled. Some would argue that it is functionally invisible because motorists generally respond to the total price of a gallon of fuel, not to the tax component of this price.

The times are changing. In an effort to help the U.S. become more energy independent and to improve the air quality in our cities, the auto industry and the federal government are working cooperatively to design a new generation of vehicles that are either hybrid–a combination of electric and conventional internal combustion power–or are powered by hydrogen fuel cells. Several auto manufacturers also are experimenting with internal combustion engines powered by hydrogen. Various prototype vehicles have performed favorably in early testing, and several hybrid vehicles already have entered the marketplace.

It will be a few years before vehicles with these new propulsion systems become prevalent enough to severely impair motor fuel tax revenues, but the day almost certainly will come. Thus, this is a propitious time to explore a new approach to assessing road user charges—one that will accommodate vehicles with any of the possible propulsion technologies. This research has been carried out to develop such a new approach.

We began our research with a clean slate, in that many possible approaches were considered. Ultimately, the choice came down to smart roads and dumb vehicles or smart vehicles and dumb roads. Smart roads already are in operation; various technologies are being used to charge users of high-capacity toll roads (e.g., E-ZPass in the eastern U.S.), but roadside interrogators have little to offer in applications such as residential streets or low-volume county roads.

Rather quickly, we concentrated on smart vehicle technology: some form of on-board system that would enable a user charge to be assessed on the basis of the distance driven, wherever the travel occurred. In designing the new approach presented in this monograph, we emphasized user friendliness. The new approach must preserve the privacy of the road user, and it must be convenient and amenable to desirable features such as on-board navigation and emergency vehicle location. From the standpoint of the agency operating public roads, the new approach must be secure, robust, reliable, and sufficiently flexible to enable a variety of public policies to be supported.

Our research has been funded by a special pooled funding arrangement led by the Minnesota Department of Transportation. The participating agencies included 15 state departments of transportation and the Federal Highway Administration. The research was carried out at the University of Iowa's Public Policy Center.

# ACKNOWLEDGMENTS

In the preface we mentioned that this research was funded by the Federal Highway Administration and a special consortium of the departments of transportation serving 15 states. Contributing states include California, Connecticut, Iowa, Kansas, Michigan, Minnesota, Missouri, North Carolina, Ohio, Oregon, South Carolina, Texas, Utah, Washington, and Wisconsin. We are grateful for the support that made this research possible and for the interest and encouragement of our sponsors.

Before his retirement, Robert Benke, then Director of Research for the Minnesota Department of Transportation, played a pivotal role in forming the consortium and informing other states about the research to be undertaken. Without his efforts, this project would not have begun. His successor, Adeel Lari, shared Bob's enthusiasm for the project and was highly instrumental in recruiting additional state DOTs to the consortium. Ken Buckeye, of the Mn/DOT Office of Alternative Transportation Finance, served as the point of contact with the consortium and did a fine job of keeping everyone informed and making our meetings run effectively.

Members of the advisory panel are listed on the next page. We cannot say enough about the interest, support, and collegiality they showed. Attendance at the five panel meetings was excellent, nearly 100 percent. Discussions at the meetings were always stimulating, and they benefited our work greatly.

Several researchers made important contributions to this monograph. Paul Hanley, an assistant professor of urban and regional planning, helped prepare Chapter 3 on global positioning system (GPS) accuracy. Evan Seamone, a University of Iowa law student, conducted the majority of the legal analysis presented in Appendix A. Kyle Kroner, a graduate student in urban and regional planning, contributed to the discussion of possible data enhancements in Chapter 4. Ben Goldsworthy and David Harkins, also graduate students in urban and regional planning, helped assemble the data presented in Appendix B. Ryan Abel, a graduate student in electrical and computer engineering, contributed extensively to Chapter 6 on data storage and transfer.

We are grateful to Michael Shaw of the Office of the Secretary, U.S. Department of Transportation, who reviewed Chapter 3. Mr. Shaw oversees planning and policy development within the U.S. DOT regarding radio-navigation systems, including GPS.

Teresa Lopes, editor at the Public Policy Center, ensured that the text is accessible to a wide audience, while maintaining the monograph's technical accuracy. Kathy Holeton, administrative assistant at the Center, developed the graphics and made certain that the project proceeded smoothly. Leigh Bradford designed the cover.

With real appreciation, we acknowledge the many and diverse contributions of these capable people.

## ADVISORY PANEL MEMBERS

Adeel Lari, Minnesota, Chair
Doug Anderson, Utah
Todd Ashby and William Stone, Missouri
Charles Barone, Connecticut
Kenneth Buckeye and Robert Benke (former Chair), Minnesota
Peter Downey and Ashley Probart, Washington
Aarne Frobom, Michigan
Robert Haley, Kansas
Mark Joerger and Jack Svadlenak, Oregon
Robert Kranz, Wisconsin
Chris McAdams and Mrinmay Biswas, North Carolina
Thomas McPherson, Ohio
Susan Moe, Patrick DeCorla-Souza and Jim March, FHWA
Reza Navai, California
Keith Bishop, South Carolina
Carl Swerdloff, Office of the Secretary, U.S. DOT
Joanne Walsh and Victor Holubec, Texas
Don Ward and Stuart Anderson, Iowa

# TABLE OF CONTENTS

# FIGURES

# TABLES

# CHAPTER 1
# INTRODUCTION

At both the state and federal level in the United States, the primary method for charging road users is the motor fuel tax. In many ways this tax has served quite well. Road users are charged roughly on the basis of the amount of travel on the public road system. As such, motor fuel taxes have the desirable attribute of being a "pay-as-you-go" form of user charge. There are, however, several major shortcomings with motor fuel taxes including:

- an inability to generate the necessary revenue to provide quality transportation services in future years as hydrogen fuel cell vehicles and those with other new propulsion systems become more commonplace;
- high evasion, in the range of 10 to 15 percent for diesel fuel;
- increased fuel efficiency meaning lower receipts per mile traveled;
- no relationship to the type or cost of the facility being used or the level of service provided; and
- a weak relationship to the relative costs of particular trips such that some vehicle operators pay user charges that exceed the costs they impose, while others pay substantially less than their costs.

From the standpoint of efficiency, motor fuel taxes are not entirely satisfactory. Vehicle operators are not given signals to make them aware of the costs a particular trip may impose on society. With motor fuel taxes, it is not possible for government agencies to provide incentives to vehicle operators to change the nature of their road use, such as traveling on higher-standard roads or during off-peak hours.

The move away from state and federal motor fuel taxes must be accomplished with great care. When combined, fuel tax receipts at both levels of government account for almost two-thirds of all road user charges. In short, a very large amount of road financing capability is at stake.

Placing greater emphasis of vehicle registration fees is not a good alternative. These fees have no relationship to the amount of road use and thus the cost of serving the traveler. Property taxes, which are a major source of revenue to finance local streets and roads, also have no relationship to road use. Visitors to a jurisdiction, especially through travelers, pay no property taxes directly, and indirect payments through patronizing local businesses are very limited indeed. Quite clearly, a new means for assessing road user charges is needed.

## STUDY OBJECTIVES

The purpose of this research has been to design a system for charging road users that embodies as many attributes of an ideal system as possible. The key attributes of such a system include:

- a low cost of collection for both agency and user,
- a stable revenue stream,
- an ability to assess higher charges for users who impose higher costs,
- a low evasion rate,
- the ability to offer incentives for users to travel on appropriate roads and to spread their trips across time periods, and
- a procedure that is unaffected by the method of vehicle propulsion.

The approach to charging road users must not be burdensome, and it must be tamperproof, absolutely reliable, and a useful tool for achieving a variety of policy objectives. Perhaps of greatest importance, it certainly must not diminish the privacy of road users.

Fortunately, newly emerging technology makes it possible to design an approach to charging road users that avoids the problems and shortcomings of current mechanisms and that embodies the desirable attributes listed above. A wide variety of new locational and computing equipment is collectively referred to as intelligent transportation system (ITS) technology.

To begin moving toward an ideal system of road user charges, we have developed a new approach that is practical and cost-effective. The new approach will enable a real-time assessment of road user charges that are based on mileage accrual and, in the case of heavy vehicles, the option exists to take into account actual vehicle operating weights and configuration, as well as on the type of road being traveled.

The simplest way to assess a per-mile road user charge would be to periodically record the readings of certified odometers. Virtually no additional equipment would be required, and because on the total mileage traveled over a given period of time would be recorded, user privacy would be protected. Such a system, however, has a fatal flaw—there is no reasonable way to apportion the road user charges that are collected among the jurisdictions (primarily states) where the road usage actually occurred. Quite likely, the jurisdiction where the vehicle is based would retain all user charges collected; as a result, jurisdictions that attract numerous trips from other jurisdictions (e.g., those with major tourist attractions or those that serve substantial through traffic originating elsewhere) would fare poorly.

Thus, a key requirement of a mileage-based approach to assessing road user charges is the capability to return the revenue collected to the jurisdictions in a manner consistent with where the travel actually has occurred. A related point is

that each jurisdiction should be able to establish per-mile road user charges that are in accord with its needs and public policy choices. This said, the approach must respect the privacy of the traveling public, and it should incorporate the other attributes of an ideal user charge system as outlined above.

## SKETCH OF THE NEW APPROACH

A simple graphical overview of the new approach appears in Figure 1-1 on page 4. Key to the new approach is a simple on-board computer. The computer stores a record of actual road use charges. Periodically, this record is uploaded and transmitted to a data processing center; we refer to it as the collection center. The center bills a vehicle owner and reimburses the states, counties, and cities operating the roads on which the vehicle has traveled. The on-board system is simple, secure, and capable of protecting the user's privacy. Importantly, the on-board system enables a variety of user charge conventions. In its simplest form, this approach can be used to assess a vehicle-miles-traveled (VMT) tax. With a VMT tax, the computer calculates the number of miles actually traversed; then it compares this mileage with that obtained through an odometer feed. It then applies appropriate user charge rates to the mileage traveled within each jurisdiction. In a more sophisticated form, the new approach would enable a lower per-mile user charge for energy-efficient vehicles or others that help advance other societal objectives.

### Charging Autos

Inputs to the computer can be quite simple for autos, involving only a global positioning system (GPS) receiver, a geographic information systems (GIS) data file, and the vehicle's odometer (for back-up data on distance traveled). The GIS file contains data that define boundaries of the respective states. A receiver on board the auto uses GPS signals to determine the vehicle's position. The computer reconciles this position with the stored data polygons (a series of coordinates that define the boundaries of the respective states) to determine the state in which travel has occurred; the miles traveled within that data polygon are used to compute user charges, which in turn are stored. When a vehicle crosses into another state, it enters a different data polygon; and travel within that polygon is used to compute user charges. Of course, substate polygons, such as those defining a metropolitan area, also are feasible.

The GIS file that defines polygons is stored in the on-board computer and is readily updateable. Periodically, the collection center transmits updates of the GIS file to the vehicle using a smart card as a "messenger." A smart card is a small credit card-sized plastic device that contains an embedded computer chip in the form of a microprocessor and/or a memory module. This technology was developed in France more than 20 years ago. Smart cards are very durable and should serve a typical user for the life of the vehicle. If the smart card is lost or destroyed, it can easily be replaced at a small cost to the user (a typical smart card costs less than $5). Communication via a smart card is done using a reader that closely resembles the credit card readers found in nearly all businesses. Normally, the smart card

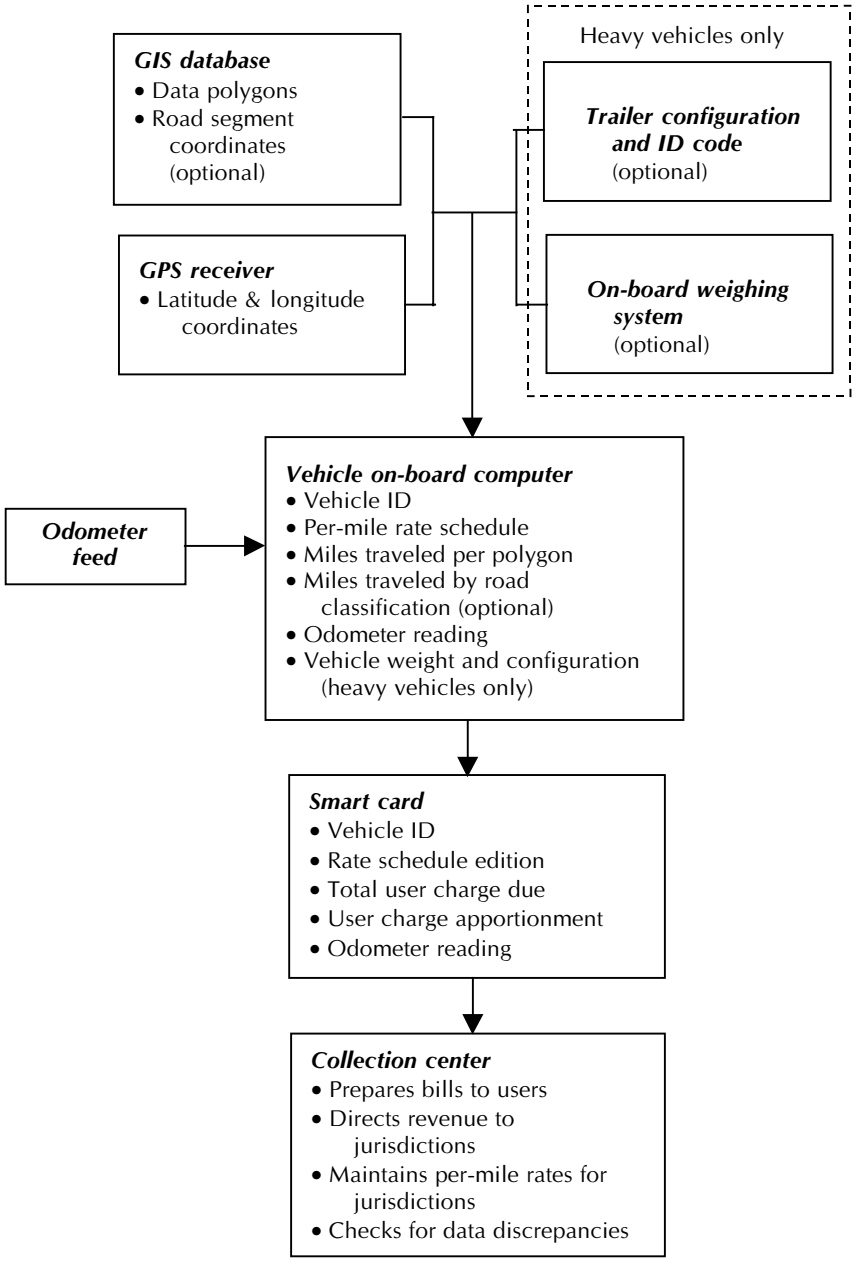



**Figure 1-1. Overview of the new approach to assessing road user charges**

occupies a slot in the vehicle's dash panel. The on-board computer continuously updates the smart card regarding total user charges owed to each state or other jurisdiction defined by a polygon. Data transferred to the smart card, then, are in units of dollars. Before storing the data, the on-board computer will have (1) measured the distance traveled within each polygon, (2) applied the appropriate per-mile user charge as established by the applicable jurisdiction, and (3) calculated the user charges owed to each jurisdiction. Thus, the vehicle operator can remove the smart card at any time and insert into a reader to transmit the charges due to the collection center.

Why would a vehicle owner want to upload billing data promptly? A simple display on the instrument panel during vehicle start up displays the current user charges stored in the on-board computer. Each jurisdiction can choose to levy an interest charge for road use that occurred more than, say, 30 or 45 days in the past. The instrument panel display can show both current user charges and interest accrued. As the interest charges mount, the display will serve to encourage the vehicle owner to upload the billing data. Failing to upload data at all may result in a requirement to pay all user charges in arrears before receiving the next year's vehicle registration.

During the data uploading process, the smart card authenticates the user and then anonymously uploads the road use information. When the collection center identifies the user, it checks for fraudulent behavior or malfunctions. If there is a problem, the smart card is notified to prompt the user to go to a service center; and the system flags that particular vehicle. During this communication, the collection center updates the vehicle's rate schedule through the smart card, if the stored schedule is not current. The center also provides a one-time encryption key to the smart card to facilitate anonymous uploading of the user charges arising from travel in each jurisdiction. Once the collection center receives the information on how much mileage occurred in each jurisdiction, the center apportions the funds to the appropriate jurisdictions.

We stress that the apportionment data will be anonymous. It is not necessary to know which vehicle generated a particular sum of user charges for each jurisdiction; what is necessary is the amount to be apportioned to them. In every case, the total amount for all jurisdictions taken together equals the single value uploaded in the initial contact made by the vehicle via the smart card. Thus, the only figure that can be tied to a particular vehicle is a single dollar amount for total user charges and interest due, if applicable. This approach maximizes user privacy and ensures a fair distribution of revenue.

User acceptance of the new approach to assessing user charges could be increased if other benefits result. For example, navigation displays, now a costly option on luxury autos, could become standard equipment or a low-cost option. Nearly all of the components needed for such displays will be on board the auto; mass-producing them for all vehicles will be simple. Note, too, that looking a few years into the future, regardless of how user charges are assessed, traveler information displays are likely to become commonplace (their costs already are beginning to

fall). In that case, adding the capacity to store road use information will be easy and inexpensive.

Another user benefit of the GPS/GIS system will be emergency location notification. The Advanced Collision Notification System, which is beginning to receive national attention, uses cellular transmissions to relay a vehicle's exact location to the appropriate service provider in the event of a crash, health problem, or mechanical breakdown. The protection this sort of system offers motorists is likely to be valuable to many people, but it will be especially beneficial to elderly drivers and those who travel in remote areas or unsafe parts of cities. It should be stressed, however, that the GPS system itself does not transmit any form of location data. GPS satellites only send radio waves that the vehicle's GPS receiver uses to calculate its location. GPS satellites are unable to receive any form of information from a vehicle.

**Charging Heavy Vehicles**

In the case of large trucks and other heavy vehicles, simple per-mile user charges could be instituted in a manner similar to that for autos. Optionally, these charges could be slightly more tailored to take into account vehicle and roadway attributes. Like autos, heavy vehicles will have a GPS receiver and stored GIS information in the form of data polygons. Because privacy is much less of an issue with commercial vehicles, the polygon data could be supplemented with several levels of road classes. In this way, user charges for road use by heavy vehicles could be varied according to the standard of road traveled. For example, a state may choose to levy a lower per-mile charge for travel by heavy vehicles on interstate highways and other facilities that are capable of withstanding high axle loads without being damaged. The road user charges uploaded to the collection center can easily be made to reflect several different per-mile rates that vary with the standard of road used.

One way to tailor user charges for heavy vehicles is through the use of an on-board weight indicator. The weight indicator would be activated each time the cargo doors are closed (in the case of a freight semi-trailer truck). The weight indicator, which is a simple strain gauge attached to the trailer's suspension, would transmit information to the on-board computer, indicating the current weight. A code would inform the computer about the configuration of the trailer, especially the number of axles. The computer then would take into account vehicle weight and configuration, along with type of road being traveled, in calculating the road use charges that are due.

It is noteworthy that the new approach eliminates the pitfalls of methods such as weight-distance taxation: The uniform per-mile rate (regardless of current weight) of that approach is replaced with a much more flexible approach, and evasion will cease to be a problem. Of course, individual states can determine the extent to which they assess user charges based on the type of road being traveled or on vehicle weight and configuration.

With the new approach, motor carriers will benefit by the elimination of tollbooths; and interstate permitting can be automated. Also, opportunities that do not exist today become available; for example, by adding axles and traveling on higher-standard roads, operators can minimize their user charges.

## OVERVIEW OF THIS MONOGRAPH

In developing the new approach to assessing road user charges, we have had to address a variety of issues, some practical, others technical, and still others related to a series of intertwined public policy considerations. As we designed the new approach presented in this monograph, we emphasized user friendliness. The new approach must preserve the privacy of the road user, and it must be convenient and amenable to such desirable features as on-board navigation and emergency vehicle location. From the standpoint of the agency operating public roads, the new approach must be secure, robust, reliable, and sufficiently flexible to enable a variety of public policies to be supported.

The chapters to follow address these issues. In Chapter 2, we present the data system that is the heart of the new approach. It is designed to enable the necessary data on road use to be collected without compromising the privacy of vehicle operators who are traveling on public roads and highways.

In Chapter 3, we assess the capabilities of the global positioning system (GPS) to support the new approach. We discuss current GPS accuracy levels, sources of accuracy degradation, and new GPS technologies that lie in the not-too-distant future.

Chapter 4 contains a discussion of optional data-gathering capabilities inherent to the new approach to assessing road user charges. While we do not recommend that these capabilities be exercised before public acceptance is established, we think it important to take them into account in the basic design. Generally, these enhancements will facilitate major improvements in transportation planning and road system management.

If the new approach is to be a viable method for assessing road user charges, it must be highly reliable, incapable of being "spoofed" (fed erroneous information regarding road use by the vehicle), and protective of the vehicle owner's privacy. In Chapter 5, we lay out a series issues regarding robustness, security, and protection that must be addressed in the design and operation of the new approach to assessing road user charges.

In Chapter 6, we present practical methods for (1) acquiring road-use data and converting these data to a total user charge, (2) uploading this user charge to a collection center, and (3) anonymously instructing the collection center as to how the user charge should be apportioned among the states in which travel has occurred. The methods suggested build on the concepts contained in earlier chapters.

Chapter 7 contains the study conclusions and our recommendations pertaining to implementing the new approach to assessing road user charges. In this chapter we suggest beginning with a fairly simple polygon approach but building in capabilities that a given state may choose to include at a later time. We stress the importance of making the new approach highly flexible and thus capable of supporting a host of policy initiatives that the states or communities within them may find desirable either now or in the future.

Appendix A is a thorough assessment of the legal issues surrounding the right to privacy while traveling in a private vehicle. The appendix includes both a review of applicable legal principles and case law. To make this analysis useful to appropriate legal council, we have formatted the appendix in a slightly different manner than the remainder of the monograph (e.g., legal citations and expository footnotes).

Appendix B contains a projection of auto and truck vehicle turnover rates. Our objective is to provide a preliminary estimate of how quickly the auto and truck fleets can be expected to be replaced and thus how soon the new approach could become the predominant method of charging road users.

Appendix C provides greater technical detail on the robustness, security, and protection issues discussed in Chapter 5. In this appendix, we specify a set of security, privacy and robustness requirements for the new approach and suggest a preliminary architecture that demonstrates the technical feasibility of meeting these requirements.

# CHAPTER 2
# A DATA SYSTEM TO ENSURE USER PRIVACY

There is no question that the new approach constitutes a major change in the way road users are charged for their travel on public roadways. While in many cases the actual amount users pay may change relatively little, the new approach to assessing road user charges will be a substantial departure from the traditional motor fuel tax. Maximum privacy for road users is likely to be the most critical single issue and must be addressed in a creative way. At the same time, it is important that the approach be designed with enough flexibility to enable a variety of public policy initiatives to be pursued at a later date, if the public supported them. In this chapter, we examine the feasibility of implementing a simplified version of the new approach that maximizes user privacy initially yet enables additional features to be added later as public acceptance grows.

## DETAIL IN USER DATA

Many of the possible features of the new approach to assessing road user charges are optional, depending on the preferences of a given jurisdiction. The most fundamental requirement is that the new approach be capable of assigning road user revenue to the state where travel occurred. For this requirement to be met, all that is required is that road use within each state during a billing period be recorded. It is not necessary to know upon which roadway the travel occurred or when it took place. There are practical reasons for a state DOT to want such data (see Chapter 4); but they are not required for the new approach to be implemented.

A second type of data that would be logical to collect is information on the type of vehicle making the trip. Even the motor fuel tax results in heavy vehicles paying greater user charges than smaller, light-weight vehicles that impose far less wear on, and hence cost to, the road system. The new approach will enable per-mile charges to vary with vehicle type to whatever extent policy makers feel is appropriate. Other than data on road use in each state, the general type of vehicle using the road system, and the person or organization to be billed for this road use, no data are required for the new approach to be implemented.

There is a clear need for a road user charge system that is fairer and more flexible than the state motor fuel tax. One of the problems with the fuel tax is that travelers often purchase fuel—and thus pay the motor fuel tax—in one state and then use the roads in another. One could argue that, on balance, where fuel taxes are paid and where road use occurs averages out. Particularly in the case of states with major highways running through them en route to large metropolitan areas, however, that may well not be the case. Likewise, states with major tourist attractions often draw trips from contiguous states, with travelers arriving and returning home on a single tank of fuel. It makes sense to ensure that state-level road user charges are

distributed to the state in which travel actually occurred. The motor fuel tax is incapable of this.

It is worth stressing that if the new approach did nothing more than enable a near perfect match of user charge revenue and actual road system use by state, it would be a significant improvement. Add to that its capability to charge vehicles fairly, however they are powered; and the inherent strength of the new approach becomes apparent.

### The Critical Issue of Privacy

In Appendix A, we explore the legal foundations of privacy and conclude that even if extensive data were collected, the new approach would not constitute a legal infringement of users' privacy. For the new approach to gain widespread acceptance, however, it must be perceived as in no way violating commonly accepted standards of privacy. Specifically, there is abundant evidence that people tend to be more protective of their privacy in terms of others knowing where and when they travel than they are about many other aspects of their lives. It is widely understood that credit card companies inform businesses about the purchasing behavior of their customers, and telephone billings indicate with whom one has spoken and when. Yet, it would be unwise to assume that the general public would be comfortable with a road user charge approach that enables government agencies to know much about their travel patterns on a person-specific basis.

It is difficult to predict trends in what the public will accept or reject in its relationship with the government. To be sure, the motor fuel tax does not facilitate scrutiny of people's travel; and any sort of alternative approach to charging road users must not do so either. Two features are key to maximizing public acceptance of the new approach. First, the data on road use stored on board the vehicle and transmitted to the collection center should be as non-specific as possible (i.e., should not reveal which roads were traveled or when). Second, the collection center at which the data are processed should be operated by a private firm working under a stringent series of controls. Under no circumstances should these data be used for any purpose other than assessing road user charges.

The first of these two issues, keeping the data as non-specific as possible, is the primary topic of this chapter. Underlying the discussion that follows is the presumption that it is imperative to assure the public that only very basic road-use data will be collected and that person-specific data will never be used for any purpose other than assessing road user charges. Possible uses of aggregate data are discussed in Chapter 4.

### Differences in Data Detail Between Autos and Trucks

Very fundamental differences exist between the nature of operations involving private autos and larger commercial trucks. In short, privacy is very much an issue with people riding in autos but generally is less of an issue with commercial trucks. The distinction between privacy expectations for autos versus trucks is important

because equity issues are far more pressing among trucks than among autos. Specifically, the societal costs imposed by autos operating on any given standard of roadway do not differ much. In fact, the only significant variation in the costs to society of different auto trips are those arising from congestion; and, in the interest of public acceptance, varying road user charges to mitigate congestion certainly should not be an initial objective of the new approach (see Chapter 4).

The situation is very different with regard to trucks. Especially in the case of heavy trucks, societal costs of travel vary substantially with the standard of road. Data from the 1997 Federal Highway Cost Allocation Study (FHWA 1997) indicate that the per-mile costs imposed by a heavy truck can vary by a factor of five, depending on the standard of the particular road being traveled. These costs also vary greatly with a truck's gross weight and configuration (i.e., number of axles). Small, et al. (1989, Table 3-4) contend that an 80,000-pound combination truck imposes pavement costs 34 times as great as one weighing 33,000 pounds. The same authors estimate that an 80,000-pound combination truck with six axles damages pavement about 41 percent less that a comparable truck with five axles (Table 3-5).

These differences suggest that an appreciably simpler approach is appropriate for autos than for trucks. Specifically, if the policy objective is the collection of user revenue at the state level, it really is only necessary to know in which state an auto has traveled. There is no need to record the standard of road on which this travel has taken place. In the case of trucks, the simplest method would be to identify a backbone road system consisting of interstate highways and other high-standard roads. User charges for travel on high-standard roads could be set lower than for travel on lower-standard roads, where the societal costs are generally higher. Likewise, data on a truck's configuration and gross weight could be recorded and used to influence the per-mile user charge that is assessed. It is true, however, that more elaborate road classification distinctions will improve equity among trucks, such that the true cost of facility use will be more accurately reflected in the user charges assessed. Generally, a more disaggregated system of road user charges would benefit long-haul carriers operating on interstate highways.

In summary, much less detailed data on road use could be collected from autos traveling on public roadways than from heavy trucks (e.g., those over 26,000 pounds). A standard per-mile user charge for autos will suffice quite nicely. Because of the considerable disparity in the costs imposed on society by trucks of different weights and configurations operating on roads of different standards, it is advisable to vary per-mile assessments for heavy trucks. Such variation in user charge structures would mean that more detailed data will need to be collected for trucks than for autos. As privacy requirements are very different for the two general types of vehicles, collecting the different levels of data should not pose much of a problem.

## A STATE-LEVEL DATA POLYGON SYSTEM

To allay privacy concerns during the initial implementation phase, we suggest that no road-specific data be included in the road use file stored on board autos.

Instead, only the boundaries of the 48 contiguous states (and possibly Alaska and Hawaii) should be stored (requiring only a very small GIS file). The on-board GPS receiver will position the vehicle within a given polygon (state). In this way, road use within each state could be recorded for uploading to the collection center. No data need to be stored regarding the specific roads traveled or the time of travel. A billing statement could merely list the miles driven by state and the per-mile charge levied by the applicable states. Even better, only the total user charge owed for each state could be stored in the on-board computer for eventual uploading to the collection center. Such an approach would absolutely minimize potential invasions of privacy.

A graphical depiction of a data polygon system defining state boundaries is presented in Figure 2-1. The arrows depict both intrastate trips and those that begin in one state and end in another. For each trip, the on-board computer will store the appropriate data for road use within a given state before the vehicle crosses the boundary into a neighboring state.

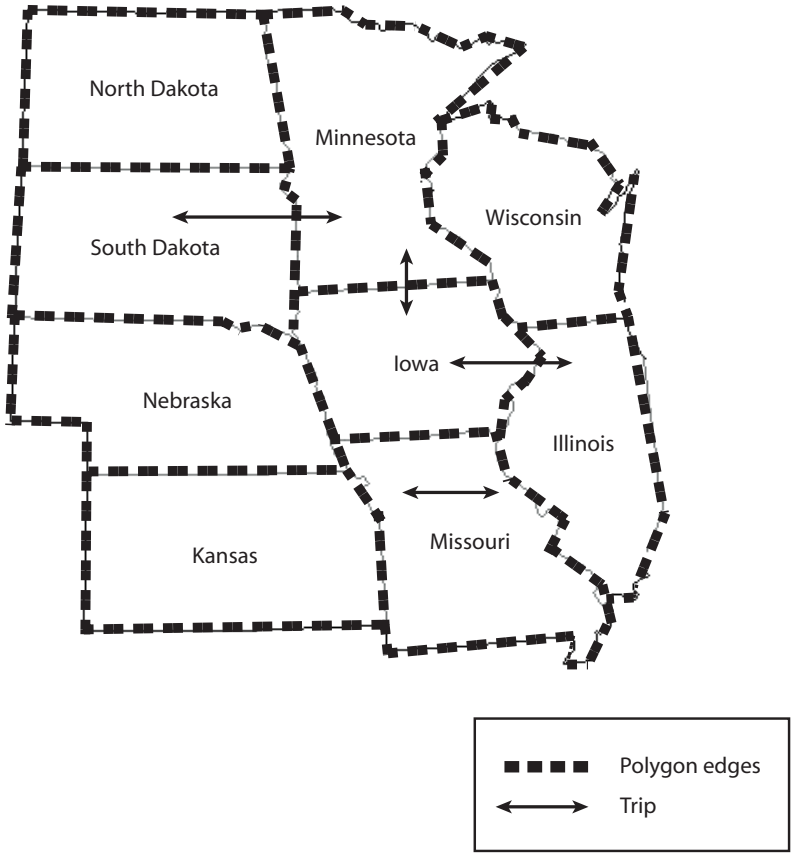



**Figure 2-1. Example of state data polygons**

### Two Options for Data Storage

Applying the smart-card technology we discuss in Chapter 6, two different data storage options are workable: vehicle miles traveled (VMT) or total road user charges. If VMT data were stored, the number of miles actually traveled within each state polygon would be uploaded to the collection center. The center would apply the correct per-mile user charge for each state in which travel occurred, and the vehicle's owner would be charged for the total amount owed to the respective states.

Smart-card technology, however, also can enable the collection center to download to the vehicle the current per-mile user charge rate for all states when the vehicle operator uploads data on road use. It would thus be feasible for the on-board computer to multiply the number of miles traveled within each state by the applicable per-mile charge. If this were done, only one number would be uploaded for road use within each state—the total user charge due.

There are several advantages to the latter approach. It absolutely maximizes privacy and comfort on the part of the public that no data on miles traveled on particular roads or even in specific areas of the state will be stored. A second advantage is that it will be possible to display on a vehicle's instrument panel the current total user charge owed. For user charges that are delinquent beyond a certain period of time, perhaps 30 or 45 days, an interest charge could be applied to encourage prompt payment. This interest charge also could be displayed.

It is somewhat ironic that with this approach, if different functional classes of roads within a state had varying per-mile user charge rates, privacy would be further enhanced. Looking at someone's total user charge for a state, it would be impossible to determine exactly how many miles were traveled within the state; there could have been more miles traveled on lower cost, high standard roads or fewer miles driven on lower standard roads for which user charges may be higher.

Upon review of the pros and cons of each data storage option, we recommend the one in which user charges will be computed on board the vehicle, stored, and uploaded as a dollar amount to the collection center. Being able to inform users of their exact current total charge owed constitutes a major advantage. The slight improvement in perceived privacy also is an advantage worth pursuing. Accordingly, in the remainder of this chapter and in Chapter 6, we will emphasize this option.

### Accuracy of Data Polygons

We should emphasize that it is possible to construct very accurate data polygons. Using established coordinates that define each state's boundaries, the margin of error in the GIS data file will be insignificant. In fact, the only real source of error will be position inaccuracy introduced by a vehicle's GPS system. Because it is extremely rare for a major roadway to be located directly on a state boundary, whatever minor inaccuracies do occur will be longitudinal errors that take place

when vehicles cross state boundaries. In the vast majority of cases, these errors will equate to tiny fractions of a cent. To the extent that GPS errors are Gaussian (normally distributed over time), such errors will come very close to canceling out as vehicles cross a boundary going in opposite directions.

### Features Needed to Charge Heavy Trucks

For medium to heavy trucks, a nominal amount of road-specific coding may be advisable to accompany the state-defining polygons. As noted above, high-standard roads can be designated and a lower per-mile user charge assessed on them. The default per-mile charge will apply to lower-standard roads, those more likely to be damaged by heavy vehicles. It is worth noting that the trailers of combination (semi-trailer) trucks could have small transmitters that send two pieces of information to the on-board computer: (1) the current configuration (primarily the number of axles, but also the number of trailers in the case of multiple-trailer combination trucks) and (2) the current vehicle weight, as measured by a simple on-board scale attached to the trailer suspension. Each time the cargo doors are closed on a freight trailer, for example, the current weight can be relayed to the on-board computer.

It will be feasible for states to keep per-mile charges on file at the collection center so that user charges vary with the standard of road traveled, trailer configuration, and vehicle weight. The rate schedule can be downloaded to trucks' on-board computers as with autos, and these computers can then compute user charges based on these considerations. Because privacy is much less of an issue with commercial trucks, provision could be made for fuller documentation of road user charges, such as mileage on various categories of roadway, each truck's weight and configuration while these mileages were driven, and, of course, the jurisdiction in which the travel occurred.

### Different Data Systems for Trucks and Autos

No serious problems will result from using slightly different road data systems for trucks and for autos. Both data systems will employ state-defining polygons, but the data system for trucks will have at least a partial coding of roads. As mentioned above, high-standard roads, such as interstate highways and other designated four-lane or higher facilities, can be given special designation in the GIS road file. When road-use VMT within each state are used to calculate charges in the vehicle's on-board computer, these VMT can be separated into travel on high-standard and other roadways. Each state can choose how much, if at all, to vary road user charges between the two (or more) general classifications of roads.

## RELIABILITY PROVISIONS

While GPS receivers generally are highly reliable, it is possible that a significant malfunction could occur (see Chapter 3). It also is possible that a vehicle's GPS antenna could be inadvertently or intentionally blocked from receiving the satellite signals needed for proper operation. Travel through tunnels likewise could disrupt the ability of the GPS receiver to provide the vehicle's on-board computer with accurate information. Thus, it is essential that vehicles be equipped with a back-up

system capable of providing the on-board computer with information about their location.

Redundant data on distance traveled can quite easily be obtained from a vehicle's odometer. Increasingly, modern motor vehicles feature electronic odometers that are fully integrated into the electrical system of the vehicle. Auto manufacturers feel it is important to produce relatively tamperproof odometers in the interest of enforcing mileage limitations of vehicle warrantees. With the latest rotation-sensing equipment used for stability control and anti-lock braking systems (ABS), extremely accurate and secure odometers are rapidly becoming universal.

For reasonably accurate dead reckoning, however, distance information must be augmented with information on the vehicle's direction of travel. Micro-scale inertial chips are a simple and inexpensive means for providing the on-board computer with directional information for limited periods of time. If the signal interruption to the GPS receiver is of short duration, the inertial chip in combination with the odometer can provide a reasonably good estimate of when the vehicle crossed from one polygon into another. The road-use data obtained under these conditions will not be error free; but in nearly all cases, it will provide a fairly accurate means for apportioning the revenue from road user charges among neighboring jurisdictions. It is important to stress, however, that over a protracted period of time the back-up data acquisition system just discussed will not be an accurate mechanism for keeping track of the polygons in which a vehicle has traveled.

Thus, while accurate data on distance traveled will be fed to the on-board computer, in some cases it may become increasingly unclear which polygon was the site of the travel. The importance of accurately apportioning road user charges among jurisdictions in which travel has occurred argues for penalties if an owner allows his or her vehicle to operate with a defective GPS receiver for a substantial time. It would be a simple matter to provide a message to the vehicle operator that the per-mile user charge will progressively increase if the on-board system is not restored to full functionality. Such a provision is needed for the comparatively rare occasions when prolonged failures occur. Note that with the redundant capability to estimate miles traveled, the incentive for anyone to attempt to disrupt the normal operation of the GPS receiver is very small—it only will affect how the user charges paid will be distributed among jurisdictions.

## EXPANDABILITY FOR FUTURE POLICY CHOICES

For auto travelers, this simple, state-defining polygon data system will enable the new approach to assessing road user charges to achieve its primary objective of providing a reliable, flexible mechanism for collecting revenue. It also will minimize concerns on the part of the traveling public about the government or a firm under contract to it keeping data on individuals' travel patterns. There is little doubt that perceptions of privacy invasion are the most significant barrier to implementation of the new approach. The idea of being billed by a private entity for the total user charge owed to a state over a period of time might well be widely accepted, particularly if the phase-in is managed carefully (see Appendix B).

### Contrast Between a Polygon Data System and Road Segment Coding

In Chapters 3 and 4, we discuss a series of issues related to coding road segments stored in a geographic information system (GIS) data file. To briefly preview these chapters, with segment-specific coding a vehicle's on-board computer will constantly compare the vehicle's present position, as determined by a global positioning system (GPS), with the GIS road file. In this way, the computer will keep track of the vehicle and generate a record of road use. Each road segment in the GIS file could be coded to reflect the standard of road for the segment, as well as the political jurisdiction in which it was located. Thus, relatively detailed road-use data could be amassed regarding miles traveled by type of road within each jurisdiction.

Given that road user privacy is a primary concern for auto travelers, however, the simpler data polygon system is likely to have much greater public appeal. To be sure, the level of data transferred to the collection center will be appreciably less, and it will not be possible to make inferences about travel behavior by an individual (e.g., miles traveled on rural collector roads within a particular state during a specific month). As discussed earlier, the only data that will be transferred will be the total user charge accrued within an entire state during the billing period.

### Substate User Charges

In time, once society becomes accustomed to the state-level mileage-based user charge, it very well may be the case that substate user charges will become attractive replacements for other less equitable means of financing roads. For example, local governments (e.g., municipalities and counties) could choose to replace property taxes with mileage-based user charges. In many locales, up to three-quarters of the revenue used to construct, maintain, and repair roadways is derived from property taxes. Out-of-town visitors generally do not contribute property taxes, but they impose costs comparable to those of local residents. By the same token, local property tax payers who make little use of the local road system pay property taxes regardless.

At some point in the future, it would not be difficult to update polygons to define substate areas, if the public supported doing so. Such polygons could coincide with the limits of a multi-government metropolitan area, a several-county area, or even a single community. Miles traveled within each polygon could easily be measured by the on-board computer and appropriate per-mile user charges applied to them for subsequent transfer to the collection center for inclusion in billings.

Eventually it may even be acceptable to record road use by type of road standard. Should that materialize, moving from a polygon data system to one based on coded road segments would not be difficult. The GIS files stored aboard vehicles would be replaced with updated, more detailed versions. Beginning with a polygon data system and progressing to coded road segments would mean that more time will be available to geocode the many lower-standard roads across the country that do not appear in currently available GIS road files.

## CONCLUSIONS

In the earlier stages of our research, we developed a more complex and date-intensive system that would have generated information valuable to policy makers. The concept of a simpler approach to identifying the jurisdiction in which travel has occurred evolved from concerns that a more detailed road-segment specific record may generate resistance on the part of motorists. The polygon data system emerged from extensive research into possible mechanisms that will accomplish the primary objective of collecting a stable, reliable stream of revenue from road users to finance transportation services at the state level. It represents new thinking about how to accomplish this objective with the greatest possible level of public support. We conclude that the polygon data system is the simplest possible mechanism that will enable the computers on board autos to accurately record the miles traveled within each state. Because travel on individual roads will not be recorded, privacy implications are absolutely minimized.

A key trade-off, however, is that the advantages of more precise aggregate records of road system usage will have to be delayed or foregone. It will not be possible to conduct travel demand analyses using aggregated data on origin and destination zones within metropolitan areas, nor will volume and vehicle mix data by road segment be available. On the other hand, initial acceptance of the new approach will almost certainly be greatly enhanced.

Privacy is much less of an issue for heavy freight trucks. The costs to society of operating these trucks vary substantially with the standard of roadway and with the weight and configuration (mainly the number of axles) of the truck. By coding major, high-capacity, and high load-bearing highways, it will be feasible to charge heavy trucks a different per-mile rate for travel on these facilities and on lower-standard roads. This simple coding system, as a supplement to the state polygon system, will enable a two-tier user charge system for heavy trucks.

Redundancy in distance traversed and direction of travel is essential with the new approach. While GPS receivers are very reliable, it is possible for failure to occur due to equipment malfunction, tampering, or travel through tunnels. A fully integrated odometer is capable of providing the on-board computer with accurate information on distance traveled, and inertial components are capable of providing information on direction of travel for short periods of time (e.g., when traveling through a tunnel).

It is important to keep in mind that this polygon data system could eventually be enhanced in numerous ways. If the public supported it, smaller substate regions could be defined. This would enable areas that chose to do so to replace less fair and effective revenue-generation mechanisms with mileage-based road user charges. Eventually, it may become desirable to implement the more detailed road-segment coding conventions discussed in Chapter 4, at which time much greater flexibility in assessing road user charges would become possible.

The new approach to assessing road user charges represents a major change in the way travelers on public roadways would pay for the services provided them. Because it is so new and different, it seems prudent to move carefully and incrementally. Simply charging for the number of miles traveled within a state will constitute a significant improvement over traditional motor fuel taxes, and it will minimize pubic concerns over intrusions of privacy. The state polygon data system will fully enable the new approach to be implemented. With time and public support, a variety of flexible options for road user charges could then be pursued.

**REFERENCES**

Federal Highway Administration (FHWA). 1997. *1997 Federal Highway Cost Allocation Study*. U.S. Department of Transportation. Washington, DC: U.S. Government Printing Office.

Small, Kenneth A., Clifford Winston, and Carol A. Evans. 1989. *Road Work: A New Highway Pricing and Investment Policy*. Washington, DC: The Brookings Institution.

# CHAPTER 3
# GPS ACCURACY ISSUES

At the heart of the new approach to assessing road user charges is an on-board computer that stores data on road use. The primary data for the computer relate to the vehicle's present position as determined by a global positioning system (GPS) receiver, augmented with a dead reckoning system. The computer reconciles the GPS data with a road file stored in a geographic information system (GIS). The computer keeps track of the progress of the vehicle and generates a record of road use. As we discuss in Chapters 2 and 4, these data could be stored in the on-board computer at various levels of detail. At one extreme, only a record of total user charges owed to each political jurisdiction could be stored for eventual uploading to a billing or collection center; at the other extreme, it would be technologically feasible to store a record of the origin, route, and destination of each trip made by a sample of vehicles and to upload the data without divulging the identity of these vehicles. We stress that each state or local jurisdiction could enable road users to decide how much detail provide to public agencies. The new approach is designed to be highly flexible.

In terms of the feasibility of the new approach, the issue of data accuracy is as crucial as that of data detail; and thus it is the topic of this chapter. We explore the accuracy required by the new approach when two quite different (but interrelated) objectives are pursued: (1) collection of revenue from general user charges and (2) varying user charges to pursue equity or influence patterns and nature of road use. In general, much less accurate data are needed to collect user charges per se than to implement most public policies that involve some form of variable road user charges. As we stressed earlier, our purpose in discussing broader policy initiatives is to ensure that the new approach has the capacity to eventually enable a variety of objectives to be pursued. Clearly, the initial objective of the new approach to assessing road user charges should be revenue collection.

We begin by briefly discussing the necessary and desirable attributes of road-use data for each of these purposes and then go on to assess the current accuracy capabilities of GPS equipment. Finally, we offer conclusions as to how capable current GPS/GIS technologies are of supporting the two purposes that may be pursued via the new approach to assessing road user charges.

## THE OBJECTIVE OF REVENUE COLLECTION

The primary objective of the new approach to assessing road user charges is to provide a fair, stable source of user-generated revenue to support the nation's streets, roads, and highways. More specifically, we have sought to develop an approach that has as many of the desirable attributes listed in Chapter 1 as possible:

The approach to charging road users must not be burdensome; and it must be tamperproof, highly reliable, and capable of protecting users' privacy.

### Data Needed

For these attributes to be pursued, fairly basic equipment on board the vehicle will suffice. All that is needed is a GPS and GIS system capable of identifying the specific roadway one is traveling, along with an on-board computer capable of storing a record of user charges within each data polygon (i.e., by jurisdiction; see Chapter 2). Even with the objective of revenue collection, some states may want to charge different per-mile rates for vehicle miles traveled (VMT) by (1) the classification of roadway (e.g., rural interstate, urban collector, residential street) and (2) the political jurisdiction within which the roadway is found. As we discuss in Chapter 4, more extensive data would substantially enhance the capacities of state DOTs and local governments to plan and manage their road systems. These enhancements, however, are not necessary to pursue the purpose of revenue collection per se.

### Accuracy Requirements

When revenue collection is the objective, for autos the basic accuracy necessary with the new approach is the ability to identify polygon in which one is traveling. As discussed earlier, in some applications data on the classification of the roadway upon which a vehicle is traveling also will be needed. This requirement would come into play if a jurisdiction were to choose to base its user charge rate (within its data polygon) on different road segments' functional classifications.

We should stress that for autos the per-mile charge generally would not vary much, if at all, with these different road classifications. In the vast majority of cases, the issue will really be how many miles were traveled within a given jurisdiction, not upon which roads the travel occurred. Thus, for autos, in the rare occasion when the GPS/GIS system is unable to pinpoint which road segment was being traveled serious problems would not occur in terms of charging the user too much or not enough.

The most confining circumstance for charging autos with the simple data polygon mechanism would be a case in which two roads were in close proximity but lay in different political jurisdictions. Erroneously recording the jurisdiction in which travel occurred would result in too much revenue flowing to one of these jurisdictions and not enough to the other. There is no good way to state definitively how close in proximity such roads might be found, but very rarely will the spacing be closer than 20 meters (65 feet). We suggest that a 20-meter level of accuracy will be quite sufficient in essentially all circumstances when revenue collection is the objective. As we discuss later, certain applications that involve varying user charges would require greater accuracy.

The necessary accuracy level is only slightly greater for heavy vehicles. In many jurisdictions, policy makers are likely to want to charge different rates for roads that

are less able to withstand higher axle loads than for those designed for such loads. An issue of accuracy may arise if roads of different standards are in close enough proximity that the GPS/GIS system cannot accurately determine which road is being traveled. As discussed later, this separation would have to be less than about 20 meters for the problem to occur. This situation is not likely to arise frequently; but in limited cases, it could result in an incorrect user charge being levied. The worst case would be that the low standard roads nearby a high standard road (which ordinarily will have a low user charge) would have to be assigned the same user charge rate as that road.

**Assessment**

To apply the new approach for the purpose of revenue collection using data polygons, current levels of GPS and GIS accuracy will suffice. If different road classifications within a given jurisdiction are to have varying per-mile user charge rates, completeness of GIS databases may be an issue. In some jurisdictions, part of the road system is yet to be geocoded (included in GIS road data files); so at least for the time being, it will not always be possible to identify the road on which a vehicle was operating. In such cases, the on-board computer could be programmed to assign a default per-mile user charge, probably equal to the charge on the highest road standard (lowest per-mile charge) to ensure that an overcharge does not occur. We should note, however, that rapid progress is being made by private data vendors that are developing GIS road files for such commercial applications as on-board navigation systems.

The larger question relates to system reliability. To accurately record the number of miles traveled within a given jurisdiction, including when the GPS receiver is not able to acquire a reliable signal from earth-orbiting satellites, it is necessary to provide the on-board computer with back-up data, from an alternative source, on distance traveled. Loss of signals from a number of satellites that would degrade the receiver's ability to position a vehicle can result from several causes:

- rugged topography, such that the line of sight from satellites to the GPS receiver is blocked;
- "urban canyons"—city streets between tall buildings that interfere with signal acquisition;
- dense tree cover that shades the GPS receiver from the satellite signal;
- intentional blocking of the vehicle's GPS antenna, such as covering it with a metallic object; and
- malfunction of the vehicle's GPS receiver.

This suggests that the back-up tracking system should be completely independent of GPS and, therefore, immune to the above sources of degraded accuracy. Dead reckoning options are discussed later in this chapter.

## THE OBJECTIVE OF VARIABLE ROAD USER CHARGES

In addition to assuring an adequate stream of revenue, user charges could be used to pursue two other public policies:

- To improve fairness, such that those who impose greater costs on the road system, on other users, or on society in general pay higher user charges.
- To modify behavior, such as encouraging motorists to increase vehicle occupancy, to travel at less congested times of day, or to operate more energy-efficient or less-polluting vehicles.

Realistically, the objective of influencing the nature of road use is not likely to be implemented for a number of years after the new approach is in place. The evidence to date is that in most locales, the public has yet to become comfortable with the concept of increased user charges to manage demand for travel on public roadways. Even so, the new approach should be designed to accommodate policy initiatives because many observers believe that varying road user charges will eventually become an important public policy tool. There is little doubt that some day travel demand management is going to have to be taken seriously, given the mounting evidence that society cannot invest its way out of traffic congestion.

There are various types of policy initiatives that the new approach should be designed to accommodate. Several forms of initiatives are discussed in turn.

### Congestion Management

Congestion management can involve charging users of designated roadways higher per-mile amounts during periods of traffic congestion. This practice can be carried out at several levels of precision. At the lowest level, designated urban highways (generally freeways) could have a weekday per-mile user charge that is higher during peak hours. Motorists would be aware of the higher charge and would take it into account when making travel decisions. The user charge could be adjusted periodically to influence demand in keeping with the current and desired traffic volumes.

A more sophisticated regimen might involve adjusting user charges on a real-time basis such that the per-mile rate would vary according to current traffic volumes. Changeable message signs would inform drivers of the current per-mile rate. Presumably, these drivers would remember how road user charges vary and would take these rates into account when making travel decisions. Such a system would necessitate communication between the roadway and the vehicle to instruct the on-board computer to adjust upward by some factor the user charge being levied, given the traffic conditions at the time.

### Lane-Specific Charges

This policy initiative involves assessing different levels of user charges, depending on the traffic lane in which one is traveling. One form of varying road user charges

by lane—high-occupancy free, low-occupancy toll (HOT) lanes—already is growing in popularity. Suppose that a freeway has three lanes in each direction. One lane each way may be reserved for high-occupancy vehicles, perhaps those with three or more passengers. If other motorists, such as those traveling alone, wish to use this lane to avoid much heavier congestion in the other two lanes, they must pay a higher user charge. This higher user charge acts as a rationing mechanism so that there will not be enough vehicles using the HOT lane to induce congestion.

HOT lanes have two important advantages: First, they encourage higher-occupancy vehicles, and that enables the freeway to operate more efficiently. Second, they allow the otherwise underutilized high-occupancy lanes to be more heavily traveled by offering those who value their time sufficiently the option to enjoy a higher quality of service. Equity problems are in part avoided by providing low-income travelers the opportunity to use HOT lanes without additional charges simply by carrying several passengers.

HOT lane user charges, however, would require considerable accuracy in terms of the GPS/GIS inputs to the on-board computer, as the specific lane being used would influence the user charge. One- or two-meter accuracy would be needed to identify the lane in which a vehicle is traveling. If this level of accuracy is not feasible, it would be possible to physically separate the HOT lane so that vehicles could not enter it except at one or several designated points. At these points, the roadway and the vehicle could interact electronically to identify the lane that will be used.

**Weight/Configuration-Based User Charges**

This policy direction means that vehicles are assessed road user charges at a level consistent with the costs they impose on the road system and on other motorists. Federal and state highway cost allocation studies have shown that vehicles vary greatly in terms of the costs they create. For example, a heavy vehicle with more axles will damage the road much less than an equally heavy vehicle with fewer axles; and a heavy vehicle will damage lower standard roads (e.g., flexible pavement) much more than roads designed to accommodate higher weights (e.g., interstate highways). By varying user charges with the type of road, it would also be possible to influence operators of heavy vehicles to drive on roads that are best able to withstand their axle loads.

The new approach has great potential as a means for assessing road user charges that are consistent with the damage a given vehicle imposes on a particular standard of roadway. GIS road files could contain a code for the road classification, and the on-board computer in heavier vehicles (e.g., 26,000 pounds gross weight or more) could be configured to accept inputs from the trailer regarding current configuration (especially axles) and weight. One option is an on-board scale that could record the vehicle's weight each time the cargo doors are closed (Other provisions could be made for flat-bed trailers and different types of trailers.). The

scale would provide an accurate enough indication to enable the vehicle to be placed into a weight category for determination of the appropriate user charge.

There would be no special GPS/GIS accuracy requirements for this sort of policy initiative. It would be especially important, however, to be able to establish with certainty the classification of roadway on which a heavy vehicle is traveling. This need would be particularly great in jurisdictions where the user charges vary substantially for heavy vehicles, depending on the road classification being traveled.

**Data Needed**

The types of data needed to apply the new approach to assessing road user charges for these and other policy initiatives are generally not much more extensive than for basic revenue collection using data polygons. As we discuss below, the real issue is accuracy. The GIS road file must contain (1) the classification of the roadway (e.g., rural interstate, urban collector, residential street) and (2) the political jurisdiction within which the roadway lies. In the case of heavy vehicles, the on-board computer must be able to record the vehicle's weight on the specific trip in question. The type of on-board scale that we are envisioning is one that will measure suspension deflection when the vehicle is loaded or unloaded. When the cargo doors or other forms of closing devices are secured, the scale will send a reading to the on-board computer which will store it. Data on the vehicle's configuration also will be needed, given that road damage is much more closely related to axle weights (the pressure applied to the pavement by tires) than to a vehicle's total weight.

**Accuracy Requirements**

To be sure, the accuracy of road-use data needed for assessing lane-specific user charges would be appreciably greater than for revenue collection. Specifically, an accuracy level of one to two meters would be necessary. On the other hand, for most forms of congestion mitigation, an entire roadway would be assessed the same user charge rate, so the principal concern would be to ascertain that a vehicle was in fact traveling on that facility. A useful cross check would be the record that the vehicle had received a signal from the roadway indicating that in effect a surcharge was being added to the normal per-mile rate. The cross check would verify the presence of the vehicle on the tolled facility. A weight- and configuration-based user charge regimen also would only require that the roadway being traveled be firmly established. In the case of especially heavy vehicles (those approaching 80,000 pounds gross weight) the user charge may vary considerably among classifications of roads; so it would be vitally important to be sure which type of road was being traveled.

Regarding the necessary accuracy of the on-board scale, it probably would be wise to use a series of graduated weight classes to minimize the difference in user charges between classes. Large differences between adjacent user charges could produce inequities if the on-board scale were not sufficiently accurate to ascertain

exactly which weight-based class is appropriate in a particular instance. Oregon uses a series of rather fine-grained weight and configuration classes for its modified weight-distance taxation system, and similar classes could be applied in the case of the new approach. We envision approximately 12 classes with ranges of about 5,000 pounds gross weight. How much user charges vary by vehicle class is a choice to be made by each individual state and local political jurisdiction.

**Assessment**

From the standpoint of GPS and GIS, the most confining data and accuracy requirement of the policy initiatives possible with the new approach would be lane-specific road user charges, in which case one-meter accuracy would be necessary. For other variable user charge applications, a 20-meter accuracy level generally would be sufficient. Obviously, the greater the difference in user charge rates for two different roadways, the more important it is to be absolutely sure on which road a vehicle is traveling. For this reason, it is more likely to be technically possible to implement variable user charges for congestion management and for weight/configuration-based equity in the near term than charges that vary by lane. Lane-specific user charges probably are a number of years away, unless the facility was equipped to communicate the necessary information on current user charge rates to the vehicle. It should be noted that this communication technology is in use today.

## GPS ACCURACY CURRENTLY AVAILABLE

GPS World magazine recently published a survey of manufacturer claims regarding GPS receiver accuracy levels (*GPS World* 2001). One category includes receivers specifically designed for vehicle installation; thus, these receivers are designed to process satellite signals while in motion. As one would expect, the more expensive receivers generally have more impressive accuracy claims; but overall, the claims are in the two- to ten-meter range. Such claims should be considered with a certain amount of skepticism, however. It is widely recognized that many manufacturers boast a level of accuracy they were able to achieve only under optimal conditions.

Receivers vary in terms of their circular accuracy (more precisely, their probable circular error) under optimal as well as marginal conditions. Receiver manufacturers use any of several measures to express their claimed accuracy, the most common being the root-mean-squared (RMS) error. To establish the RMS error, one averages the squared errors of a series of fixes and then takes the square root of this average. It is worth repeating that direct comparisons of different GPS receivers are problematic. This is because different receivers perform best under different sets of conditions. It is not possible, therefore, to make a blanket statement implying that in a given situation (e.g., driving an auto across the Midwest on an interstate highway) one can anticipate a specific level of GPS accuracy.

One way to think about factors that may degrade receiver performance is to apply what is commonly referred to as the “error budget.” The term applies to the

individual and collective contributions to GPS error of several factors, which include the following sources.

**Atmospheric Conditions and Satellite Position**

From the satellite to the receiver, the GPS signal must pass through the atmosphere, specifically the ionosphere and troposphere. Atmospheric conditions, such as abnormal solar activity disrupting the ionosphere or rainstorms in the troposphere, affect the speed of the GPS signal. The change in signal speed causes the GPS receiver to calculate erroneous positions. To some extent, atmospheric errors can vary between day and night and can be magnified in the case of signals from satellites at low angles in the sky (Misra, et al. 1999, p. 69).

To reduce these errors, manufacturers of GPS receivers have implemented such methods as dual frequency receivers and differential GPS (DGPS). In brief, dual-frequency receivers process two signals, L1 and L2, that are transmitted by the satellites. Dual-frequency GPS receivers use the data and the wave characteristics of signal L1 and the wave characteristics of L2 to correct errors, thereby refining the positional accuracy obtained. DGPS receivers adjust the calculated position using correction values transmitted to them from land-based stations located on towers.

An issue that is important but not entirely understood is the effect of a vehicle's proximity to DGPS correction stations. The data currently available suggest that differentially corrected GPS fixes (positions) often are superior to uncorrected fixes within about 80 kilometers (about 50 miles) from the correction station. Lemmon et al. (2001, p. 7) report losses in DGPS accuracy of about one meter for each 150 kilometers of distance from the reference station. Possible exceptions, however, are areas near tall buildings that can deflect signals causing what is called "multipath errors." Wood and Mace (2000, p. 2) contend that DGPS may actually give worse accuracy in central business districts. It is worth noting that any multipath errors present at the correction towers will be transferred to the mobile DGPS receiver. In such a case, the DGPS receiver will then accumulate the correction station's multipath errors along with its own multipath errors (EOM 1998). At greater distances from stations (e.g., over 160 kilometers, or 100 miles), some tests have indicated very little if any improvement in accuracy. More testing of DGPS accuracy under variable conditions is needed.

Regarding satellite position, the number and location of satellites that the GPS receiver uses to calculate its location influences the accuracy of these calculations. The ideal geometry is satellites uniformly spaced across the sky, with one directly overhead. Deviation from the ideal is called "dilution of precision" (DOP). Early GPS receivers were able to use signals from a limited number of satellites, regardless of their position. Modern GPS receivers are able to select satellites with the best geometry or use all satellites that are in view to minimize the DOP effect. One aspect of the DOP effect that GPS manufacturers cannot control is the influence of latitude. Because of satellite geometry, the maximum horizontal error tends to be largest at locations with latitudes of about 40 degrees. Unfortunately,

this is the latitude of the central part of the United States, running east-west. Lesser errors are likely at northern latitudes because more satellites can be "seen."

### Severe Terrain and Multipath

The GPS receiver in a vehicle processes time-difference signals from several terrestrial satellites to compute the position of the vehicle. It follows that if the signals from optimally placed satellites are blocked or otherwise interfered with, inaccuracies will result. More technically, the receiver benefits most from the satellite signals with very different azimuths from the vehicle so that each one is able to add to the location information provided by the others. Severe topography (e.g., mountain passes) can limit a GPS receiver to signals from satellites that are almost directly overhead, a circumstance that is not conducive to good accuracy. If the terrain does not actually preclude signal reception, research by Hoffman et al. (1996, p. 4) indicates that characteristics of the terrain alone may not seriously degrade differential GPS (DGPS). An effect related to severe terrain can be found in "urban canyons," where tall buildings restrict the receipt of signals from numerous directions.

To make matters worse, signals may bounce off tall, smooth surfaces like buildings or even tree canopies, giving erroneous time-delay signals and thus inaccurate positions. These multipath errors can potentially be quite great if a receiver does not have features to mitigate them. Currently, however, there are several methods being incorporated into receivers to reduce these errors, including antenna design and signal-filtering software (EOM 1998). Misra et al. (1999, p. 70) contend that multipath errors can be reduced to as little as one meter using measurement smoothing.

### Receiver Characteristics

GPS receivers vary greatly in their capabilities; and, of course, better capabilities generally mean greater cost. Among the ways in which GPS receivers vary are:

**Dynamic limitations.** Any GPS receiver is most accurate when it is stationary. GPS receivers, however, vary considerably in terms of how much their accuracy diminishes when placed in a moving vehicle. This is known as "occupancy time." Changes in the rate of vehicle acceleration may compound the error resulting from less frequent sampling (satellite signal processing and establishing a fix).

**Capability to use differential corrections.** Differential correction of satellite signals is available in some locations. Real-time DGPS requires two antennae, one to receive the satellite signal and the other to receive correction data. Differential correction capabilities may add considerably to the cost of a GPS receiver (Bohnenstiehl 2001, p. 2). Also, the degradation of accuracy with distance from the differential correction tower, known as "spatial decorrelation," varies among receivers.

**Multipath rejection capabilities.** As noted above, several receiver manufacturers have developed techniques for estimating the magnitude of multipath errors and

compensating for them. Some tests have indicated that under certain circumstances, these errors can be reduced to the point where they become inconsequential.

**Signal processing capability.** Of the two wavelengths of signals transmitted by the satellites, the typical low-cost consumer GPS receivers use only one, called L1 (more specifically, the C/A code from L1). Beginning in 2003, a second stream of data called L2C transmitted on the second signal, L2, will become available for civilian use, although full implementation with 24 or more satellites will not occur until 2011 (see Fontana et al. 2001). Among other benefits, L2C will reduce ionospheric refraction error. Shaw et al. (2000, p. 4) estimate that receivers capable of processing both the L2C and L1 signals will have horizontal inaccuracies as low as 8.5 meters in circumstances when L1 alone would have inaccuracies of about 22.5 meters. To receive L2C as well as L1 signals, a dual-frequency GPS receiver will be required. Initially, these receivers will be more costly than conventional L1-only receivers; but their price can be expected to fall quickly. It also will be possible to configure single-frequency receivers to receive only L2C signals, which will be markedly more accurate than L1 signals.

### Combined Effects

To summarize the potential inaccuracies of a GPS receiver, in Table 3-1 we present an error budget that is based in part on that suggested by Van Dyke (2000). In the worst case—the very rare circumstance that all of the above sources of error were maximized—the total error (termed the user-equivalent range error) will be plus or minus three sigmas (that is, the error level that will not be exceeded in 99.9 percent of these worst cases), or $\pm$ 37.5 meters. Notice that the error sources are not precisely additive.

**Table 3-1. Error budget for GPS receiver inaccuracies**

| Error source | GPS one-sigma error (meters) |
|---|---|
| Atmospheric conditions and satellite position | 12.0 |
| Severe terrain and multipath | 1.2 |
| Receiver characteristics | 4.8 |
| Other | 0.5 |
| User-equivalent range error | 12.5 |

SOURCE: Derived from Van Dyke (2000, Table 3)

The main point is that it is not prudent to make highly specific, generalized statements about the current accuracy of GPS receivers. In our review of the literature, we saw numerous admonishments not to take manufacturers' accuracy claims too literally. There are many factors that influence accuracy, and the methods used to rate accuracy vary too much to make direct comparisons

especially meaningful. One message is consistent in the review articles we read: The best way to assess the accuracy of alternative receivers and of GPS generally under specific circumstances is to conduct one's own tests.

All this said, a conservative estimate of the accuracy of a quality (but not high-end survey-level) GPS receiver installed in a moving vehicle that is not operating near tall buildings or severe topography is about 15 meters. In many situations, the error will be less; but in particularly adverse conditions the error may be twice as great or more. Within a few years, however, substantial improvements in the accuracy of quite inexpensive GPS receivers are a virtual certainty.

## THE ROLE OF DEAD RECKONING

No matter how accurate GPS positioning is, there inevitably will be times when the position of a vehicle on the road system cannot be ascertained. The two primary reasons for this limitation are:

- **Lack of satellite signals**. Signals can be blocked by driving in tunnels or under dense, wet tree canopies, by intentionally covering a vehicle's GPS antenna, or by some form of system malfunction.
- **Incomplete GIS road files**. Currently, there are many roadways that have yet to be digitized for inclusion in GIS road files. These roadways include newer segments in major cities, streets in smaller communities, and lower-level rural roads. As time passes, more and more of these roadways will be accurately digitized and included in commercially available data files. This limitation is not applicable for the basic data polygon approach.

Other reasons GPS may fail include operation of a vehicle on private roads or off roads entirely and rare conditions in which the error level is too great to ascertain which roadway is being traveled.

In some of these cases, a dead reckoning (DR) system would substantially improve system performance. This system would keep track of the vehicle's movements (distance and possibly direction) between GPS fixes. A host of possible DR technologies are possible; but for mass applications associated with the new approach to assessing road user charges, the system must be low cost. In the case of revenue collection, the principal requirement of the DR system will be to provide an accurate estimate of the vehicle miles traveled. Thus, if the problem were an incomplete GIS road file, the GPS receiver could provide the on-board computer with the horizontal distance traveled over the earth's surface; and an appropriate per-mile charge could then be applied.

More complex DR requirements exist should the objective be policy initiatives that involve variable road user charges. For example, suppose that a vehicle were traveling along an arterial roadway leading into a central business district (CBD) with numerous tall buildings and even tunnels and that GPS signals were at best sporadic. If the user charge rate for the arterial happens to be different than for nearby city streets, the DR system should be capable of informing the on-board

computer that either the vehicle remains on the arterial or that it has exited it. It is worth stressing that the realistic function of a DR system is to approximate a vehicle's position between fixes, not to in any way replace GPS positioning. DR systems can encompass various types of technology. Among them are:

- odometer feeds that measure the distance traveled,
- inertial chips that sense changes in direction,
- rate gyros capable of sensing changes in direction,
- radar imaging devices that measure the distance from recognized landmarks such as the faces of certain buildings, and
- magnetic compasses that provide a heading input to the on-board computer.

A simple design would involve a feed from the vehicle's speedometer or odometer. Such a system could provide a reasonably accurate estimate of the distance traveled between reliable GPS fixes, but it could not estimate the direction of travel. More elaborate DR systems might include a basic rate gyro capable of sensing changes in the vehicle's direction of travel (a good discussion of rate gyros appears in Abbott and Powell 1999). This feature may not necessarily be costly; some sources cite cost estimates as low as $10, in large quantities. Mass-produced inertial chips very likely would cost a similar amount. Radar imaging devices would be extremely accurate, but this technology probably is a long way in the future. Magnetic compasses in vehicles tend to be quite inaccurate because of the magnetic fields they encounter. Clearly, field testing of alternative DR technologies is necessary.

Our point is that if GPS/GIS systems are to be used to provide sufficiently accurate data to measure exactly when a vehicle departs one data polygon for another or to enable more fine-grained user charges to be implemented, especially where multipath complications are likely, DR capabilities may prove to be essential. Of course, as GPS fixing capabilities improve, the need for DR systems aboard vehicles will subside; but indications are that this advancement will take time. A cost-effective DR system may well prove to be a key component of the on-board equipment used to implement the new approach.

## CONCLUSIONS

The two primary objectives of the new approach to assessing road user charges are (1) revenue collection and (2) variable road user charges. Realistically, the first objective is likely to drive the initial adoption of the new approach. At a minimum, revenue collection using the new approach requires that the roadway being traveled can be identified. We suggest that a 20-meter accuracy will be sufficient in essentially all circumstances for this objective to be pursued. Using the new approach to vary road user charges would require greater positional accuracy in some applications, particularly lane-specific charges (as in HOT lanes). In most applications involving variable user charges, however, the same accuracy level would be quite sufficient.

Can current GPS equipment and GIS road files promise 20-meter accuracy? In almost all instances, the answer is yes. It is worth noting that GPS positioning standards published by the U.S. Department of Defense (DoD 2001, p. A-35) assess the average current accuracy of single-frequency GPS at 8.3 meters 95 percent of the time. The worst sites have an accuracy of 19.7 meters. Even so, more research on GPS accuracy is needed to assess the effects of receiver performance level and environmental circumstances. Also, new technological breakthroughs are emerging that portend substantial improvements in accuracy in most if not all conditions. Regarding GIS road files, there are two limitations that need attention. One is accuracy such that the roadway coordinates reflect its true position on the earth's surface. The other is completeness: Many road segments have yet to be digitized and included in commercially available GIS road files. For now, these limitations restrict the ability of most types of variable road user charges. The limitations, however, generally will not be a problem for revenue collection, except in the case of roadways located near political boundaries. Even in these cases, the error in user charge revenue apportionment will be minuscule relative to the total revenue collected and far superior to current methods for charging road users.

For both revenue collection and variable user charge applications, an alternative system (e.g., dead reckoning) to back up most current GPS receivers will be virtually essential. Several technologies are currently available to meet this need. More research is called for to ascertain which of these technologies is the overall cost-effective solution.

In summary, technological limitations are not likely to constitute a significant barrier to implementation of the new approach to assessing road user charges. It would be prudent to consider phasing implementation, however, beginning with revenue collection as the primary objective. Then, as new technological advances reach the market place—and they most assuredly will—more demanding applications can be entertained. That said, we believe that by the time the new approach is actually needed for revenue collection due to declining motor fuel tax revenues (five to ten years), technology will have advanced to the point where variable user charge applications will be entirely feasible from the standpoint of accuracy.

**REFERENCES**

Abbott, Eric, and David Powell. 1999. "Land-Vehicle Navigation Using GPS." *Proceedings of the IEEE*, Vol. 87, No. 1 (January), pp. 145–162.

Bohnenstiehl, Kyle. 2001. "A Look at GPS." *GIS Vision*. Available at http://www.giscafe.com/GISVision

Department of Defense (DoD). 2001. *Global Positioning System Standard Positioning Service Performance Standard*. Washington, DC: U.S. Department of Defense. Available at http://www.navcen.uscg.gov/cgsic/meetings/summaryrpts/38thmeeting/default.htm

*Earth Observation Magazine* (EOM). 1998. "GPS Q & A." Vol. 7, No. 10 (October). Available at http://www.eomonline.com/Common/Archives/October%2098/gqa.htm

Fontana, Richard D., Wai Cheung, and Tom Stansell. 2001. "The Modernized L2 Civil Signal: Leaping Forward in the 21st Century." *GPS World*, Vol. 12, No. 9 (September), pp. 28–34.

*GPS World*. 2001. "GPS World Receiver Survey." Vol. 12, No. 1 (January), pp. 32–47.

Hoffman, Randy, John Lemmon, and Ron Ketchum. 1996. "Field Strength Measurements of DGPS and FAA Beacons in the 285 to 325 kHz Band." Boulder, CO, Institute for Telecommunication Sciences, National Telecommunications and Information Administration. Available at http://tfhrc.gov/its/fsm/fsm.htm

Lemmon, John J., and Ronald L. Ketchum. 2001. "Performance Parameter Tradeoff Analysis for a Nationwide Differential GPS Service." Boulder, CO, Institute for Telecommunication Sciences, National Telecommunications and Information Administration. Available at http://tfhrc.gov/its/fsm/fsm.htm

Misra, Pratap, Brian P. Burke, and Michael M. Pratt. 1999. "GPS Performance in Transportation." *Proceedings of the IEEE*, Vol. 87, No. 1 (January), pp. 65–85.

Shaw, Michael, Kanwaljit Sandhoo, and David Turner. 2000. "Modernization of the Global Positioning System." *GIS World Online*. Available at http://www.gpsworld.com/1000/1000shaw.html

Van Dyke, Karen L. 2000. "The World After Selective Availability: Benefits to GPS Integrity." Institute of Electrical and Electronic Engineers (IEEE) Position Location and Navigation Symposium (PLANS) 2000, March.

Wood, Chris, and Owen Mace. 2000. "Dead Reckoning Keeps GPS in Line: Vehicle Positioning in Urban Environments." *GIS World Online*. Available at http://www.gpsworld.com/0601/0601wood.html

# CHAPTER 4
# OPTIONAL DATA GATHERING

The new approach to assessing road user charges is designed to be as flexible as possible and thus enable individual jurisdictions to pursue the public policies they choose. In earlier chapters, we have suggested that at least initially, a simple polygon approach should be used to collect data on road use. We noted, however, that it will be feasible to distinguish types of roads within each polygon using some form of simple classification system. Such a system will enable different per-mile rates to be assessed for roads falling into different functional classifications. For example, a community may wish to increase per-mile rates in residential neighborhoods to encourage through traffic to remain on arterial roads to the fullest extent possible. This chapter looks ahead at some of the features and capabilities that could feasibly be embodied in the new approach. At the outset, we stress that these features probably should not be included in the initial implementation of the new approach; and they should never be added if the public opposes them.

Among the optional capabilities discussed in this chapter are those designed to greatly enhance transportation planning and facility management over the current state of the practice. If handled correctly, these features need not reduce the privacy of road users, even though on a sample basis more extensive data on travel patterns would be gathered and analyzed.

Benefits of improved transportation planning, especially in larger metropolitan areas, and pavement management must be weighed against the greater complexity that will be required to assure the privacy of the traveling public and to upload and process these travel data. We begin by briefly reviewing the methods currently used by transportation agencies to estimate and forecast travel between zones within cities, including the limitations inherent in these methods. As each of the key issues related to current travel demand modeling is discussed, we suggest how the new approach might contribute to improved estimation and forecasting accuracy. Finally, we suggest several ways to maximize the quality of travel data while ensuring that those who wish to have the greatest possible privacy need only provide the most basic data for accurate billing purposes.

## TRAVEL DEMAND ESTIMATION AND FORECASTING

At the very center of transportation planning is travel demand analysis. Its purpose is to (1) determine where trips within an urban area are generated and where they go and (2) forecast the number of trips between zones of the urban area several years into the future. Such forecasts enable planners to assess the adequacy of facilities now and in the years ahead; the probable effects of alternative investments and public policies (e.g., land use controls, parking, public transit services) can also be assessed.

The current approach to travel demand analysis is to use computer models that attempt to estimate and project traffic levels. These models contain a series of mathematical equations that simulate the travel choices drivers make, given the current system of roads, availability of alternate modes of travel, and location of trip-generating and -attracting activities. Parameter values in the equations are calibrated using data from observed traffic flows.

Demand models operate in a sequence of steps that are intended to simulate human travel behavior. The models take into account many factors such as household characteristics and the routes and modes available to travelers. Forecasting traffic based on these characteristics requires that a series of assumptions be made regarding the relationship between household characteristics and travel. One typical assumption, for example, is that a household with a high level of income will make more trips than a household with a lower level of income. Normally, a relationship such as this is assumed to remain constant into the future (Beimborn 1995, p. 1).

## ASSESSMENT OF THE TRAVEL DEMAND MODELING PROCESS

Forecasting future traffic levels involves a four-step process that attempts to answer questions about how people make decisions regarding travel. The four steps are: trip generation, trip distribution, mode split, and traffic assignment. Data generated by the new approach to assessing road user charges could potentially improve three of the four steps. Those three steps (trip generation, trip distribution, and traffic assignment) are discussed below in terms of the current approach used, problems with the current approach, and how the new approach to assessing user charges could address these problems.

### Step 1: Trip Generation

**Current approach.** When applying travel demand models, transportation planners use data on population, along with economic and land-use characteristics in various zones within the urban area, to estimate likely trip-making patterns. This process is referred to as trip generation. To carry out trip-generation analysis, an urban area is represented by a series of small geographic areas called traffic analysis zones (TAZs). TAZs are laid out to include relatively uniform population, employment, and land-use characteristics that produce or attract trips. The characteristics of each TAZ are used to estimate how many person trips will be made to and from it. A TAZ with primarily residential characteristics will most likely be a large trip producer, while a TAZ with a large employment center will tend to attract multiple trips.

As the travel demand process exists today, trip-generation rates are estimated using a variety of techniques, including travel surveys, census data, and trip-generation manuals. Travel surveys attempt to capture where, when, why, and how trips are made by each household along with demographic data about that household. Demographic data from the U.S. Census are used to predict trip-generation figures by making broad assumptions about the relationship between household

characteristics and the number of trips produced per household. Household income, number of drivers per household, and residents over age 16 are all characteristics that have in the past been used to predict behavior. Regression analysis is performed on the Census data to estimate the number of trips per household, and thus trip-generation rates can be derived. The Institute of Transportation Engineers has published the *Trip Generation Manual* (ITE 1997) to guide the prediction of trip-generation rates for a wide variety of land uses. The resulting trip-generation rates are refined using actual traffic counts conducted on-site for those land uses.

**Problems with current methods.** Several limitations are associated with the ways trip-generation rates currently are estimated. Typically, travel surveys are completed using a small sample of the travelers in the given study area to represent trips in the area as a whole. Travel surveys can be biased or statistically insignificant, depending on how they are administered, leading to inaccuracies and misrepresentations of actual travel behaviors. Additionally, obtaining survey samples that are unbiased and statistically significant can be expensive.

Like travel surveys, applying regression analysis to Census of Population data is a flawed process. It is not possible for demographic data to fully explain trip-making behavior, as this behavior varies from person to person, and from household to household. Any resulting trip-generation rates are gross averages, with varying accuracy. In a similar vein, trip-generation rates obtained from the *Trip Generation Manual* must be used with great caution. In fact, this manual includes a disclaimer implying that "extreme care should be exercised in using many of the supplied generation rates due to limited data creating situations that may not be indicative of particular land uses" (ITE 1997, p. iii). Furthermore, many of the actual traffic counts were conducted as many as three decades ago; and travel behavior has significantly changed in that period of time. Also, the number of observations used to estimate trip-generation rates may not always be sufficient to produce robust rates. Finally, land-use descriptions often are so generalized that the trip-generation rates for them may not be sufficiently accurate to predict rates in specific zones of a given urban area.

**Improvements with the new approach.** Data that could be collected in conjunction with the new approach to assessing road user charges would greatly simplify the accurate estimation of trip-generation rates. Data collection, a resource- and time-intensive process, would be reduced to obtaining the empirical data set for the region being modeled. Current generation methods could be abandoned in favor of using actual trip data. The new approach would provide analysts with empirical, non-estimated data on trip origins, destinations, temporal aspects (e.g., time of day, day of week, peak versus non-peak), specific routes, and chaining. Trip-generation estimates using basic demographic data, surveys, and out-of-date studies would become obsolete, as data on actual trip patterns became available. When forecasting future traffic patterns, travel demand models could use the actual numbers of trips generated by different land uses, instead of the at times rough estimates currently used.

### Step 2: Trip Distribution

**Current approach.** Each trip has a beginning (production) and an end (attraction). To estimate in what zones trips produced in a particular zone end, a process called trip distribution is used. In other words, trip distribution is used to represent the way in which destinations are chosen. This is a rather complex process. For example, a study area with 100 TAZs would require a matrix with 10,000 possible trip combinations, as each TAZ sends trips to and attracts trips from every other TAZ.

With current procedures, trips originating in a particular zone are distributed to other zones by a conceptually simple mathematical model called a "gravity model." The gravity model distributes trips to other zones based on (1) the size of attractions in each zone (e.g., employment or retail square footage) and (2) the difficulty of traveling to these other zones (often measured by distance or travel time). In essence, the number of trips distributed to a particular zone decreases as distance or travel time increases.

**Problems with current methods.** In the real world, an individual's choice of destination is influenced by spatial (distance), temporal (time of day), and personal factors (demographics, constraints, and preferences). As noted above, the trip distribution process relies upon a mathematical representation to estimate where a trip beginning in a given zone will end. Kitamura, et al. (1998, p. 76) point out that as currently applied, these gravity models are somewhat flawed. Significant destination choice factors such as (1) the effects of the time of day a trip is made, (2) the association between the destination choice and the duration of the activity at that destination, and (3) the importance of the trip (e.g., a person will travel farther to consult a health specialist than to purchase routine goods) are not fully considered. Social, economic, and cultural factors are rarely included as variables in gravity models to enhance their ability to represent travel between zones. For example, some persons may avoid certain zones based on perceptions of crime rates and lack of personal safety, even though the travel time or distance to those zones may be relatively small.

**Improvements with the new approach.** Empirical trip origin and destination data would be available to travel demand analysts, making the current process of estimating how many trips departing a given zone are allocated to each other zone obsolete. Analysts would no longer have to use mathematical models to represent how travelers currently make choices, as the actual choices would be evident from the empirical data. Impedance factors (travel costs) could be estimated with great accuracy; these factors would be useful in assessing the impacts of future transportation investment and land use decisions. As an added benefit to planners, social, economic, and cultural characteristics of originating TAZs could be compared with actual origin-destination matrices to provide insights into the patterns of neighborhood interactions.

### Step 3: Traffic Assignment

**Current approach.** After transportation analysts estimate the percentage of trips likely to be taken by automobile or transit, specific routes for those trips through the existing transportation network from origin to destination are estimated using a process called traffic assignment. Traffic assignment is the most time-consuming and data-intensive aspect of travel demand modeling, and it is done differently for automobile and transit trips. For automobile trips, complex algorithms generally are used to calculate shortest travel-time paths from origins to destinations; each trip is then assigned to the shortest network path. The assigned trip volume for each network link is then compared to the link's specified capacity to see if it is congested (typically defined by the volume-to-capacity ratio). If it is found that a link is congested and more trips still need to be assigned, traffic on the network is reassigned to the next shortest travel path. This process may be repeated several times until an equilibrium between travel demand and supply exists, meaning that trips on congested links will be shifted to those that are not yet congested. The iterative process continues until the overall travel time for all trips occurring simultaneously is minimized.

Equilibrium traffic assignments on the transportation network give an idea of the amount of travel (and thus congestion) that can be expected on each link at an established future date (based on forecast trip volumes). Levels of congestion, estimated travel times, travel speeds, and vehicle miles of travel (VMT) are important standard data outputs of this phase of the demand modeling process. With these data, the effects of new or upgraded roads and transit services could be tested by simply adding them to the established network and re-running the model.

**Problems with current methods.** Hasan and Al-Gadhi (1998, p. 127) point out that in most applications, trip assignment models are based exclusively on travel times. A strong and not entirely realistic assumption of these models is that travelers know which routes will minimize their times en route, given prevailing traffic levels. Also, trip assignment models do not consider other qualitative characteristics that may influence a person's route choice. Qualitative characteristics are not easily measured, but they play a significant role in route choice. One such characteristic is route aesthetics: the physical attractiveness of a given route due to landscaping or natural beauty. Many persons may also consider the physical condition of the road facility when selecting a route.

Traffic assignment models have other limitations, as well. When estimating travel times through the network, assignment procedures often ignore signal and intersection delays. Recent research suggests that intersection delays impact overall network travel times far more significantly than do average road link speeds (U.S. DOT 1994, Section 2.2.3). While ignoring intersection delays may not constitute much of a problem in the case of limited access facilities such as freeways, this omission can pose a more substantial difficulty when highways and major arterials with signalized intersections are considered. This may lead to over-assignment on some links where significant intersection delays are experienced.

Network traffic assignments are usually forecast for the peak hour on a typical weekday to test overall system capacity. Forecasting traffic for one hour out of a day does not yield much information about traffic flows during the other 23 hours. Questions about the accuracy of this practice may arise when considering that peak congestion periods may be spread over several hours. Also, a "typical weekday" is not sufficiently defined; traffic flows on certain days at different times of the year may be less or greater than how a traffic assignment model defines a typical weekday.

**Improvements with the new approach.** Data generated by the new approach to assessing road user charges could provide the actual route choices people make when traveling from their origin zone to their destination zone. Trip assignment models using only travel times as the basis for route assignment would become unnecessary, as the influences of all time-based, qualitative, and roadway physical condition factors would already be captured by these empirical travel route data. Likewise, traffic assignment using simplified networks would no longer be necessary. Actual travel route data would provide information about the number of trips on every network link, not just main commuting routes. The most important point is that complex assignment algorithms used to replicate route choice would no longer be necessary, reducing calculations to a bare minimum.

## IMPROVING OTHER TRANSPORTATION ANALYSES

Empirical data obtained from the alternative approach to assessing road user charges will have the ability to greatly improve other transportation-related analyses. Analyses that could benefit from improved travel data include transportation system management (specifically, pavement management), capital improvement programming, and signal timing. These types of analyses are briefly discussed in turn.

### Transportation System Management and Capital Improvement Programming

Transportation system management, specifically including pavement management, could be greatly improved with the aid of detailed empirical data collected from the new approach. Data describing exact volumes by vehicle class on individual links in the road network during specific time intervals (e.g., peak periods, a particular day of the week, a month, or a year) would be invaluable to pavement-related analyses. These data could be used to assess the extent of wear and tear on roadway surfaces over time. Engineers developing capital improvement programs could then schedule repair or resurfacing projects and facility upgrades based on actual volumes and would not have to rely upon far less accurate data.

Empirical data on the actual vehicle mix of traffic on specific road segments could substantially enhance the capital improvement planning process. Automobiles, light trucks, and heavy trucks all damage pavement at different rates and in different ways; and the relative effects of these vehicle types in turn vary with the standard of road on which travel is occurring. According to Forkenbrock (1998), the heaviest allowable semi-tractor-trailers on average damage pavements 5.42 times more than

automobiles. Knowing the vehicle mix and the associated damage each category of vehicle inflicts upon various types of roads could enhance capital improvement programming to the point that each vehicle, and the amount of damage it causes, could be accounted for.

### Signal Timing

Traffic engineers would also greatly benefit from detailed traffic volume data. Engineers responsible for intersection performance and signal timing would have access to highly accurate traffic flow and volume data available for optimal signal timing. Empirical traffic volume data would also have a temporal aspect, allowing engineers to program different signal cycle lengths for different periods of the day, including extended cycle lengths and green phases for directional peak volumes.

## TRAVEL DATA COLLECTION FEASIBILITY

The current social climate places a rather high value on individual privacy when it comes to personal finances, health, activities, and various other aspects of daily life. While impressive technological advances in data collection and transactional security have been occurring, it is not yet possible to absolutely guarantee the security of travel data and therefore the privacy of motorists. Thus, while relatively detailed data on travel patterns would be of great value for transportation planning and system management, privacy and security concerns are a very important consideration.

### Three Different Objectives in Data Collection

In simple terms, there are three separate objectives that could be pursued when using the new approach to assessing road user charges to collect travel data:

- Most important is the central objective of providing a general basis for charging motorists for their use of roadways in a fair, reliable manner.
- Also important, but much less central as an objective, is varying user charges by factors such as the time of day when a trip occurs.
- A lesser objective is gathering travel data to facilitate the improved technical analyses discussed in this chapter.

While certainly valuable, variable road user charges and the facilitation of improved transportation planning and pavement management should be pursued only if it were clear that doing so would not jeopardize the primary objective, that of assessing general road user charges. The question thus emerges, “Can the data that would support variable user charges and improved technical analyses be gathered without causing serious concerns on the part of the traveling public?”

To explore this question, it is useful to distinguish the additional data necessary for technical analyses from the more basic data needed to charge motorists for use of the roads on which they travel.

### Assessing Basic Road User Charges

For the central purpose of assessing road user charges, the following data need to be acquired by the vehicle:

**Miles traveled by jurisdiction.** Because user charges may be assessed by the federal, state, and local (counties and municipalities) levels of government, miles traveled need to be measured for each level. Thus, the data need to indicate that a certain number of miles were traveled in Minneapolis, Hennepin County, the State of Minnesota, and the United States. These data need not be stored in the on-board computer but only used for computing user charges due.

**User charge rates.** Per-mile road user charge rates for each jurisdiction need to be stored in the on-board computer. These rates are applied to the miles traveled in the respective jurisdictions. As we discuss in Chapter 6, the charges are aggregated into a single figure that is uploaded to the collection center. A subsequent encrypted anonymous message from the vehicle to the center specifies how the total user charge should be apportioned to the jurisdictions in which travel has occurred.

**Type of road.** If a particular jurisdiction chooses to vary user charges by the functional classification of road segments, this classification must be contained in the GIS road file. Five or six such classifications would generally be appropriate, ranging from an interstate highway to an unpaved county road. Per-mile user charges could then vary by both road classification and vehicle characteristics.

**Vehicle identification.** The vehicle traveling on the road system must be identified to facilitate billing. At the time of registration, the vehicle's description will be recorded and provided to the collection center; the owner and his or her billing address also will be established. (Data uploading and billing options are addressed in Chapter 6.) In the case of heavy vehicles, the option should exist for data on the configuration (e.g., number of axles) and actual weight on each mile traveled (using an on-board scale that records the weight when the cargo doors or filling hatch are closed).

It is worth noting that these rather basic data are not very invasive and therefore will not constitute an affront to one's privacy. The data will not need to include time of day, date of travel, or the specific road on which the travel has occurred. This very basic data configuration, of course, will not enable variable road user charges to occur other than by vehicle weight and road classification.

### Variable Road User Charges

To institute user charges that vary with the time of day, some loss in privacy almost certainly would be necessary. Least intrusive would be a road-to-vehicle signal on roadways where a different per-mile user charge is to be assessed. This signal could be recorded for interpretation by the collection center. The signal could, for example, indicate that the per-mile user charge on a particular roadway was being

increased by 150 percent. A changeable road sign could alert travelers that the normal per-mile charge was being elevated. In its simplest form, this approach to varying user charges would not require that the exact roadway traveled or the precise time when this travel occurred be recorded. Of course, a traveler's ability to dispute a bill would be inhibited by the generality of the road-use data that would be available.

### Acquiring Data to Support Technical Analyses

For the third objective to be attained, that of gathering sufficient data to enable improved travel demand analyses and pavement management to occur, the data collected would need to be considerably more detailed. In addition to the basic data, these more detailed data would normally include:

**Origin and destination.** Trip data would include the TAZ where the trip began and the TAZ where it ended (i.e., the vehicle's engine was shut off). Chained trips could be recorded using a specified standard for length of time the engine was shut off (e.g., if under 30 minutes, the trip might be considered part of a chained or longer trip).

**Travel and time.** Time and route data would include the specific road segments on which the travel occurred, as well as the date and time of day.

As observed earlier, the central issue is whether the traveling public would accept the collection of more detailed data than those required to achieve the primary objective of assessing per-mile road user charges. There is little doubt that the pervasive and increasing problems of congestion require new and innovative public policy solutions, such as variable road user charges. Also apparent is the need to substantially upgrade analysts' capacity to accurately represent actual travel patterns and use profiles of existing road segments. How much detail to collect and how to collect it are critically important issues. Setting aside for the moment the issue of variable road user charges, we explore a possible means for gathering more detailed road-use data to support technical analyses.

### An Opt-in, Opt-out Option

A potentially effective way to help address questions about privacy and travel data collection is to give users the choice of opting-in to the collection program. Users could be given a choice of whether or not to have more detailed data collected than the data for assessing user charges, specifically data about their travel patterns. This "opt-in, opt-out" approach could take one of several forms:

- The decision to have data collected could be made by a user simply toggling an "on/off" switch on the vehicle's instrument panel. If the motorist were to want greater privacy on a particular trip or during a certain period of time, that preference could be accommodated. A potential difficulty with such an approach is that at a later time the motorist may not bother to reactivate the mechanism to record more detailed data.

- A more permanent approach might involve giving participating users discounts on vehicle registration fees in return for full in-motion travel data collection. An advantage of opting in is that more complete records of vehicle road use could be made available to vehicle owners. The governing jurisdiction (i.e., the jurisdiction overseeing data collection, typically the state department of transportation) could provide vehicle owners who opt in with a legally-binding document that promises them that (1) the data so collected will not be used for law enforcement or civil litigation and (2) these data will be accessible by the public only in an aggregate form (not specific to the individual vehicle).

An opt-in, opt-out program could be successful if enough persons opted to allow their travel data to be collected to provide meaningful origin-destination and segment-specific data. If even of 10 percent of motorists chose to participate in the program, origin and destination data sample sizes would be more than large enough to keep sampling errors to a minimum. As a practical matter, in the unlikely circumstance that all motorists opted in, it is extremely doubtful that any agency would have sufficient computing power to analyze the literally billions of trips taken weekly in many metropolitan areas. Thus, in terms of the number of observations, a strong argument can be made for an opt-in, opt-out program.

It is possible, but not very likely, that even with large sample sizes, some biases regarding travel patterns could emerge in the data. For these biases to occur, the trip-making behavior of those opting in would have to be substantially different in one or several ways from that of those opting out. It is unlikely that the demographics, economic circumstances, or travel preferences of the two groups would be so diametrically opposed that serious biases would result. Even if some biases did occur, the origin-destination and segment data would be a great improvement over input data currently used in travel demand modeling and pavement management.

It is worth stressing that by applying the encryption technology discussed in Chapter 6, it may be technologically feasible to upload trip origin-destination data anonymously. In other words, it may be possible to completely protect the identity of the vehicles whose trip data were aggregated into data files used to examine travel patterns within a metropolitan area. This suggests that the major barrier to collecting anonymous travel data is likely to be perceptions of privacy invasion rather than actual fact.

## CONCLUSIONS

As more of the nation's urban roads become congested and road expansions become more difficult to carry out, the roles of transportation planning and system preservation are becoming increasingly vital. Travel demand models are among the most important tools for transportation planning because they help analysts understand where travelers begin and end their trips. Current models have many serious limitations, including the quality of travel data that are fed into these models. The new approach to assessing road user charges has the potential to provide origin-destination data that are dramatically better than those currently used

in travel demand modeling. Additionally, the limitations inherent in the models themselves could be entirely avoided using the new approach. Likewise, it would be technically feasible to develop use profiles for specific road segments, enabling a vastly superior level of pavement management. Perhaps the most important benefit for motorists who allow data collection on their travel patterns would be the higher performance of the road system that good planning helps provide.

The objective of greatly improving transportation analyses must be balanced against the privacy concerns of the motoring public. To address those privacy concerns, decisions must be made as to the types of data that would be collected and the level of detail. The simplest form of data collection is uploading only the information necessary for assessing basic road user charges. These basic road-use data would have virtually no potential impact on privacy, but would also do little to improve transportation analyses. A system that collects only the necessary billing information from all motorists but allows those wishing to do so to opt-in to the travel data collection system in return for minor reductions in user fees may provide enough detailed travel data to greatly improve analyses while protecting the privacy of both those who choose to opt-in and those who do not. We stress, however, that only user charge data should be collected in the initial implementation of the new approach.

**REFERENCES**


Beimborn, Edward A. 1995. *A Transportation Modeling Primer*. Milwaukee, WI: University of Wisconsin-Milwaukee, Center for Urban Transportation Studies. Available at the following web site: http://www.uwm.edu/Dept/CUTS/primer.htm

Forkenbrock, David J. 1998. *External Costs of Truck and Rail Freight Transportation*. Iowa City, IA: University of Iowa, Public Policy Center.

Hasan, Mohamed K. and Saad A.H. Al-Gadahi. 1998. "Application of Simultaneous and Sequential Transportation Network Equilibrium Models to Riyadh, Saudi Arabia." *Transportation Research Record 1645*, pp. 127–132.

Institute of Transportation Engineers (ITE). 1997. *Trip Generation*, 6th Edition. Washington, DC: Institute of Transportation Engineers.

Kitamura, Ryuichi, Cynthia Chen, and Ravi Narayanan. 1998. "Traveler Destination Choice Behavior: Effects of Time of Day, Activity Duration, and Home Location." *Transportation Research Record 1645*, pp. 76–81.

United States Department of Transportation (U.S. DOT). 1994. *New Approaches to Travel Forecasting Models: A Synthesis of Four Research Proposals*. Travel Model Improvement Program Report, Washington DC: U.S. Department of Transportation.

# CHAPTER 5
# SYSTEM ROBUSTNESS, SECURITY, AND PROTECTION

For the new approach to be a viable method for assessing road user charges, it must be highly reliable, incapable of being "spoofed" (fed erroneous information regarding road use by the vehicle), and protective of the vehicle owner's privacy. In this chapter, we provide a summary of robustness, security, and protection issues that must be addressed in the design and operation of the new approach to assessing road user charges (see Appendix C for a more technical discussion). For the purposes of this discussion, the following definitions of these terms apply:

**Robustness.** Ability of a system to carry out its intended functions reliably and in accordance with system specifications under all reasonably anticipated conditions and circumstances.

**Security.** System immunity to various forms of malicious and non-malicious attempts to subvert correct and intended operation of the road user charge system.

**Protection.** Ability of a system to preserve the privacy of sensitive or personal data and assure that these data are accessible only by authorized parties for appropriate uses.

The central issues and considerations for each of these three areas are discussed separately below. The intent is to assess risks and identify critical issues and tradeoffs that must be resolved in the architectural specification, design, implementation, and operation of the new approach to assessing road user charges. Where appropriate, specific approaches and mechanisms are proposed. We stress, however, that any specific recommendations at this point should be considered preliminary and subject to careful review, analysis, and prototyping before being incorporated into a final system design concept.

## SYSTEM ROBUSTNESS

To be successful, the new approach to assessing road user charges must be implemented in a manner that ensures data are collected, stored, and reported in an accurate and highly reliable fashion. This implies that all components and systems on board the vehicle, as well as the mechanisms for reporting road use to the collection center, must function dependably and accurately under a wide range of environmental and operational conditions. Four important aspects of overall system robustness are:

- hardware reliability of in-vehicle system component,
- software and system integration reliability,
- GPS/GIS reliability and accuracy, and
- reliability of data uploading from the vehicle to the collection center.

We discuss each of these aspects separately in turn.

### Hardware Reliability

The primary hardware components include the on-board computer system, smart card interface, GPS/GIS subsystem, and interface(s) with the vehicle electrical bus(es) or other sources of relevant data on the vehicle's state. Fortunately, all of these components represent reasonably mature technologies that are already in widespread commercial use for in-vehicle applications. A number of vendors presently market various forms of Automatic Vehicle Location (AVL) systems that integrate GPS, on-board computers, communications systems (typically they are wireless), and interfaces to vehicle buses. The majority of these systems (e.g., TripMaster, QualComm, GeoNav, WebTech, Motient, Trimble Navigation, and Xata) are aimed at the commercial trucking industry and some are quite sophisticated. Features of these systems include automated department of transportation (DOT) log maintenance and real-time monitoring and/or control of vehicle parameters. The AVL market for commercial trucking is expected to exceed $1 billion per year by 2004 (Strategis 2000).

AVL and associated technologies are also becoming widespread in the passenger vehicle arena. General Motors' OnStar system, which integrates GPS, monitoring and control of vehicle parameters, and a cellular wireless communications link, currently has over 100,000 subscribers. Ford's competing Wingcast system is currently coming on line.

Temperature- and vibration-hardened on-board computers, wireless transceivers, GPS systems, and bus interfaces for in-vehicle applications are readily available; and a highly competitive industry is actively tracking and incorporating technological advances.

A large body of associated AVL system engineering experience and expertise also exists in the commercial sector and could easily be tapped for development of the new approach to assessing road user charges. While none of the current AVL systems embodies all of the properties needed for the new approach to assessing road user charges, they provide ample evidence that integrating sufficiently robust in-vehicle hardware will not be a major risk factor.

### Software and System Integration Reliability

In any widely fielded hardware/software system, the correctness and robustness of embedded software should be considered a major risk factor. For even modest systems, embedded software can be extremely complex; subtle errors, oversights, or inconsistencies in the design and implementation of this software can lead to major problems that compromise system functionality and result in large downstream maintenance costs. Even at early prototyping and design stages, inadequately engineered software, or insufficient attention to system integration, can result in large project delays and erosion of customer confidence. It is therefore important that software development for the new approach to assessing road user

charges employ the best software engineering practices, including a well-defined development process that incorporates requirements engineering, rigorous testing and other active quality assurance measures, and configuration management (Sommerville 2001). Our perspective is that extensive prototyping should be used to evaluate and validate design concepts at the earliest possible stage before they become codified in the final system design.

### GPS/GIS Reliability and Accuracy

The use of GPS data and an associated GIS database to accurately determine a vehicle's location on a given road segment is clearly of central importance to the automated road usage charge concept. The two major robustness issues for the GPS/GIS subsystem are accuracy (not generally a problem, see Chapter 3) and the ability to deal with a transient loss of GPS signal. Any GPS system will be subject to temporary loss of GPS signal due to physical obstructions, atmospheric conditions, or other periodic conditions. It is therefore necessary that the new approach include mechanisms to compensate for this loss.

To provide back-up information, various types of software-based schemes, such as dead reckoning and motion prediction algorithms could be used. Dead reckoning algorithms typically extrapolate an expected vehicle motion path from past motion history. If necessary, they can also employ a predictive vehicle motion model that utilizes control signals derived from on-vehicle sensors (e.g., accelerations, velocity, and steering angles), although this would be quite difficult to implement for the new approach because the predictive model must be vehicle-specific. Various dead reckoning algorithms have been developed and used extensively in various applications ranging from the U.S. Department of Defense's Distributed Interactive Simulation (DIS) program (IEEE 1993) to video games (Caldwell 2000). However, even sophisticated prediction algorithms can only accurately track vehicle trajectory for short periods of time without recalibration to a known location.

For short losses of GPS signal, relatively simple interpolation and extrapolation schemes will probably suffice because the cost (in terms of assessed road use charge) of inaccurately placing the vehicle for a brief time interval would be negligible in most cases. Only if the vehicle were operating near the edge of a data polygon would there even be an issue. For longer losses of GPS signal (e.g., a vehicle operating in an "urban canyon" environment, or in the event of GPS system failure) some alternative form of approximating vehicle movement will be needed. The simplest alternative is an independent odometer that is sampled and maintained by the on-board system. Coupled with the knowledge of the vehicle location at the onset and end of GPS signal loss, data generated by the odometer may permit a sufficiently accurate approximation of the vehicle's location during the signal loss period to permit appropriate user charge allocation. To provide more accurate directional tracking, a relatively basic inertial chip or simple rate gyro may prove valuable although slightly more costly. Extensive prototyping and experimentation will be needed to determine the best solutions for the new approach to assessing road user charges.

Extended GPS subsystem malfunctions (i.e., on the order of weeks or months) could be detected from uploaded vehicle data (e.g., discrepancies between the GPS-based road user charges and the odometer reading), and vehicle owners would be notified to undertake needed repairs. Escalating charge schedules could be used to motivate owners to effect these repairs in a timely manner. This would also be an effective means of dealing with deliberate disablement of the GPS receiver as discussed below under the security heading.

**Data Upload Reliability**

In Chapter 6, we suggest a highly secure and reliable system for uploading data on road user charges from a vehicle to the collection center. At the core of the communications link is smart-card technology. A smart card can enable road user charges that are stored in the on-board computer to be uploaded to the collection center. Fortunately, smart cards are well tested in commercial applications and are very inexpensive. In essence, the smart card resides in the vehicle, and the on-board computer constantly transfers road-use data to it. The vehicle operator removes the smart card and takes it to a reader in a convenience store or service station. The reader, which resembles a credit/debit card reader, is linked to the collection center; and data transfer occurs. Just as credit/debit card data transfer mechanisms are extremely reliable so also will be the data transfer system envisioned for the new approach.

There are numerous advantages to a direct transfer using smart-card technology over wireless data transfer, which is the logical alternative. A brief discussion of wireless communication technology provides insight as to the limitations of the wireless alternative. The range of technology options for the wireless transfer of data from the vehicle to the collection center include: direct link (RF or infrared), wireless local area network (WLAN), cellular link (analog or digital), wireless wide-area network (WWAN), and satellite relay. Each of these approaches currently is in commercial use for AVL-type applications.

There are two primary reliability issues related to wireless data transfer: (1) ubiquitous availability of service and (2) communication of vehicle data without loss, corruption, or duplication. The first issue relates to the need for a vehicle to come within range of a wireless service access point at sufficiently frequent intervals to upload data prior to overflowing on-board data storage capacity or incurring unduly long update times. Of the wireless technologies listed above, only satellite relay could be considered truly ubiquitous at this juncture. Currently available low-earth orbit satellite service is relatively expensive, however; and it provides low up-link data transfer bandwidth. Analog cellular service is very widespread but still has significant gaps in coverage in some areas. The vast majority of vehicles would likely come within range of analog service on a daily basis. On the other hand, vehicles driven primarily in remote areas might remain out of range for considerable periods of time. Both digital cellular and WWAN technologies still have large gaps in coverage, particularly in rural areas. Point-to-point and WLAN solutions would require the establishment of access points to which vehicles would need to become proximate at sufficiently frequent intervals.

Whatever the choice of wireless communication service, the system must ensure that data are transferred reliably from the vehicle to the collection center via the provided link. Because wireless links are especially vulnerable to service degradation or interruption, the system would need to employ carefully designed transactional protocols to ensure that all data sent from the vehicle successfully reach the collection center and, equally important, that the same charges do not accidentally get assessed more than once.

In addition, wireless communication technologies suffer from a lack of standardization and are subject to relatively rapid change and technical obsolescence. Currently there are several competing commercial systems for wireless data service. During the past half-decade, two generations of cellular telephone technology have been deployed. A third generation is currently being fielded, and a fourth generation is under development. This rapid evolution would be difficult to track in a road user charge collection system that might be phased in over a timeframe of a decade or longer.

Given these significant limitations, we conclude that direct-transfer smart-card technology is a superior choice for communications between a vehicle and the collection center. As noted earlier, the smart-card based data transfer system is discussed in detail in Chapter 6.

**SECURITY**

The new approach to assessing road user charges will undoubtedly be subject to various attacks upon its integrity and must be explicitly designed to successfully resist such threats. Likely security threats include individual attempts to avoid assessment of charges, the typical range of Internet hacking activities, and coordinated efforts to compromise or disrupt system operation. Some modes of attack are likely to be quite sophisticated. At a minimum, the following specific threats are possible:

- disabling the on-board system or data communications link,
- blocking GPS signal acquisition,
- overriding of true GPS signals by false signals,
- overriding data communications to report falsified vehicle data,
- uploading false data reports for other real or fictitious vehicles,
- coordinated “denial of service” attacks on system access points and/or collection authorities, and
- various forms of hacking directed at the collection center.

System disablement would result in a complete absence of reported vehicle data. This could be detected at the collection center by noting the failure of a vehicle to report data for a long period of time. Of course, such a procedure would result in some false alarms because there are legitimate reasons why vehicles are not driven

for extended time periods. The owners of vehicles failing to upload road-use data for an extended time period could be sent advisories to have their system checked for possible malfunctions. These advisories would also serve notice to parties who had deliberately disabled their systems that the collection center was aware that the vehicles in question were not transmitting road-use data.

Manual odometer checks could be done at periodic intervals such as the time of vehicle license renewal or sale (or mandated in the case of suspected fraud) and reported to the collection center. If the odometer reading is not consistent with reported vehicle data, an accidental or deliberately induced malfunction of the system could be identified and appropriate remedial actions could be initiated.

Blockage of GPS signal acquisition or use of a false GPS signal source should be detectable both by the on-board system and at the collection center via discrepancies between GPS readings and odometer data. This could trigger a system malfunction indication in the vehicle and a generation of malfunction notice from the collection center advising the user to undertake system repair. If the independent odometer is sufficiently secure, it would be very difficult to mount an attack that would subvert both the GPS signal and the odometer reading in a sufficiently coordinated way to escape detection.

A particularly sophisticated attack might couple system disablement with installation of an alternative system that reports false vehicle data to the collection center. With sufficient integration, such a system could couple its false reports with the vehicle odometer to avoid detection. For example, a system might report the proper number of miles but attribute these miles to lower cost roads than actually traveled. Security against this form of attack requires an embedded security key within the on-board computer that can be used to authenticate data sent from the on-board computer to the collection center. This is best accomplished using an asymmetric (public/private key) encryption algorithm such as the Rivest, Shamir, and Adleman (RSA) algorithm (Stinson 1995) and a digital signature technique (Stinson 1995; Stallings 1999). The approach would work as follows: Each manufactured on-board computer would be programmed with a unique private encryption key. An associated public decryption key would be provided for the on-board computer and this key would be registered with the collection center as part of the vehicle record. The on-board computer would digitally sign all data transmissions by sending both an encrypted and plain-text (unencrypted) version of the data. The collection center would decrypt the encrypted version of the data using the appropriate public key and compare it to the plain text version. If they match, the collection center can be assured that the message is authentic and has not been altered after leaving the vehicle.

The digital signature technique just described would also thwart attempts to submit erroneous reports for other vehicles. Without knowledge of a vehicle's embedded private encryption key, it would be essentially impossible to electronically sign messages to the satisfaction of the collection center. This security measure is discussed more fully in Chapter 6.

The final two threats listed above, denial of service attacks and general hacking, are unfortunate aspects of everyday life on the Internet. As such they are best dealt with by adhering to the standard best practices that are used in large-scale commercial Internet sites and information technology enterprises, including firewalls, proxy servers, and intrusion detection mechanisms. There are many capable experts in this domain.

**PROTECTION**

Given the sensitive privacy issues surrounding this application, it is essential that vehicle usage data be carefully protected from unauthorized access at all times. Specifically, every reasonable step should be taken to minimize the potential for use of the system to obtain information regarding vehicle location or movement for unauthorized or unintended purposes. This protection must span three time domains: (1) while the information is stored on-board the vehicle, (2) during the uploading of the data to the collection center, and (3) while the data are stored at the collection center.

The most effective protection mechanism is to minimize the amount of sensitive data that must be stored or communicated. It is not necessary to store or report a complete history of vehicle time and location in order to compute road-use charges. There are, however, certain tradeoffs to be considered between protection and system reliability/security because reporting less specific data to the collection center reduces the center's ability to detect anomalies resulting from system malfunction or deliberate subversion.

If the GIS database contains specific cost data for different types of road segments (see Chapters 2 and 4), it is preferable to compute accrued charges on board the vehicle. In this case, only the accrued charge totals for each taxing jurisdiction will need to be stored and uploaded. Such a design will need to accommodate changes in charge rates because such changes will require updating of all on-board GIS databases. This can be accomplished by downloading rate schedules for participating jurisdictions (primarily states) periodically via the same communication link used for vehicle data upload (discussed in Chapter 6). At less frequent intervals, a new version of the GIS database will need to be installed (e.g., via a DVD disk) to reflect changes in the road system. An efficient means of integrating downloaded GIS database updates with the static, on-board database will need to be developed.

Although uploading total user charges for each jurisdiction would in itself go far in protecting user privacy, routine encryption of the uploaded data nevertheless would be prudent. Standard encryption techniques, such as those widely used in e-commerce and electronic banking applications, can be utilized for this purpose (see Chapter 6 and Appendix C for more details). Note that the digital signature of data via encryption discussed above under the Security heading does not obviate the need for the encryption discussed here. The digital signature provides authentication and validation of uploaded data, but it does not provide protection because the public key required for decryption is not closely held. Also note that

the order of application of the encryption procedures is important. Uploaded data should first be digitally signed using the on-board system's private key and then encrypted.

The protection of road-use data prior to upload (i.e., while it is stored in the non-volatile memory of the on-board computer system of the vehicle) should also be considered because the vehicle owner may be subject to legal or illicit attempts to gain access to these data. A local symmetric-key encryption scheme, using an internally generated key, should suffice here, provided that the system is carefully designed to thwart efforts to discover this key or force the system to reveal unencrypted data.

The final issue to be considered related to protection is the potential that the new approach may be used to collect additional, fairly detailed, road usage information for planning purposes, as discussed in Chapter 4. Because such information would presumably be more specific than that for assessing road user charges, the privacy implications would also be greater. Protection of such data while stored on board the vehicle and during upload can be reasonably ensured by the protection mechanisms described above for road use charge data.

Using the encryption procedures discussed in Chapter 6, road-use data can be stripped of any remnants of personal identification so that data forwarded on to planning agencies or other constituencies could be guaranteed to be anonymous. It must be noted, however, that the potential exists for the collection center to associate an identity with uploaded planning data, should the center or some entity able to co-opt it choose to do so. In addition, an entity with knowledge of the encryption key could eavesdrop on data upload transmissions and successfully decrypt the uploaded information. Because the collection center can, and should, change its key frequently, the eavesdropping entity would need to co-opt the security of the collection center on an ongoing basis in order to successfully access data uploads for any extended period of time. These relatively modest privacy threats cannot be entirely eliminated by system design alone and will require appropriate regulatory and statutory controls governing the actions of the collection center and any potential co-opting parties.

## CONCLUSIONS

None of the robustness, security, or protection issues associated with the development of the new approach to assessing road user charges appears to pose a fundamental obstacle to successful system deployment. Most of the basic hardware components needed for this application are relatively mature and have been used extensively in similar application domains, such as AVL systems. An extensive body of relevant technical and engineering expertise can be easily tapped to develop the proposed system to commercial standards. Given the potential for extremely widespread deployment, software and system integration risks should be carefully managed through best engineering practices, including early prototyping. The design of the smart-card technology to be used for uploading road-use data to the collection center will be of critical importance and should be evaluated carefully.

Regardless of the selected technology, transactional protocols will need to be developed to ensure the reliable and accurate transfer of data.

The new approach to assessing road user charges must be designed to cope with a wide range of security threats, ranging from individual attempts to subvert the system to avoid payment of charges to large-scale, coordinated attacks intended to disrupt operations of the system overall. These security threats can be effectively dealt with by incorporating the following features into the design of the system:

- Using an independent, reliable, and secure odometer signal as a validation mechanism. This odometer information will allow both the on-board computer system and the collection center to detect disablement or subversion of the GPS system as well as general system malfunctions. Digital odometer data are available on the vehicle data bus of all currently manufactured vehicles and commercial trucks.
- Providing an additional, completely separate and independent verification of the actual vehicle odometer reading to the collection center at periodic intervals such as at the time of license renewal or vehicle sale. This will allow the collection center to detect disablement of the on-board system or disablement/subversion of the data communications subsystem.
- Employing digital signatures to authenticate and validate all data uploaded from the vehicle to the collection center. This requires that each manufactured on-board computer be assigned an embedded private key with an associated public key that can be registered with the collection center as described earlier. With digital signatures, the collection center can authenticate the source of all reported data and can ensure that the reported data has not been altered or otherwise compromised.
- Checking at the collection center for lack of reporting activity by vehicles for extended time periods to identify potential cases of in-vehicle system disablement or failure.
- Employing standard best practices in the design and operation of the collection center to minimize exposure to hacking and denial-of-service attacks.

Almost any modern information system poses at least some threat to personal privacy. In the case of the telephone system, detailed records are kept of calls placed to and from a given phone. For cellular phones, additional information is recorded regarding the cells from which calls originate; and, in fact, the movement of a powered-on cellular phone can be traced through cells even when no calls are being made. Even everyday activities such as paying for purchases by credit card generate recorded time and location information. While the new approach to assessing road user charges cannot guarantee absolute protection of personal privacy, there is no need for such a system to compromise personal privacy to a greater extent than is routinely accepted in today's society. Specific steps that can be taken in the design and operation of such a system to minimize its intrusion on personal privacy include the following:

- Limiting the amount of specific time and location data that are stored and reported by a vehicle's on-board system.
- Encrypting any potentially sensitive data that are stored in the on-board system using a local, embedded encryption key that cannot be revealed by the system to any external entity.
- Encrypting all data communicated to the collection center using asymmetric encryption. In this case, the encryption should be done using the collection center's public key so that the data can be decrypted only via the collection center's closely held private key. The collection center should change its private key frequently to minimize the potential of discovery by an outside entity.
- Reporting data anonymously where possible (as described in Chapter 6).
- Employing standard best practices in the design and operation of the collection center to prevent unauthorized access to any potentially sensitive information stored there.
- Enacting appropriate regulatory and statutory controls on the collection center to minimize the potential for misuse of collected data.

System robustness, security, and protection are critical aspects of the new approach to assessing road user charges. Each of these aspects brings its own complexities and trade-offs, but there is nothing in the concept of the new approach that should preclude achieving these three important qualities.

**REFERENCES**

Caldwell, Nick. 2000. *Defeating Lag with Cubic Splines*. Available at: http://www.gamedev.net/reference/articles/article914.asp

Institute of Electrical and Electronics Engineers (IEEE). 1993. *International Standard, ANSI/IEEE Std 1278-1993, Standard for Information Technology, Protocols for Distributed Interactive Simulation*. Piscataway, NJ: IEEE Press (March).

Sommerville, Ian. 2001. *Software Engineering*, Sixth Edition. New York, NY: Addison Wesley.

Stallings, William. 1999. *Cryptography and Network Security—Principles and Practice*, Second Edition. Upper Saddle River, NJ: Prentice Hall.

Stinson, Douglas R. 1995. *Cryptography, Theory and Practice*. Boca Raton, FL: CRC Press.

Strategis Group. 2000. *AVL and Fleet Communications Marketplace*. Washington, DC.: Strategis Group Report.

# CHAPTER 6
# DATA STRUCTURE, STORAGE, AND UPLOADING

A critical element of the new approach to assessing road user charges is the communication and management of road-use data. This includes acquiring data on the vehicle miles traveled (VMT), maintaining current rate schedules for user charge calculations, computing applicable road user charges, storing the charges, uploading this information to the collection center, and error checking. For data communication and management to be carried out well, the key attributes of privacy, reliability (including robustness and redundancy), security, and user convenience must be emphasized.

In this chapter, we focus on management of road-use data on board the vehicle and on communication between the vehicle and the collection center. Building on Chapter 5, we explore how best to upload road-use data using smart-card technology or specialized infrastructure at refueling stations. To thoroughly convey the practical application of these technologies, we present a simple case analysis. In this case analysis, a hypothetical traveler uses the new approach to assessing road user charges while taking a trip through several states. As we discuss the applicable concepts and their application throughout this chapter, we illustrate them via our hypothetical traveler.

## DATA MANAGEMENT CONSIDERATIONS

We begin with a brief review of the most important considerations in acquiring, storing, and uploading road-use data. These considerations delimit the types of data that can be collected, how they can best be stored, and the appropriate mechanisms for communicating them to the collection center.

### Privacy

Because the success of the new approach to assessing road user charges will depend on public acceptance, privacy must be a major design consideration. As we discussed in Chapter 2, at least initially the system should log and report only the minimum amount of data necessary to fairly assess and apportion road user charges. For instance, while the system must store road use information according to the jurisdiction in which this use occurred so that the funds can be apportioned properly, there is no need to maintain specific information regarding routes traveled or other potentially sensitive data. Rather than submitting VMT information for each road class within a jurisdiction, privacy can be enhanced by computing charges on board the vehicle and submitting only aggregate charge data for each jurisdiction. Furthermore, only the gross charges accrued by a user must be reported in a manner that reveals the user's identity. The additional (and more sensitive) data needed for apportionment of charges to political jurisdictions can be reported anonymously.

### Convenience for Road Users

The new approach should not place an additional burden on road users. One way to enhance user convenience is to permit vehicle owners to select from a variety of payment options and to upload road use information at their convenience. Smart-card technology can provide secure and convenient payment options, which include monthly billing, threshold billing, real-time billing, and smart-card charging. As the system evolves, a direct connection between the vehicle and the refueling station probably will become feasible. This will eliminate the need for any direct user interaction. The smart-card interface discussed in this chapter could be maintained, even after a direct connection is made available, for users who prefer any of the wide variety of payment options available through its interface.

### Simplicity

The new approach must be simple and cost-effective. Due to the difficulty in maintaining a sophisticated GIS road network, the system should first use simple data polygons (see Chapter 2) which will be easy to create and maintain yet still allow road user charges to be broken into jurisdictions. Vehicle equipment also will be simple and relatively inexpensive. A small on-board computer, a GPS receiver with inertial backup capabilities, an odometer feed, a fairly basic GIS data file, and a smart-card connection interface are all that will initially be required. Both the smart card and direct connection will provide a simple, user-friendly interface.

### Security

Because virtually all road user charges ultimately may be collected through this system, security and reliability will be of paramount importance. The entire system must be highly resistant to tampering, falsification, cyber-terrorism, and other security breaches. All security measures used in the design must be well tested. All technologies must be industry proven to resist tampering and protect against attacks on the system.

Smart cards are widely used throughout the world today to store sensitive information such as fingerprints, retina scans, PIN numbers, cryptographic keys, and electronic funds. They have been widely accepted by institutions such as the Department of Defense, American Express, and Visa. The cryptography approaches used to ensure security and privacy in the on-board system have been well tested, and they are extensively used in applications ranging from commercial banking to e-commerce.

### Robustness

Even under extreme operating conditions, the new approach to assessing road user charges must be fully capable of assessing fees based on the actual number of miles traveled within a given jurisdiction. If a good GPS signal is unavailable, the system must be able to blend redundant information, including inertial navigation and the vehicle's odometer readings, to accurately process road use information. The system must be fully capable of handling urban canyon effects, as well as time-to-

first-fix errors. Cross-checks should be performed between the GPS receiver, the inertial navigation system, and the vehicle's odometer to ensure that the road user charges are accurate. The cross checking will also allow the system to detect malfunctioning components and will ensure that the system is processing data to the highest possible degree of accuracy. By frequently downloading jurisdictional per-mile charge rates from the collection center, one can be sure that the appropriate rates are applied at all times.

## OVERVIEW OF THE DATA COMMUNICATION SYSTEM

As has been discussed in earlier chapters, the new approach to assessing road user charges relies on a computer on board the vehicle. The computer receives information on VMT from a GPS receiver and the odometer. It contains a polygonal GIS database (see Chapter 2), which is used to place the vehicle within a specific political jurisdiction, typically a state. Key to the new approach is communication between the vehicle and the collection center. Smart-card technology is the means used to facilitate this communication.

### Smart-Card Technology

A smart card is a small credit card-sized plastic device that contains an internal embedded computer chip in the form of a microprocessor and/or a memory module. The technology was developed in France more than 20 years ago. Smart cards are very durable and should serve a typical user for the life of the vehicle. If the smart card is lost or destroyed, it can be easily be replaced at a small cost to the user (a typical smart card costs less than $5). Communication via a smart card is either done through a short-distance wireless communication link or through direct physical contact with gold contact plates on the surface of the card. In the new approach to assessing road user charges, a direct-contact smart card is most appropriate; it contains a microprocessor with internal memory.

Several smart-card frameworks are in widespread commercial use. These include Sun Microsystems' Java Card technology and Microsoft's SmartCard for Windows. These frameworks support mechanisms for customizing smart cards for various applications while providing protection of data and programs stored on the card and secure communication of data to and from the card. An example of this type of smart card is depicted to the right. Smart cards can have built-in encryption modules that allow them to be used for applications requiring high security. Currently, smart cards are being used to store electronic money, PIN numbers, and cryptographic keys. Some applications even use smart cards for personal identification, which depends on biometric technology such as fingerprints and retina scans.


In the new approach to assessing road user charges, a smart card can be used as an intelligent and flexible interface between a vehicle's on-board computer and the

collection center. This technology does not require specialized infrastructure at refueling stations. The importance of this becomes clear when one considers advances such as electric vehicles, which do not require conventional refueling stations, they constitute an appropriate application of this technology. In the initial phase of implementation of the new approach, vehicles could also take advantage of the smart-card approach until the refueling infrastructure adapts to support a more user-friendly, direct connection to the vehicle through its refueling point.

A rate schedule downloaded from the collection center and stored in the on-board computer enables a road user charge to be computed for each jurisdiction using the incoming VMT information. While the vehicle is in use, a smart card is connected to the vehicle's computer and is constantly updated with road user charge information. When a user wishes to upload his or her road use information, the person removes the card from the vehicle's dash panel and inserts it into an upload station. These stations will resemble a credit card reading device and will be located in numerous convenience stores and other businesses or even in a person's home. In time, refueling facilities may be equipped to allow a direct data transfer between a vehicle and the refueling apparatus.

During the uploading process, the smart card authenticates the user, uploads the total charges accrued during the reporting interval, and then anonymously uploads the road use information needed for the apportionment of these charges among jurisdictions. When the collection center identifies the user, it checks for fraudulent behavior or malfunctions. If there is a problem, the smart card is notified to prompt the user to go to a service center, and the system flags that particular vehicle. During this communication, the collection center updates the vehicle's rate schedule through the smart card if the stored schedule is not the current edition. Once the collection center anonymously receives the information on how much of the mileage occurred in which jurisdictions, the center correctly apportions the funds to the appropriate jurisdictions in which travel has occurred.

**An Illustrative Road User Case**

To provide a practical illustration of how the road-use data will be gathered, processed, stored, and uploaded to the collection center, we provide a progressive case study. In our scenario, a woman named Karina owns an fuel-cell powered auto that is equipped with the on-board system we are discussing. As our discussion progresses, we illustrate the use of the new approach in short additions to our case study. These short elaborative discussions are contained in text boxes for convenience in reading.

**Technical Description**

In the discussion that follows, we use several technical terms which are briefly defined below.

Karina has recently purchased a new fuel-cell powered passenger vehicle. It is equipped with the technology needed to support the new approach to assessing road user charges, including a smart-card interface. She is now preparing to take her first long trip, driving from Princeton, New Jersey, to Iowa City, Iowa. Karina travels 63.4 miles through New Jersey, 284.2 miles through Pennsylvania, and 77.9 miles in Ohio. She stops to purchase fuel in Ohio. The station has not yet been updated to support a direct connection between the vehicle and the refueling pump, so she uses her smart card to upload road use information to the collection center. After the refueling is completed and she pays for her fuel, she continues on her way.

**Encryption**. The conversion of data into a form called cipher text that cannot be easily understood by unauthorized entities. Encryption is generally done via some form of an encryption algorithm that employs one or more encryption keys.

**Decryption**. The process of converting encrypted data back into its original form so it can be understood. Decryption normally requires the possession of an appropriate decryption key, which is matched to the encryption key used to create the cipher text.

**Symmetric encryption**. Use of a shared (or private) key for both encryption and decryption of the information. One of the advantages of symmetric encryption is that it is very fast. The key must be held secretly by both the encrypting and decrypting parties. Inadvertent or deliberate divulgence of the key to a third party will compromise security.

**Session key**. A disposable symmetric encryption key used for efficient data encryption. Session keys have a short life cycle. In this application, they live (remain valid) on the order of a few minutes.

**Asymmetric encryption**. A cryptographic system that uses two keys, a public and a private key. The public and private keys are related in such a way that the public key can only decrypt messages encrypted using the corresponding private key, and the private key can only decrypt messages encrypted using its corresponding public key. The public key cannot decrypt a message once it has been encrypted. At that point, only the private key can be used for the decryption.

**Public key**. An encryption that can be freely distributed. Once data are encrypted with a public key, only the corresponding private key can decrypt it. A public key can decrypt data encrypted with its corresponding private key. Public keys are only used with asymmetric encryption.

**Rate schedule**. A table relating each jurisdiction (and, optionally, road classifications) to a per-mile-traveled charge. It is stored on the vehicle's on-board computer and updated via communications using the smart card.

**Handshaking**. The exchange of information between two computers. In this application, it is used to identify a user of the new approach. During the

handshaking, the system collects the information needed to identify fraudulent behavior by the user or detect a malfunctioning computer. The system also updates the rate schedule stored in the vehicle's on-board computer. Once the user has been uniquely identified, the collection center sends a symmetric encryption session key that is used to transmit sensitive data. All system users make use of this session key during its life, giving as much anonymity as possible.

**Digital signature**. An electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable and cannot be imitated by someone else.

## VEHICLE COMMUNICATION WITH THE COLLECTION CENTER

Applying the conventions discussed so far, we now turn to how smart-card technology can be applied to facilitate the transfer of information between a vehicle and the collection center. In this discussion, we provide a "big picture" general description of how this communication takes place, building on the simple case study under discussion. We illustrate how the messages from the vehicle to the collection center will be structured. We also explain the technical elements of this communication, including the encryption methods that are most appropriate to ensure that the privacy of road users is preserved.

### Communication Steps

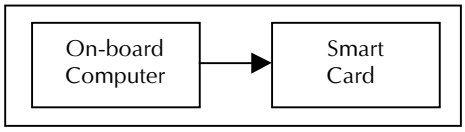
At least initially, most vehicles participating in the new approach will depend on a smart card for communication between the vehicle and the collection center. As the refueling infrastructure evolves, a direct connection interface between the vehicle and the pump is likely to become possible, allowing users to upload road use information without any direct intervention. New refueling infrastructures, such as those needed for hydrogen fuel cell technology, can be designed to support a direct connection. The following discussion is predicated on the use of a smart card.

Communication between the vehicle and the collection center occurs through a five-step process. Figure 6-1 on page 61 provides a simple overview of how the communication between a vehicle and the collection center takes place.

**Step 1. Transfer from the on-board computer to the smart card.** As a vehicle is driven, a smart card resides in a slot in the dash panel. Information from the on-board computer is continuously fed to the smart card so that the smart card always has current information. This transfer of information requires no action on the part of the vehicle operator.

**Step 2. Initial handshake.** Periodically, the vehicle operator removes the smart card and takes it to a card-reading station at a convenience store, service station, or even the user's home. The smart card is used to facilitate communication between the

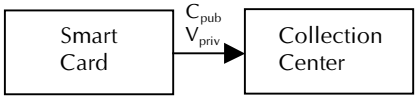
**1. Transfer from the on-board computer to the smart card**




Information from the on-board computer placed on the smart card

- Vehicle ID
- Rate schedule edition
- Total user charge due
- User charge apportionment
- Odometer reading and date

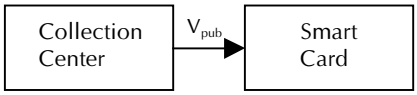
**2. Initial handshake**




Information transferred from the smart card to the collection center

- Vehicle ID
- Rate schedule edition
- Total user charge due
- Odometer reading and date

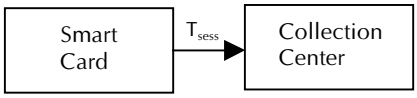
**3. Response from the collection center**




Information from the collection center to the smart card

- Confirmation of total user charge
- New rate schedule, if needed
- Discrepancy, if one exists

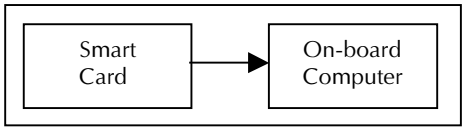
**4. Smart card communication back to the collection center**




Information from the smart card to the collection center (***anonymous message***)

- User charge apportionment among jurisdictions

**5. Smart card to the computer on board the vehicle**




Information from the smart card to the on-board computer

- Confirmation of total user charge transfer
- New rate schedule, if needed
- Discrepancy, if one exists

**Figure 6-1. Vehicle/Collection center communication**

vehicle and the collection center. Via the card reader, which resembles a credit/debit card reader, the smart card sends a message to the collection center.

The initial message is encrypted such that the collection center can identify the sender, a necessity so that the appropriate user account can be charged for the road use that has occurred. The second message, that informing the collection center as to the jurisdictions in which the road use occurred and the magnitude of the road use, is anonymous. Thus, the only information that can be positively tied to a particular road user is the total amount of charges owed. Information on how the charges should be apportioned among jurisdictions is sent anonymously so that there is no practical way to identify where the travel has taken place. The use of two messages enables the collection center to obtain all of the information it needs to (1) properly charge the road user and (2) distribute the resultant revenue among the relevant jurisdictions. The only information traceable to the particular vehicle is the odometer reading and the amount of user charges due.

The encryption protocol operates as follows: the smart card initiates communication with the collection center using a handshaking packet comprised of a short message and a digital signature. This handshaking packet is encrypted using the collection center's public key ($C_{pub}$). The digital signature is computed using the vehicle's unique private asymmetric encryption key. This private key, denoted by $V_{priv}$ in Figure 6-1, is deeply embedded in the vehicle's on-board computer system and in the smart card. For simplicity, this discussion assumes that the same embedded private key resides in the on-board computer system and the smart card. In reality, it may be logistically simpler and more secure to have the on-board computer and smart card employ distinct private keys. The approach described in this chapter could be easily adapted to accommodate this change. The embedded private key serves as the primary authentication mechanism for the vehicle. The corresponding public key ($V_{pub}$) is registered with the collection center, together with the vehicle identification number (VIN), when the vehicle is purchased. The handshaking packet serves to uniquely identify the vehicle, report total road use charges since the last upload, and prevent fraudulent activity.

In the case study under discussion, the user has uploaded data to the collection center related to travel in three states. The data uploaded from the smart card might appear in a form like that below.

*Message 1*

| |
|---|
| Vehicle ID (VIN): IJ6GZ6767PD459634 |
| Date range: 05192002,05192002 |
| Odometer: 624.1 |
| Total road user charge: $3.91 |
| Rate schedule edition: 4.2.02 |

**Step 3. Response from the collection center.** In response to Message 1, the collection center confirms to the smart card that it has received the billing information, updates the rate schedule, and sends a temporary session key for use in transmitting a subsequent anonymous message (Step 4).

In greater detail, after the collection center has verified the authenticity of the vehicle's communication, it sends the smart card (1) confirmation that it has received the amount of road user charges due, (2) a new rate schedule if needed, and (3) a new session key ($T_{sess}$), which is encrypted using the vehicle's public key ($V_{pub}$). Encryption prevents unauthorized third parties from gaining access to the session key. The smart card extracts the session key from the message using the vehicle's private key ($V_{priv}$).

**Step 4. Smart card communication back to the collection center.** Now, using this session key ($T_{sess}$), the smart card encrypts the information on the appropriate user charge apportionment and sends it to the collection center. The encryption is based on the vehicle's public key ($V_{pub}$). Thus, the apportionment data cannot be tied to the specific vehicle. (It might be possible to approximately link this data to a specific vehicle by matching the time and location of the upload to that of the corresponding non-anonymous charge data. However, this represents a relatively minor compromise of privacy. If deemed necessary, more sophisticated mechanisms could easily be employed to de-correlate these messages.)

The smart card uses this session key to send the following message:

*Message 2 (Anonymous)*

| |
|---|
| Jurisdiction: 09 (New Jersey) |
| Road use charge: $.57 |
| Jurisdiction: 12 (Pennsylvania) |
| Road use charge: $2.56 |
| Jurisdiction: 09 (Ohio) |
| Road use charge: $.78 |

**Step 5. Smart card to the computer on board the vehicle.** After the smart card is inserted back into the vehicle, the updated rate schedule is stored in the vehicle's on-board computer. Also, upon receiving confirmation from the smart card that the data on road user charges was successfully received by the collection center, the on-board computer deletes the relevant data on road use. This ensures that double billing will not occur, and enhances privacy by eliminating old road-use data from on board the vehicle.

### Distribution of Funds

All funds collected by the collection center are placed into single accounts for each participating jurisdiction. On a periodic basis, the collection center will transfer funds to the correct jurisdictions according to payments processed during the previous interval.

Karina's vehicle has traveled through three states; therefore three entries were included in the encrypted anonymous allocation message transmitted via a smart card. Next month, when the collection center apportions the road user charges, the amounts listed above will be transferred to the corresponding jurisdictions. Because Karina selected the real-time payment option, the road user charges are automatically billed to her chosen credit card. Once again, following payment verification, the road user charges were removed from the smart card, and when the card was reinserted into the vehicle, these charges were deleted from the on-board computer.

Since Karina's last road use upload, a few jurisdictions have changed their per-mile user charge rates. The collection center has compiled them into a new rate schedule. After the collection center successfully processes all the data contained in the handshaking packet, the center sends the smart card a session key and the new rate schedule. When the smart card is reinserted into Karina's vehicle, its on-board computer is updated.

## OPERATIONAL CONSIDERATIONS

### User Privacy

Due to the sensitive nature of people's travel patterns, privacy is a paramount design consideration for the new approach to assessing road user charges. The communication method just discussed ensures privacy by:

- recording and storing minimal data in the on-board computer,
- removing unneeded data as soon as it is verified that these data have been uploaded to the collection center, and
- the anonymous upload of sensitive data (jurisdictions where road use occurred).

The new approach protects the privacy of road users by keeping data requirements to a minimum. Several points underscore this important attribute. First, the data are stored as a road user charge per jurisdiction. After payment of a road user charge has been verified, the salient data are removed from the system. Second, even if an entity were to subvert system security, it would only find road user charges for the jurisdictions in which the vehicle had traveled since the last upload. Third, the uploading of road use information is done anonymously with the use of a general

session key ($T_{sess}$). Because all other vehicles use the same encryption key during the life of that key, the smart card data uploads will be anonymous. It would be virtually impossible for the collection center to determine which vehicle sent the road use information. Data needed to test for errors and fraudulent behavior are sent separately via a handshaking packet.

> The state in which Karina drives most frequently varies road user charges by the standard of road traveled. The lowest per-mile charges occur on major facilities, such as interstate highways; middle-level charges pertain to travel on arterial highways and collector streets; and the highest rate applies to residential streets and certain other roads where traffic creates problems. Because all computations are done by her on-board computer and only a dollar value is uploaded for each jurisdiction (normally a state), it is impossible to discern whether she has traveled many miles on a high standard (low per-mile cost) facility or fewer miles on a lower-standard facility to which higher per-mile charges apply. Thus, Karina's privacy is preserved.

**Security**

Once the new approach to assessing road user charges has been implemented, some attempts to defraud the system to avoid payment of road user charges must be anticipated. In order to protect against fraud, each vehicle must uniquely and reliably be identified each time it uploads its road user charges. As we discussed earlier, each registered vehicle will have an account with the collection center which is keyed by the vehicle's public encryption key ($V_{pub}$) and the VIN.

Each time a vehicle or smart card communicates with the collection center, it first creates a handshaking message. A hashing function is applied to that message to create a message hash (a shorter string of characters to facilitate encryption). Encrypting the message hash using the vehicle's private encryption key ($V_{priv}$) creates a digital signature. The vehicle's private key is deeply embedded into the hardware of the on-board computer; it would be prohibitively expensive for a user to gain access to the private key and use it to defraud the system. Even if the private key of a vehicle were compromised, this information could be used only to subvert data collection for a single vehicle. Without the private key, a user would be unable to create digital signatures and subvert system security. A handshaking packet, comprised of the original handshaking message and the attached digital signature, serves to uniquely and reliably identify a vehicle and detect fraudulent changes to the original handshaking message.

When the collection center receives a handshaking message, the vehicle's account at the collection center is accessed using the VIN. In order to validate the vehicle, the public key contained in the handshaking message is compared to the public key held by the collection center for that particular vehicle. The digital signature is

decrypted using the vehicle's public key. The resulting message hash is compared against the original handshaking message to verify that the message has not been tampered with. All data in the handshaking message are logged for future system error checking. The logged information can be used to detect duplicate or missing payments, malfunction of the on-board vehicle computer, a faulty GPS receiver, fraudulent behavior, or abnormally long gaps between road use submissions.

### GPS Inaccuracies

A small discrepancy may occur between the distance traveled as calculated by the GPS receiver and by the odometer. Under normal operating conditions, this discrepancy can be periodically reconciled. If the error becomes too large, the odometer's value will be used; and a message to have the vehicle serviced will be displayed in the instrument cluster. Of course, either a malfunctioning GPS receiver or fraudulent behavior could cause readings substantially at variance with odometer-based mileages. Servicing the vehicle will alleviate the problem in either case. In both instances, the system logs the error and notifies the collection center. If a particular user's vehicle frequently exhibits this type of erroneous behavior, an investigation may be conducted.

### Encryption

Encryption is often used to secure private data transactions from malicious entities. In the new approach to assessing road user charges, it also is used to aid in the unique identification of a user. Both asymmetric key encryption and symmetric key encryption are used in the new approach.

> The GPS receiver in Karina's vehicle has encountered a malfunction and is unable to provide the on-board computer with accurate road-use data. Two safeguards are then activated. First, the vehicle's on-board computer goes into dead-reckoning mode, whereby it uses the odometer to estimate distance traveled and an inertial navigation module to estimate any changes in direction. The on-board computer is thus able to accurately allocate miles traveled to the appropriate polygon and hence jurisdiction. Second, a prominent display advises Karina that she needs to have her vehicle checked. She does so because the display notes that she is subject to a fine if she exceeds time or distance limits with an inoperative component related to road user charges.

Symmetric key encryption is used to upload road use information to the collection center. It is faster but generally less secure than asymmetric encryption. The lack of security lies in the inability to uniquely identify which entity encrypted the message. On the other hand, this anonymity is very desirable for the transfer of sensitive road use information in the communication system. Because the key would be valuable to malicious groups that desire to disable the system, the

symmetric key must be changed often. In the case of the new approach, the symmetric key is referred to as a session key because its life is very short. Given that symmetric key encryption is many times faster then asymmetric key encryption, using symmetric key encryption for the transfer of road use information helps to ensure anonymity of sensitive data; and it reduces the computational overhead involved in the communication between the vehicle or smart card and the collection center.

As discussed previously, a handshaking protocol is used to identify a unique user of the system, and the collection center sends a session key to the vehicle or smart card for the transfer of sensitive data. A digital signature is used to uniquely identify each user of the new approach. Asymmetric encryption is used to create the digital signature. The information contained in the handshaking message (vehicle's identification number, date range of the submission, odometer reading, and the rate schedule version number) provides a means to check for fraudulent behavior or a malfunctioning computer in a vehicle. When the information in the handshaking message is received by the collection center, the center applies its error-checking capabilities for the communication system.

> Karina is walking from her vehicle to a convenience store to upload her road-use data when she slips and falls, damaging her smart card. At her convenience, she goes to the state division of motor vehicles (DMV) to obtain a replacement. The process is much like purchasing replacement license plates. Salient information is encoded onto her new smart card by the DMV. When she inserts the new smart card into her vehicle, the on-board computer again transfers the road-use data she had been trying to upload because her smart card did not carry the verification of receipt it would have from the collection center if the upload had been successfully accomplished.

In the event that a user tries to prevent a vehicle from updating its rate schedule, the attempt would be revealed by the presence of a non-current vehicle rate schedule version number. Long-term disablement of the data collection system, extended lapses in road usage uploads, and missing or duplicate data can be detected using the logged odometer readings and data ranges of submission. The odometer reading is actively monitored via the vehicle's communication bus, and it is frequently compared to the GPS readings during vehicle operation. In the event that there is a large discrepancy between the two readings, the collection center is notified through the handshaking message; and a message is displayed in the vehicle's instrument panel to have the on-board computer serviced. When there is a GPS outage, the vehicle's on-board computer uses the odometer reading for the vehicle miles traveled. If the GPS outage is persistent or overly frequent, the behavior is reported to the collection center; and a message is displayed in the vehicle to have the computer serviced. We should stress that it would be exceedingly expensive for a user to carry out an attack against the system that would go unnoticed by the collection center or the vehicle's on-board computer.

## BILLING OPTIONS

One of the most exciting features of the new approach to assessing road user charges is the wide range of payment methods it offers. When a person purchases a vehicle and registers it with the state of residence, he or she can select how to pay the road user charges that arise. Possible options include, but are not limited to, the following:

**Monthly billing.** With this option, the collection center sends the vehicle owner a billing statement each month. It resembles a telephone bill or a municipal utility bill and reflects the total user charges due. Charges for all jurisdictions can be lumped into a single figure to enhance privacy.

**Smart card "charging."** In this payment method, the user has control over his payments. The smart card holds a certain amount of credit, much like a rail transit pass in some larger U.S. cities. The credit can be purchased online with a smart-card reader-equipped personal computer or even from a form of vending machine. The vending machine would operate much like a traditional ATM and could be widely distributed. The user could even charge road use costs to the smart card when he or she purchases fuel at a service station. Road usage information will be uploaded at the time the smart card is debited.

**"Threshold" billing.** The user works with the collection center to establish a bill payment amount for road usage. When the balance of his or her account falls below a certain threshold, he or she is automatically billed this pre-set amount. There will always be a credit on the account with this type of billing. The payment is typically drawn against a credit account or checking account. This payment method is currently used by E-ZPASS in certain eastern U.S. states. The user is required to upload his or her road usage information via a personal computer, a special vending machine, or a pay-at-the-pump service station.

**Real-time billing.** This type of billing may be the most convenient for the majority of users. Through a prior arrangement, the user's smart card is tied to a credit/debit card or a checking account. The person can use the smart card to pay for fuel and road use at a pay-at-the-pump refueling facility or inside the service station, much like one would with a traditional credit card. Whenever the smart card is used, it automatically uploads the road use information; and the collection center directly bills the user's credit/debit card or checking account.

## DISPLAYING THE CURRENT ACCOUNT BALANCE

Regardless of the billing option one selects, it will be possible to display the yet-to-be-uploaded charges being stored in the on-board computer. One way to do this would be to include this information in the instrument cluster's start-up display (along with seat belt reminders, engine diagnostics, and other routine information). Such a display will keep the user aware of his or her current account balance; it also can serve as a reminder for one to upload road user charges. If the current balance includes charges that are more than a certain number of days in arrears (e.g., 30 or 45 days), a reminder to pay the road-user charge can be displayed in the vehicle. It will be feasible to charge interest and/or late fees on accounts that

are overdue. Credit card companies, and most utility companies, currently employ this practice. Any such fees could be displayed in the vehicle's start-up cycle. This display provides an incentive for users to keep their accounts current.

As noted earlier, once the on-board computer receives verification via the smart card that the collection center has received the uploaded data on road user charges, these data are deleted by the on-board computer. By deleting this information, two desirable purposes are served: (1) double billing is prevented and (2) user privacy is enhanced.

## OPERATION OF THE COLLECTION CENTER

An independent company will operate the collection center under contract with the U.S. Department of Transportation (or the U.S. Treasury). The contracted operator is responsible for:

- maintaining an account for each vehicle participating in the new approach to assessing road user charges,
- collecting and dispersing road user charges to the proper jurisdictions,
- maintaining a rate schedule of each jurisdiction's road use rates,
- ensuring that each vehicle has the proper rate schedule, and
- maintaining all hardware and software associated with the system.

### Vehicle Accounts

Each vehicle participating in the new approach to assessing road user charges has its own individual account. Within each account, a history is maintained, including rate schedules used, submission date ranges, and any abnormal behavior the vehicle has exhibited. An account is accessed using the vehicle's identification number and verified with the vehicle's public key ($V_{pub.}$). The history will allow the collection center to detect road use submission errors and check for fraudulent behavior.

An account payment method is maintained for all vehicles participating in the program. As noted earlier, when first registering a vehicle, the owner chooses a payment method. If he or she wishes to change the payment method, this can be done by contacting the collection center. The collection center is responsible for maintaining these accounts and for collecting road user payments.

All payments received by the collection center are stored in a series of accounts corresponding to the participating jurisdictions. As payments are received, they are deposited in the appropriate accounts. On a monthly basis (or a time interval set by system administrators), the collection center will disperse payment to the appropriate jurisdictions. The dispersal amounts will be set according to the previous month's road use submissions.

When jurisdictions participating in the new approach to assessing road user charges wish to update their per-mile road user charge, these jurisdictions inform the collection center, which incorporates the revised rates into its schedule. After the new revision is finalized, whenever vehicles handshake with the collection center, the new rate schedule is downloaded to them, along with the session key. Computers on board vehicles then use the new rate schedule in making their computations of road user charges due.

**Security of the Collection Center**

The collection center uses sophisticated software and hardware communication protocols to handle a wide variety of attacks against it. Because this system will collect billions of dollars a year in revenue for maintaining the United States road network, it may be an attractive target for cyber-terrorism and hacking attacks. The most likely (and most serious) attack would be a denial of service attack, which is a coordinated attempt to disrupt the operation of a computer-based (generally Internet) service, usually carried out by flooding the server with large quantities of erroneous requests or messages intended to overwhelm its capacity.

As an aid to this discussion of security, the following definitions apply:

**Cyber center.** The main branching location for the Internet backbone; there are approximately 25 across the country.

**Collocation facility.** A site which provides a connection for high-demand Internet applications; these sites are located on the Internet backbone and provide high bandwidth connections to users.

If an attack is made against the collection center, it may be very sophisticated in nature. Such threats are not unique to this application, however. Any high-profile Internet service, including e-commerce sites and governmental web sites are regularly subjected to such attacks. Because attacks on this type of system are quite common, there are well-tested preventive measures that can be taken. The collection center should use multiple data collection points located at various cyber-centers across the country. When the operator of a vehicle needs to communicate with the collection center, the communication can be done through any of these data collection points, thus providing a large measure of redundancy. Each of these points should be placed in a collocation facility and should use sophisticated firewalls to detect and thwart attacks.

If an individual or terrorist group desired to disable the system, it would have to mount a synchronous attack against each of the data collection points and successfully disable each of them. The data collection points could use multiple backbone service providers for additional robustness. Connections between the data collection points and the collection center's internal servers should also be redundant. This makes it very difficult for hackers or a terrorist organization to cut communication lines and thereby disable the system.

## CONCLUSIONS

The new approach to assessing road user charges has three principal components: (1) equipment on board the vehicle (GPS receiver and inertial-navigation module, GIS database, odometer feed, and on-board computer with a data storage capacity), (2) a collection center, and (3) communications technology to connect the vehicle and the collection center. In this chapter, we have focused on the third component, communications. When contemplating how best to facilitate communications between the vehicle and the collection center, we stress the central importance of user privacy. Other important attributes include convenience to the user, simplicity, security, and robustness.

At the core of the communications link is smart-card technology. A smart card can enable road user charges that are stored in the on-board computer to be uploaded to the collection center, while allowing updated per-mile user charge rates for multiple jurisdictions to be downloaded from the collection center to the vehicle. Fortunately, smart cards are well tested in commercial applications and are very inexpensive. In essence, the smart card resides in the vehicle, and the on-board computer constantly transfers road-use data to it. The vehicle operator removes the smart card and takes it to a reader at a convenience store or service station. The reader, which resembles a credit/debit card reader, is linked to the collection center; and data transfer occurs.

The new approach protects the privacy of road users by using the minimum amount of data possible. It is worth emphasizing that data are stored as a road user charge per jurisdiction. After payment of a road user charge has been verified, the salient data are removed from the system. Also, because data flowing in both directions are encrypted, the likelihood of tampering or other security problems is extremely remote. Tests are built into the transfer mechanisms that diagnose any form of tampering as well as mechanical problems that may occur.

Among the more appealing aspects of using smart-card technology is that it facilitates a variety of billing conventions that may be selected by the vehicle owner. These options range from having the collection center mail a monthly billing statement, much like most utilities, to automatic charges made to a credit/debit card account. With the latter option, the vehicle owner does not need to take any action other than paying the credit/debit card balance as he or she normally would.

.

# CHAPTER 7
# CONCLUSIONS AND RECOMMENDATIONS

The primary objective of the research presented in this monograph has been to develop a new approach to assessing road user charges. A new approach is needed because there is little doubt that in the foreseeable future, new vehicle propulsion systems will enter the marketplace. As new propulsion systems, such as hydrogen fuel cells and electric hybrid systems, become more common, the traditional motor fuel tax will become less productive. Thus, our research objective was to design an approach to assessing road user charges that (1) is capable of ensuring a stable stream of revenue to provide adequate funding of the U.S. road and highway system and (2) has a series of other desirable qualities. These other qualities include a low evasion rate, efficiency in terms of cost of collection for both the agency and user, convenience and ease of use, and above all, assurance that the privacy of road users will be protected. Another important quality is the flexibility to enable the respective states (and substate areas) to pursue various public policy objectives such as creating incentives to travel on appropriate roads and to spread demand across time periods.

The best approach to assessing road user charges, we have concluded, is one that is based on the actual mileage traveled. It is essential that there be a means for crediting the state (or substate jurisdiction) for the miles of travel occurring within it. With a vehicle-miles-traveled (VMT) user charge, an individual state can tailor the per-mile rates to pursue equity and efficiency objectives as well as to encourage environmentally friendly vehicles and travel on appropriate roads (e.g., for heavy vehicles to use roads capable of supporting their axle loads).

The next question we faced was how best to assess a VMT-based road user charge. Should the intelligence lie with the road or the vehicle? Smart-road intelligent transportation system (ITS) technology has become well accepted, particularly in the eastern U.S. where the E-Zpass is widely used for tolling high-capacity highways. For area-wide applications, however, smart-vehicle ITS technologies are more promising, in part because of the many problems associated with the roadside interrogating devices necessary for a smart road system to assess user charges.

## BASIC FEASIBILITY OF THE NEW APPROACH

We explored possible smart vehicle technologies and concluded that a relatively simple, GPS-based on-board computer is likely to be the cost-effective means for achieving the objectives noted above. The key system components needed for an on-board system capable of achieving these purposes include:

- a GPS receiver to position the vehicle,

- a GIS file to indicate the road being traveled or the jurisdiction in which the travel has occurred,
- an on-board computer capable of storing road-use data and making simple computations, such as applying a given state's per-mile user charge rates to the relevant miles traveled,
- a mechanism for transmitting the stored road-use data to a collection center and receiving information from the center, and
- a means for informing the driver of accumulated user charges and, possibly, interest charges for travel that occurred earlier than a specified amount of time in the past.

Fortunately, all of these components rely on existing technology. Especially fortuitous is the likelihood that GPS receivers and GIS data files will become increasingly commonplace in both autos and heavy vehicles. There is little doubt that the on-board equipment necessary to institute a VMT user charge system will either be supplied by vehicle manufacturers for other objectives or will constitute a very modest additional cost to vehicle owners.

In addition to the on-board equipment, a collection center is needed to receive road-use data from an individual vehicle and charge the vehicle's owner. Using technology similar to that of credit/debit card companies, it is feasible to aggregate the user charges for all vehicles traveling within a given jurisdiction as well as to aggregate the user charges for a particular vehicle that has traveled within multiple jurisdictions.

Linking the vehicle and the collection center can be accomplished in several ways. Two of the more promising mechanisms are:

- A smart card inserted into the dash can receive road-use data from the on-board computer. The smart card can then be removed from the vehicle and inserted into a reader in a convenience store or other business. The reader enables data to be uploaded to the collection center much the same way that credit/debit card readers connect to billing facilities. The collection center also can transmit data, such as revised per-mile user charge rates, to the smart card for subsequent relaying to the computer on board a vehicle. Thus, the smart card acts as a form of "messenger."
- Alternatively, refueling facilities eventually can be equipped with readers that are similar to the credit/debit card readers that currently are located at refueling pumps. A positive link between the vehicle and refueling facility will enable road-use data to be transmitted as the refueling occurs. This option may not be available during initial implementation because of the more extensive infrastructure needed.

Whatever technology is applied to transmit road user data from the vehicle to the collection center, it must be private, secure, and reliable. Modern encryption

methods offer considerable promise that these qualities will be present in the approach we have developed.

In short, the new approach to assessing road user charges discussed in this monograph is technologically feasible. It is possible to incorporate the desirable attributes mentioned earlier and to preserve the privacy of road users. As we stressed in the foregoing chapters, with the new approach the only data element that can be tied to a specific vehicle is a total road user charge since the last data upload. Using a reliable form of encryption, supplemental data can be sent anonymously to instruct the collection center how the user charge paid by the vehicle should be allocated among states or substate jurisdictions.

## MAJOR POLICY CONSIDERATIONS

While the new approach definitely is technologically feasible, a series of important public policy issues need to be considered prior to implementation. First and foremost, each state must decide whether to supplement the primary objective of revenue collection with one or more other purposes. As a general rule, we recommend not complicating the new approach with other features and instead focusing on revenue collection. As designed, the new approach to assessing road user charges will not compromise user privacy when merely used to collect user charges. If, in time, the traveling public wishes, several other features can be added to the new approach, including:

- Implementing a voluntary (opt-in or opt-out) sampling procedure that would allow anonymous data to be gathered on trip patterns within a metropolitan area. These data have the potential to revolutionize the travel demand analysis process and to dramatically improve cities' transportation planning capacities. Likewise, pavement management practices could be substantially upgraded if data on traffic volumes and composition were to become available. In much the same way that the apportionment information will be transmitted from the vehicle to the collection center anonymously using encryption, data on vehicle travel patterns also could be provided to the collection center. The center would aggregate the data, further protecting the privacy of individual road users, before providing them to governmental agencies for transportation planning purposes.
- Varying the per-mile user charges assessed for different classifications of roads. For example, a state may wish to allow local governments within it to charge higher per-mile rates for travel within residential areas to discourage through traffic from taking shortcuts using residential streets. In the same vein, heavy vehicles may be charged more per mile for travel on lower-standard roads than on arterial highways that were designed to accommodate higher axle loads.
- Encouraging the operation of energy-efficient vehicles by charging a lower per-mile rate for travel by these vehicles within the state.
- Enabling privately owned highways, such as freight truck-only routes. With the new approach, the traditional barriers to privately constructed and operated

highways are mostly eliminated. Currently, the motor fuel tax corresponding to miles traveled on private facilities cannot easily be apportioned to the operating entity, making toll booths necessary at all points of entry and exit. The new approach will enable private operators to determine an appropriate per-mile user charge, and travel on these highways can be credited to these operators. Tollbooths would be unnecessary.

- Varying per-mile charges with traffic volume on major highways. With communication between the highway and the vehicle, it would be technologically possible to increase these charges as a facility approaches its functional capacity. User charges thus become a form of rationing mechanism to encourage higher vehicle occupancy rates and deferral of trips to off-peak periods.

We stress that it is our recommendation to focus on applying the new approach to ensure a stable revenue stream regardless of how vehicles are propelled in future years. When the motoring public becomes comfortable with the new approach, it may be possible to explore other public policy considerations; but we think that should wait. Our purpose in summarizing these other objectives has been to (1) highlight the substantial inherent flexibility afforded by the new approach to assessing road user charges and (2) suggest that in time several policy actions that address lingering problems may become practicable. We have designed the new approach to be a flexible tool for policy makers to use in making transportation systems function well.

## LOOKING AHEAD

The research team has explored numerous aspects of the new approach to assessing road user charges and has gradually improved the basic design to a point where it is technologically feasible and capable of achieving its intended purpose of revenue collection. Yet, the stakes are high when implementing this or any other mechanism for eventually replacing the motor fuel tax. Nationally, the motor fuel tax generates approximately $50 billion annually. Motor vehicle manufacturers will need to equip literally millions of new autos and trucks with the on-board equipment necessary to enable the new approach to perform its functions. These manufacturers have to be very certain that the on-board equipment is well designed and devoid of any fatal flaws. Perhaps most importantly, both governmental agencies and vehicle manufacturers must be certain that the new approach will find acceptance on the part of the motoring public. Any features that can make the new approach even more appealing to road users need to be identified.

We recommend that a systematic field test and demonstration be carried out. By equipping a sizable number of autos and trucks with the on-board equipment required to support the new approach, four types of necessary insights can be gained:

- The reliability and security of the specified equipment can be rigorously tested, with revisions in this equipment made as conditions warrant. For example, dead reckoning back-up data on distance from an odometer can be assessed, as

can the ability of inertial chips and rate gyros to provide the on-board computer with directional information if GPS signals are interrupted. Prototype GIS data polygons can be field-tested.

- User reactions to the system can be assessed, and changes can be made to the operating protocol of the new approach to make it as attractive as possible to road users.
- Communications between vehicles and a prototype collection center can be tested and revised as needed. Smart-card technology has considerable potential, but it needs to be fully tested as a link between vehicles and the collection center.
- Extensive interaction with vehicle manufacturers needs to occur to ensure that the prototypical on-board systems are designed for easy integration with other vehicle equipment. Emphasis needs to be placed on redundancy, accuracy, protection, security, reliability, and cost. Maximizing the use of vehicle equipment designed for other functions (e.g., electronic odometers) will help minimize production costs.

With a rigorous, multi-year testing program, we believe there is little doubt that the new approach to assessing road user charges can be developed into a successful replacement for the motor fuel tax. The concept certainly appears viable, and the need for the new approach is becoming increasingly clear. Even if most people come to understand this need, it will be essential for state departments of transportation and local governments to actively inform the public and seek its input while moving toward implementation. Our hope is that by the time alternative propulsion systems become sufficiently popular to constitute a threat to the ability of the motor fuel tax to generate revenue, the new approach will be so fully refined and tested that it will be able to step in and ensure adequate funding to maintain America's vital road system.

# APPENDIX A
# LEGAL ASPECTS OF USER PRIVACY

The new approach to assessing road user charges involves using on-board computers to record road-use data, which are then downloaded to a collection center that prepares billing statements for vehicle owners. A series of options are possible regarding the detail and nature of the data recorded. Which option is most appropriate depends on a series of considerations, one of the most important of which is privacy. How completely the privacy of the vehicle operator is protected depends at least in part upon the detail and specificity of the data that are collected, stored, and transmitted to the collection center. Arguments for transmitting relatively detailed data on road use are based largely on the value such data would represent to agencies seeking to advance the public interest through better system planning and management.

In this appendix, we examine the legal foundations of privacy related to travel on public roadways. We also examine the legal aspects of the more specific issue of privacy related to electronic collection of data regarding people's travel patterns. This appendix has three primary objectives:

- summarize privacy concepts from a number of legal practice areas and highlight accepted standards for implementation;
- arrive at an operational definition of privacy that can serve as a foundation for the design of the new approach; and
- recommend procedures to ensure that the new approach will protect the rights of its users.

This last step is necessary not only for citizen support but also to withstand challenges from special interests that may see this approach as an opportunity to protest all forms of electronic data collection, regardless of how, where, or why they are collected.*

---

* Because the courts operate on the basis of a common law tradition and often refer to cases decided hundreds of years ago, many have found it difficult to respond to rapid technological advances. In the case of *United States v. Knotts*, 460 U.S. 276, 284 (1983), dealing with a challenge that police surveillance using an electronic transmitter violated the rights of the suspect, the Court held that there might be cases of "dragnet-type" police practices that require new legal limits on monitoring.

## SOURCES OF PRIVACY LAW

The phrase "privacy law" may be a bit deceiving in that it suggests that courts and administrating agencies apply a singular privacy standard and definition in all cases. In fact, privacy involves a number of concepts that often are not wholly compatible. For example, when a new federal or state rule emerges governing police surveillance of vehicles, a citizen's right not to be unreasonably searched by the government is implicated. This circumstance is quite different from the right not to have embarrassing information from a government database published in a newspaper. The latter situation deals more with the area of tort law pertaining to privacy invasion than with government searches.

Several areas of legal practice provide guidance on how to implement a system to electronically gather data on road use. In addition to criminal and tort law, a third legal realm involves matters of administrative law (i.e., how to give drivers fair notice of the data that will be collected and how to avoid intrusions on their rights).

Basic definitions of these three areas of the law follow:

- **Torts.** The body of rules governing determinations of liability for emotional or physical injury resulting from intentional wrongs or failures to exercise a duty of reasonable care towards another, implying negligence.
- **Administrative law.** The body of rules government agencies use as a guide to conduct, including measures to ensure the validity of decisions and standards for courts reviewing such decisions outside the administrative framework.
- **Criminal law.** Rules governing inappropriate societal behavior and penalties for violations involving restrictions on individual liberties. Sec. 1.04(1) of the Model Penal Code defines a crime as an act that violates the standards of a community as reflected in a statute or rule (local, state, or federal). Crimes are punishable by fines and/or imprisonment, which distinguishes their remedies from contracts or other types of law.

Finally, if electronic data collection in any way interferes with a driver's "freedom of association," a fourth area of concern may involve the First Amendment. Freedom to associate refers to a person's right to make unencumbered decisions about participating with others in activities.

> In short, the type of privacy relied upon by courts to analyze the appropriateness of an electronic user charge system will depend on the specific allegations of those who may sue in protest. Claims potentially could arise in a criminal, tort, administrative, or freedom-to-associate context.

**Defining Privacy: Theoretical Foundations**

While the courts are still addressing privacy rights in a piecemeal manner, a number of legal theorists have proposed privacy definitions. As early as 1890, Warren and Brandeis established that privacy was simply "the right to be left alone."[1] Public agencies establishing programs that involve electronic collection of travel patterns, however, need more than a vague definition to guide them. They need a privacy definition that is sensitive to technological advances. While the following definition of privacy by Westin does not specifically encompass technology, it signifies the point at which many courts are currently operating:

> Privacy is "[t]he voluntary and temporary withdrawal of a person from the general society through physiological means, either in a state of solitude or small-group intimacy or when among larger groups, in a condition of anonymity or reserve."[2]

A definition by Allen was one of the first to address technology head on:

> Privacy is "a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others … [it] is protected when the person (or the person's mental state, or information about the person) is beyond the range of others' five senses and devices that can enhance, reveal, trace, or record human conduct, thought, belief or emotion."[3]

Allen's definition seems reasonable as an extension of Westin's conception. Her interpretation empowers the individual to determine how and to whom to reveal personal information.

There are, however, two more liberal notions of privacy that involve technology but would cause the courts to develop entirely new legal standards. The first concept is locational privacy. Here, the idea is that privacy is a right that is violated when a state gathers "space-time coordinates" on an identified individual otherwise protected by his or her anonymity.[4] For example, simply parking a car in front of a residence known to sell illegal narcotics would not necessarily establish a driver's intent to purchase drugs. Information showing that the particular driver had traveled to several similar establishments in the past hour might aid in demonstrating such intention.

With the second nontraditional theory, McClurg recognizes public privacy, in which anonymity gives people a right to keep public acts unknown.[5] According to McClurg, people walking along the street would be protected from revealing private facts about themselves because a multitude of public activities occurring simultaneously would keep them "obscure[d]." In other words, the chance that a random person in a public place would focus continually on another random person specifically for a period long enough to judge the actions of the observed person would be minuscule, especially given that standards for identifying which

public events or people to observe would vary infinitely across observers.* If accepted, both of these conceptions of privacy create a right that applies directly to collecting electronic road use information. The right to locational and public privacy would counter current legal notions that give vehicles fewer protections in public.

> While the courts have been reluctant to recognize more liberal privacy definitions (i.e., those involving locational or public privacy), agencies collecting electronic data on vehicle travel should be prepared to adopt these more stringent definitions, which could help to win public support for the new approach to assessing road user charges.

**Privacy Expectations in Context**

While interpretations of applicable laws to protect privacy differ in a number of ways, a common thread linking the court opinions has been the notion of a reasonable expectation of privacy. In the criminal case of *Katz v. United States,*[6] the Supreme Court articulated a clear rule that still stands today.** In the *Katz* opinion, the Court stated that a person's activities, if they are to be protected, must meet two tests before it will recognize his or her right to privacy. First, the person must show a subjective expectation of privacy. This means that the person must show in the actions he or she took a desire to keep his or her activities private.[7] Second, the person must show an objective expectation of privacy. "Objective" means that society is generally willing to recognize a privacy value in the specific actions of the person raising the claim. For example, society is more likely to support an expectation of privacy in one's home than in an auto driving through town.[8]

Tort law is different from criminal law in that a tort is a "civil wrong, other than breach of contract, for which the court will provide a remedy in the form of an action for damages."[9] In the tort context, privacy analysis is similar to the *Katz* test in the way that a person must show an interest in privacy while carrying out the

---

* McClurg suggests that "[I]n obscurity there is privacy." Andrew J. McClurg, 1995. "Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions" in *Public Places*, 73 *N.C. L. Rev*. 989, 1034. Accordingly, "[t]he freedom enjoyed in anonymity disappears … the moment someone begins paying attention to us." *Id*. at 1034-35.

** *Katz* was a case involving police surveillance of a suspect in a telephone booth. Officers placed a monitor directly above the telephone booth and listened in on Katz's conversation, even though the door was closed. The Supreme Court reasoned that reasonable people would expect a certain degree of privacy in their conversations within telephone booths and held the police conduct unconstitutional on this basis.

activity in question.* Yet, the *Restatement of Torts* defines "privacy invasion" in such a way that more than an infringement on someone's personal space is required to constitute a violation. In addition to the infringement, the plaintiff must demonstrate that the violating party acted intentionally.** Many courts further require that the violation involve publishing incriminating or humiliating facts to a wide public audience to prove harm.[10] These stringent requirements make it so difficult for plaintiffs to prove their cases that some scholars suggest tort law has little value in deterring privacy invasion.[11]

> Thus, as it relates to privacy, tort law is not likely to be a basis for legal action against an agency using the new approach to assessing road user charges.

While tort law has been restrictive in its recognition of privacy invasion claims, one circuit court has carved an exception recognizing a zone of privacy protecting people in public. This legal rationale comes from the case of *Galella v. Onassis*,[12] in which the Second Circuit Court of Appeals found impermissible the actions of a reporter who harassed a celebrity on a public street, thereby invading her private space. This interesting exception, which creates a privacy right, has elements similar to *N.A.A.C.P. v. Alabama*[13] and *Talley v. California*.[14] The Supreme Court in these two cases found that the freedom to associate, which relates to exercising one's First Amendment freedom of speech, creates a right to remain anonymous in political activities.*** Seemingly, the zone of privacy argument would be more

---

* In tort law, the concept of privacy can involve any combination of four components:

- **Intrusion upon seclusion.** "Intentional intrusion, physical or otherwise, upon the solitude or seclusion of another or his private affairs and concerns."
- **Public disclosure of private facts.** Offensive disclosure of personal information, such as income tax returns or personal behavior of a humiliating manner.
- **False light privacy.** Giving "publicity to a matter concerning another that places the other before the public in a false light … if the false light … would be highly offensive to a reasonable person."
- **Misappropriation of name or likeness for a commercial purpose.** Use of someone's name or likeness without his or her consent. *Restatement (Second) of Torts* **§§** 652B-652E (1977).

** See, e.g., *id*. at § 652B (requiring that the invasion of privacy "be highly offensive to the reasonable man").

*** *N.A.A.C.P.* held unconstitutional demands for the identities of dissident group members because revealing these identities might cause members not to participate in group activities. Similarly, *Talley* involved demands to identify the people responsible for posting political flyers in a neighborhood.

compelling against the collection of road-use data than the freedom to associate because motor vehicles are rarely involved in political expression.*

In the criminal context, the Supreme Court has addressed vehicle monitoring specifically, and has gone further to define impermissible governmental invasions of privacy. In *United States v. Karo*,[15] the Court reasoned that monitoring cars in enclosed areas, like subterranean garages, would violate a driver's rights because no one situated on a public street would know the precise location of the vehicle without the aid of the invasive tracking technology.** Along these lines, in *Berger v. New York*,[16] the Court held that monitoring for "prolonged" periods of time violates a suspect's privacy rights. In *Berger*, the invasive police activity included authorization of eavesdropping for a two-month period, "24 hours a day," and extending to "the conversations of any and all persons coming into the area covered by the device."[17] The Berger Court found the monitoring impermissible because prolonged surveillance is analogous to "a series of intrusions, searches, and seizures."[18] It is conceivable that a court might similarly hold that continuous vehicle monitoring violates the same interest of a driver, depending on the detail of the information so obtained.

## ALLOWANCES FOR COLLECTING ROAD-USE DATA

Unique legal allowances make the electronic collection of road-use data permissible, notwithstanding the legal standards articulated above. In the first case, if a driver consents to the electronic collection of road-use data, he or she cannot later raise a privacy invasion claim. Criminal law supports this notion by holding that consent to a search destroys a Fourth Amendment claim.*** Similarly, the

---

* In another line of reasoning, a reviewing court may also choose to apply Epstein's Unconstitutional Conditions analysis if a plaintiff alleges that driving on monitored roads has forced him or her to barter the right to privacy in return for his or her freedom to travel. Generally, such a trade-off is unconstitutional and thus impermissible if it involves "coercion" or compulsion. (Richard A. Epstein, 1988, "Unconstitutional Conditions, State Power, and the Limits of Consent," 102 *Harv. L. Rev.* 5, 7). However, in the vehicle-monitoring context, compulsion would be difficult to prove given the existence of alternative transportation sources. For a discussion of Unconstitutional Conditions, see Kathleen M. Sullivan, 1989, "Unconstitutional Conditions,: 102 *Harv. L. Rev.* 1414, 1442-43 (describing the three-prong test for when the theory applies); and Eustace T. Francis, 1995, "Legal Development: Combating the Drunk Driver Menace: Conditioning the Use of Public Highways on Consent to Sobriety Checkpoint Seizures–The Constitutionality of a Model Consent Seizure Statute," 59 *Alb. L. Rev.* 599 (applying the theory to modern situations and commenting on its difficulties).

** In *Karo*, police used a tracking device to locate narcotics that a driver transported from a storage facility to his home. The transmitter monitored the location of the drugs inside the suspect's home, even though an observer on the street would not have known their whereabouts.

*** See *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973) (recognizing the consent doctrine, but providing specific guidelines regarding whether consent is valid).

courts have held that if a person simply hopes that his or her suspicious public activity will go unnoticed, the person may very well assume the risk that authorities will become aware of incriminating behavior.[19]

In the administrative law context, courts could reason that a driver implicitly consents to having his or her travel observed every time he or she uses a public road. One rationale for this rule was first established in the case of *New York v. Burger*,[20] in which the Supreme Court allowed for an administrative inspection of a junkyard because the business was part of a "pervasively regulated industry."* In another line of similar cases, such as *Wyman v. James*,[21] the courts acknowledged the rights of public services to conduct inspections in the homes of those who consume such services.** Consider the case of *Cacioppo v. Southwestern Bell,*[22] in which a state court held that a telephone serviceman violated the rights of a tenant only after he acted unreasonably and created a nuisance on her premises.[23]

**Diminished Expectation of Privacy**

In both criminal and tort actions, courts have recognized a "diminished expectation of privacy" in vehicles due to their inherent mobility[24] and the fact that people do not normally treat cars like homes.[25] Courts often agree with this rule because vehicles are "thrust out into the public eye."[26] Furthermore, courts have articulated these concepts in two legal doctrines. First, the Open Fields rule stands for the proposition that anything seen from a lawful vantage point, like an open field, is fair game for public observation.[27] Second, the Plain View rule similarly allows for observation of anything visible to the naked eye.[28] Courts often ask whether a person on the street would have been privy to the conduct to determine if surveillance qualifies for either rule.***

---

* Building on this rationale, Weisberg suggests that mere registration of a vehicle, as it exposes drivers to a number of invasive state practices, would give a department of motor vehicles a right to monitor a driver's travels. See Robert Weisberg, 1995, "IVHS, Legal Privacy, and the Legacy of Dr. Faustus," 11 *Santa Clara Cptr. and High Tech. L.J.* 75, 88 (noting that "we invite the administrative state to monitoring our driving skill, test our cars for pollution and accident danger, and tax us for our use of roads and bridges").

** *Wyman* held that AFDC workers could enter perspective recipients' homes to conduct interviews as long as they provided advance notice and adhered to procedural limitations. However, this case might be limited by the Supreme Court's earlier holding in *Camara v. Municipal Court,* 387 U.S. 523 (1967) (finding that a building inspector violated tenants rights by entering her home without first showing probable cause to inspect).

*** Note, however, that some scholars have challenged this view. Many claim that only a long chain of witnesses who report everything they see accurately to one another from a vehicle's origin to its point of destination can truly convey the same amount of information as a police surveillance team. See Note, "Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights," 71 *Va. L. Rev.* 297, 311 (1985) (requiring an "army of bystanders, conveniently strung out on the route" citing LaFave 1983, "Nine Key Decisions to Expand Authority to Search and Seize," 69 *A.B.A. J.* 1740, 1740).

The "diminished expectation of privacy" and Plain View rule have major implications for the new approach to assessing road user charges. They suggest that because motor vehicles normally operate in an environment that is commonly visible, keeping an electronic log of basic travel data is not likely to be regarded by the courts as an intrusion.

At a recent conference regarding whether technology is changing the law, Volokh distinguished data collection (i.e., acts in which the government monitors the activities of citizens) and data revelation (i.e., acts in which the government transmits or reveals the data to other parties).[29] Volokh emphasized that data collection is more an issue of government power than it is a matter of privacy invasion. In other words, people may fear that the government will use the data for its own advancement and become more regulatory in response to its perceptions of people's activities. This distinction highlights administrative rather than legal solutions as the best protection for drivers who fear that their comings and goings will not be private.[30] The administrative context can, after all, respond to driver concerns where the Plain View and Open Fields rules would limit privacy protection.

The preponderance of legal opinions suggests that as long as vehicle monitoring is not continuous, does not extend to areas where technology would indicate the precise location of a car when the naked eye could not view it (i.e., during travel within private buildings such as parking garages), and drivers are given advance notice of the electronic system for collecting road-use data, the act of collecting these data should not violate drivers' rights to privacy.

### Criminal Justice Guidelines

In 1998, the American Bar Association adopted standards to help resolve the inconsistencies in the criminal law of electronic surveillance.* The resulting General Principles, enunciated in Standard 2-9.1, indicate that technological surveillance must be regulated, even given its tremendous potential to aid law enforcement agencies.[31] This standard first illuminates the factors that govern the

* See generally American Bar Association, Criminal Justice Standards Committee, 1999, *ABA Standards for Criminal Justice Electronic Surveillance, Third Edition, Section B: Technologically-Assisted Physical Surveillance* (developing a number of guiding principles).

validity of law enforcement interests in monitoring suspects.* Second, in subsection (d), the standard defines how to implement surveillance activities.

Purposes of the General Principles include guarding against "arbitrary" use of technology, "limit[ing the technology] to its stated objectives and terminat[ing the monitoring] when those objectives are achieved," not to mention keeping the technology only in the hands of trained personnel.[32] Even while the applicable section suggests providing notice of monitoring whenever "appropriate," the most important guideline offered may be found at subsection (d)(iii): "When a particular surveillance device makes use of more than one regulated technology and the technologies are governed by differing rules, the more restrictive rules should apply."[33] This maxim is valuable in the context of collecting road-use data, because here a number of different rules from different areas of law potentially apply. The standard seemingly supports bypassing criminal precedents that offer law enforcement officials more leeway in their surveillance activities.**

## DATA PRIVACY AND RELATED LEGAL STANDARDS

Even if the act of electronically collecting road-use data does not violate drivers' privacy, poor management of the data so obtained could do so. The Supreme Court initially developed the notion of database privacy in *United States Department of Justice v. Reporters Committee for Freedom of the Press*.[34] In this case, the Court reasoned individuals have an expectation of privacy in personal information stored on a comprehensive computerized database.*** Following this ruling, the Supreme Court focused on specific standards for securing databases. In *Whalen v. Roe*,[35] the Court ruled that database administrators must implement "adequate safeguards" to protect against unauthorized access.**** Shortly thereafter, in *United States v.*

---

* See *id.* at 11-12 (indicating, *inter alia*, consideration of: "the care that has been taken to enhance the privacy of" the area (§ (c)(ii)(B)), the "lawfulness of the vantage point … including [considerations of whether the information is gained via] physical intrusion," (§ (c)(ii)(c)), the "availability and sophistication of the surveillance technology," (§ (c)(ii)(D)), "the extent to which the surveillance of the subject is minimized in time and space" (§ (c)(ii)(F)), "the extent to which the surveillance of non-subjects [in this case, arguably *passengers*] is likewise minimized" (§ (c)(ii)(G)), "whether the surveillance is covert or overt" (§ (c)(ii)(H)), and whether First Amendment freedoms are placed at risk and the least intrusive means of surveillance are employed (§§ (c)(iii),(iv)).

** While Standard 2-9.4 governs installation and monitoring of tracking devices, including intelligent highway systems, it addresses only surveillance for the purpose of detecting criminal activity, and thus does not address the new approach to assessing road user charges.

*** *Reporter's Committee* dealt with a convict's right not to have a newspaper publish incriminating information about him that was aggregated from government databases.

**** This case dealt with the right of a drug-addicted woman not to have information released about her medical status. The Court developed this standard yet held that the hospital in question adopted adequate safeguards to protect her information.

*Westinghouse,*[36] the Third Circuit Court of Appeals established a number of criteria defining "adequate safeguards."*

Most states take one of two approaches in creating data encryption systems. Some, such as California, develop broad standards.[37] On the flipside, states including Utah and Illinois have very specific encryption standards.[38] The American Bar Association recommends more heightened protection and urges systems requiring that:

> transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key, and (2) whether the initial message has been altered since the transformation was made.[39]

Regardless of security precautions, however, as long as database administrators are privy to data regarding drivers' daily travels, programs involving the collection of road-use data must regulate employee conduct. Some specialists recommend training programs and/or certification for all employees confirming standards of professional conduct, while others would impose criminal sanctions on administrators who misuse the system.

Those who implement a program that incorporates the collection of electronic data on road use can overcome public doubt regarding its reliability by consulting potential users during developmental phases and apprising the public of potential risks before the project is launched. Studies show that the public is willing to disclose information amid threats to its security when: "(a) information is collected in the context of an existing relationship, (b) [consumers] perceive that they have the ability to control future use of the information, (c) the information…is relevant to the[ir] transaction, and (d) [consumers] believe the information will result in reliable and valid inferences about them."[40]

Transportation agencies can thus increase perceptions of fairness by explaining: (1) why the information is collected, (2) its expected uses, (3) the steps that will be taken to protect its confidentiality, integrity and quality, and (4) the consequences of providing or withholding the information.[41] Similar practices substantially increased Arizona drivers' support for photo radar devices installed at vehicle

---

* In this case, the court identified five critical factors to determine the scope of adequate database privacy protections:

> The "type of record" stored and the information it… contain[s]," the "potential for harm" in the event of any unauthorized disclosure of information, "the injury from disclosure to the relationship in which the record was generated," "the adequacy of safeguards to prevent unauthorized disclosure," and the need for governmental access via a "recognizable public interest." 638 F2d at 578.

intersections.[42] These factors suggest that drivers' major fears may not involve data security, but instead the threat that monitors will label drivers according to their incriminating travel patterns (for example, visiting unsavory establishments).[43] The best way to dispel such beliefs might be to invite computer-literate citizens to the drawing board during the design phase of the program.[44]

To gain public support for the new approach to assessing road user charges, program administrators should secure databases with the highest level of encryption, involve drivers in the creation of security standards, apprise the driving public of associated risks, and use criminal sanctions to regulate employee conduct. Additionally, giving users a choice regarding levels of invasiveness might empower them with a feeling of control over the process rather than the feeling that the process controls them.

## CONCLUSIONS

There is no single definition or standard of privacy that can provide complete guidance in designing the new approach to assessing road user charges. In different ways, each of the fundamental areas of legal practice—tort, criminal, and administrative—have implications for the privacy of motorists. Tort law is the least likely to constitute an obstacle to the new approach; it requires a plaintiff to demonstrate that the violating party intentionally or carelessly did harm to another person. It is, therefore, highly unlikely that transportation agencies adopting the new approach would be subject to tort claims.

Criminal law case precedent is more varied. The Supreme Court has provided some guidance as to what constitutes impermissible government intrusions of privacy. Prolonged surveillance has been held to violate people's privacy rights, but there is little basis for concluding that the new approach would be regarded as surveillance at all, much less prolonged. Regarding administrative law, the courts generally have held that a driver implicitly consents to having his or her travel observed by the very nature of road use (i.e., one operates a vehicle in plain view).

In tort, criminal, and administrative law cases, the courts have recognized a diminished expectation of privacy when traveling in a motor vehicle, relative to being in a private residence, for example. The more salient issue seems to be that of appropriate government power. More specifically, the issue revolves around the extent to which government agencies may use personal travel data to advance objectives other than those for which the new approach to assessing road user charges is intended. This suggests that the purposes of the new approach should be clearly articulated at the time it is implemented.

In conclusion, our review of legal precedent found nothing that indicates the new approach to assessing road user charges would constitute an invasion of motorists'

privacy. The real issues are most likely to center around implementation. How detailed the data are that the on-board computer stores for uploading to the collection center will be a prime consideration. Steps the collection center may take to ensure anonymity of the traveler when analyzing and presenting the resulting trip data also will be highly important. Additionally, it will be advisable to assure the motoring public that the only uses of the data will be for assessing road user charges and (optionally) technical analyses associated with providing transportation services.

**ENDNOTES**

[1]Samuel D. Warren and Louis D. Brandeis. 1890. "The Right to Privacy," 4 *Harv. L. Rev*. 195.

[2]Alan F. Westin. 1967. *Privacy and Freedom* 7.

[3]Anita L. Allen. 1967. *Uneasy Access: Privacy for Women in a Free Society* 15.

[4] See Daniel B. Curtis. 1995. "Examples of How IVHS Architecture Decisions Affect Personal Privacy," in Dorothy Glancy ed., *Privacy and Intelligent Transportation Systems: Legal Research Reports* 267, 267 n.3, 267-68.

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

[6] 389 U.S. 347 (1964).

[7] See, e.g., *Katz v. United States*, 389 U.S. 347, 351 (1967) (describing protection for "what a person seeks to preserve as private, even in an area accessible to the public"); *United States v. Ford*, 34 F.3d 992, 995 (11th Cir. 1994) (holding that defendant did not show a subjective expectation of privacy in the heat emitted from his mobile home when using marijuana because his "affirmative conduct" of "expel[ling] the excess heat" showed that "he did not seek to preserve the fact of that heat as private").

[8] See, e.g., *California v. Greenwood*, 486 U.S. 35, 39-40 (1988) (noting that "[a]n expectation of privacy does not give rise to Fourth Amendment protection, however, unless society is prepared to accept that expectation as objectively reasonable" and finding no objective expectation of privacy in trash bags people leave on their curbs).

[9] W. Page Keeton et al., 1984, *Prosser and Keeton on the Law of Torts* § 1, at 2 (5th ed.).

[10] See generally McClurg, *supra* note 5.

[11] See *id*. at 1000-01 (describing that a majority of judges "deprived plaintiffs the opportunity to have their privacy claims heard by a jury" in a random sampling of 1992 tort actions).

[12] 487 F.2d 986 (2d Cir. 1973). While a zone of privacy might arguably extend to drivers, computerized record keeping is hardly as invasive as media harassment.

[13] 357 U.S. 449 (1958).

[14] 362 U.S. 60 (1960).

[15] 468 U.S. 705 (1984).

[16] 388 U.S. 41 (1967).

[17] *Id*. at 59.

[18] *Id*.

[19] See *Frazier v. Cupp*, 394 U.S. 731, 740 (1969) (discussing how a bag owner "assumed the risk" that his cousin would allow authorities to look inside).

[20] 482 U.S. 691 (1987). More recently, the case of *Commonwealth v. Pertroll*, 696 A.2d 817 (Pa. Super. 1997), suggested that an invasive inventory of a commercial truck was not a search based on the *Burger* criteria.

[21] 401 U.S. 309 (1971).

[22] 550 S.W. 2.d 919 (Mo. App. 1977).

[23] *Id*. at 923.

[24] See, e.g., *California v. Carney*, 471 U.S. 386 (1985) (holding that mobile homes have less protection than stationary real estate solely because they are transportable).

[25] See, e.g., *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (recognizing that vehicles are "seldom … one's residence or … the repository of personal effects").

[26] *New York v. Class*, 475 U.S. 106, 114 (1986) (holding that there is no right to privacy in a car owner's vehicle identification number).

[27] See *Hester v. United States*, 265 U.S. 57, 59 (1924) (holding that any protection accorded to "people in their 'persons, houses, papers, and effects,' is not extended to the open fields" (internal citation omitted)).

[28] See *Harris v. United States*, 390 U.S. 234 (1968) (holding that police could seize items in plain view during an automobile inventory search).

[29] See Eugene Volokh. 2001. Remarks at the Twentieth Annual Student Symposium of the Federalist Society, *Is Technology Changing the Law?* University of California, Berkeley (March 10).

[30] See *id*.

[31] See generally American Bar Association, Criminal Justice Standards Committee. 1999. *ABA Standards for Criminal Justice Electronic Surveillance*, Third Edition, Section B: Technologically-Assisted Physical Surveillance 11.

[32] *Id*. at 12.

[33] *Id*. (added for effect).

[34] 489 U.S. 749 (1989) (holding that inspections did not constitute unreasonable searches if (1) there was a substantial government interest in the regulatory scheme, (2) the search was "necessary" to further the scheme, and (3) the inspection program was certain and regular in its application).

[35] 429 U.S. 589 (1977).

[36] 638 F.2d 570 (3d Cir. 1980).

[37] See Cal. Gov. Code § 16.5 (2001) (holding an electronic signature valid when it is "unique" to the user, "under" her exclusive control," verifiable, and "linked to the data in such a manner that if the data are changed, the digital signature is invalidated").

[38] See Utah Code Ann. § 46-3-103 (10) (2000); 5 I.L.C.S. 175/5-105 (2000) (articulating specific standards).

[39] See Information Security Committee, Section of Science and Technology, American Bar Association. 1996. *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*.

[40] See Mary J. Culnan and Pamela K. Armstrong. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," 10 *Organization Science* 104, 106 (reviewing various studies).

[41] *Id*. at 107.

[42] See Thomas M. Stanek. 1998. "Photo Radar in Arizona: Is it Constitutional?" 30 *Ariz. St. L.J.* 1209 (describing factors that caused the public to support the program in light of its potential invasiveness).

[43] See generally Dorothy J. Glancy. 1995. "Privacy and Intelligent Transportation Technology," 11 *Santa Clara Cptr. and High Tech. L.J.* 151 (exploring drivers' ten greatest fears about monitoring programs).

[44] See generally Scott D. Makar and Michael R. Makar. 1995. "Geographic Information Systems: Legal and Policy Implications," 69 *Fla. Bar J.* 44 (recommending citizen involvement to quell fears of unrestrained government surveillance).

# APPENDIX B
# PHASING IN THE NEW APPROACH

The new approach to assessing road user charges represents a completely new way of generating revenue to defray the costs of providing roadways and other transportation facilities in the United States. It also is a viable means for varying road user charges on these facilities in accordance with adopted public policies. A major impetus for studying the new approach is the growing realization that traditional methods for charging road users have serious limitations and are not likely to be fair or productive as new propulsion technologies for passenger and freight vehicles become more commonplace. For example, electric-powered vehicles or those powered by hydrogen fuel cells will not pay motor fuel taxes because they will not burn traditional gasoline or diesel fuel.

In this appendix, we explore the complex issue of how best to phase in the new approach, which would operate very differently than the motor fuel tax. We have concluded that retrofitting existing vehicles with the on-board computer, global positioning system (GPS) receiver, and associated equipment generally would not be feasible. The central issue thus becomes how best to proceed with two very different approaches operating side by side for a number of years. A major concern in this regard, especially for autos, is how to ensure that the two methods of charging road users are as close to equal in cost as possible on a per-mile basis. We begin by examining available data to provide a preliminary estimate of how quickly the auto and truck fleets can be expected to be replaced, and thus how soon the new approach could become the predominant method of charging road users.

## REPLACEMENT RATES FOR MOTOR VEHICLES

Two primary trends are germane to vehicle replacement rates. The first is new-vehicle sales, and the second is scrappage rates. Also important to implementation of the new approach are annual average mileages by vehicle type and age. We examine these phenomena in turn.

### New Vehicle Sales

Table B-1 shows the rate at which new autos and trucks are entering the vehicle fleet. The table indicates that there has not been a sustained increase in new auto sales during the past two decades. A review of auto sales during this period shows that sales generally were in the range of 8.1 to 8.9 million units annually. A few outliers occurred, such as in 1985, when 11 million autos were sold. By far the most substantial increase in new vehicle sales has been in light trucks, which increased from 1.964 million to 8.405 million units, an average annual increase of almost a third of a million vehicles. It also is worth noting that annual sales of medium-to-heavy trucks increased by 72.4 percent over the 20-year period. Sales of Class 8 heavy trucks, those over 33,000 pounds gross weight, increased by an

average of approximately 6 percent annually during the last half of the 1990s. Automotive News (2001) forecast somewhat lower new auto and truck sales by the year 2005.

**Table B-1. New auto and truck sales, 1980–2005 (millions of units)**

| Year | Autos | Light trucks | Medium-to-heavy trucks | Total |
|---|---|---|---|---|
| 1980 | 8.979 | 1.964 | 0.268 | 11.211 |
| 1990 | 9.300 | 3.984 | 0.278 | 13.562 |
| 1995 | 8.635 | 5.703 | 0.388 | 14.726 |
| 2000 | 9.005 | 8.405 | 0.462 | 17.872 |
| 2005* | 7.835 | Total trucks: 8.674 | | 16.509 |

*Values for 2005 are forecasts by *Automotive News* (2001).

SOURCES: U.S. Census Bureau (2000, Table 1031), for years 1980–1995: *Automotive News* (2001) for year 2000.

As Table B-2 indicates, from 1991 to 2000 the total number of trucks in use has grown appreciably more than the total number of autos in use. The auto fleet grew only 3.5 percent, with an average annual percentage growth of 0.4 percent. Meanwhile, the truck fleet grew by 47.1 percent over the decade, increasing by 4.4 percent annually, on average. The overall motor vehicle fleet increased by 17.5 percent during the 1990s.

### Overall Vehicle Fleet Turnover

Although 11 to 17 million new vehicles have been added to the fleet each year during the 1990s, the overall number of vehicles on U.S. highways is growing at a much slower rate. Of particular salience to this analysis is the fact that there is a substantial turnover each year as older vehicles are scrapped. Table B-3 shows that during the 1990s, an average of 5.2 percent of the auto fleet was scrapped each year; the net gain in autos registered to operate on U.S. roads generally was about one million. On average, 4.8 percent of the truck fleet was scrapped annually over the decade.

Another way of looking at the rate of change in the vehicle fleet is median age. Table B-4 shows that the median age of autos has almost doubled since 1970, to 8.3 years. A simple trend analysis suggests that the median age of autos will inch slightly higher, perhaps to 8.7 years, by 2010. In the case of trucks, the trend in the late 1990s was for median ages to decline. In Table B-2, we saw that the truck fleet grew quite rapidly during the 1990s; and this probably is the primary reason for the

drop in median age. Currently about half of the new passenger vehicles sold in the U.S. are light trucks (e.g., pickup trucks, minivans, and sport utility vehicles). If the popularity of these vehicles continues, the median age of the truck fleet will nudge down a little more, but probably not below about 6.5 years.

**Table B-2. Autos and trucks in use, 1991–2000**
**(millions of units)**

| Year | Total autos in use | Percentage change | Total trucks in use | Percentage change | Total vehicles in use |
|---|---|---|---|---|---|
| 2000 | 127.721 | 0.67 | 85.579 | 3.56 | 213.299 |
| 1999 | 126.869 | 0.72 | 82.640 | 4.51 | 209.509 |
| 1998 | 125.966 | 1.04 | 79.077 | 3.51 | 205.043 |
| 1997 | 124.673 | 0.05 | 76.397 | 3.69 | 210.070 |
| 1996 | 124.613 | 1.11 | 73.681 | 4.96 | 198.293 |
| 1995 | 123.242 | 1.02 | 70.199 | 5.22 | 193.440 |
| 1994 | 121.997 | 0.78 | 66.717 | 2.23 | 188.714 |
| 1993 | 121.055 | 0.59 | 65.260 | 6.69 | 186.315 |
| 1992 | 120.347 | (2.42) | 61.172 | 5.15 | 181.519 |
| 1991 | 123.327 | | 58.179 | | 181.506 |

SOURCE: R.L. Polk and Co., as cited in *Automotive News* (2001).

Regarding heavy trucks, particularly truck-load (TL) carriers, we surveyed six of the nation's larger firms as to how long they keep tractors (power units) in service. These units are replaced every two to seven years, with four years being the most common period. Thus, there is a fairly rapid turnover rate for long-distance heavy trucks.

**Rough Forecast of Vehicle Sales and Age**

The foregoing analysis indicates several key trends:

- New auto sales on an annual basis are essentially flat, although a downturn has been evident in recent years as light trucks have become more popular. While it is difficult to predict consumer preferences in the foreseeable future, new auto sales are unlikely to exceed 8 million units per year in the 2005–2010 period.

- New light truck sales burgeoned in the late 1990s. This growth presumably had two impetuses: a strong economy and the popularity of sport utility vehicles and pickup trucks. The forecast displayed in Table B-1 indicates that *Automotive News* magazine believes the growth in light truck sales will flatten out in the coming years.
- A reasonable annual sales estimate of these vehicles by 2005–2010 is about 8.5 million units. Medium-to-heavy trucks have experienced a steady increase in sales since 1980, as the nation's economy has grown and freight transportation has increasingly relied on the trucking industry. Annual sales of about 0.6 million units in the 2005–2010 period are likely.

**Table B-3. U.S. vehicle scrappage rate and net growth, 1991–2000 (millions of units)**

| Year | Autos scrapped | Net auto growth | Percent autos scrapped | Trucks scrapped | Net truck growth | Percent trucks scrapped |
|---|---|---|---|---|---|---|
| 2000 | 8.085 | .852 | 6.33 | 6.213 | 2.938 | 7.26 |
| 1999 | 7.216 | .903 | 5.69 | 4.447 | 3.563 | 5.38 |
| 1998 | 6.819 | 1.293 | 5.41 | 4.846 | 2.679 | 6.13 |
| 1997 | 8.244 | .060 | 6.61 | 4.265 | 2.717 | 5.58 |
| 1996 | 7.527 | 1.371 | 6.04 | 3.284 | 3.482 | 4.46 |
| 1995 | 7.414 | 1.245 | 6.02 | 2.918 | 3.481 | 4.16 |
| 1994 | 7.824 | .941 | 6.41 | 4.545 | 1.457 | 6.81 |
| 1993 | 7.366 | .709 | 6.08 | 1.048 | 4.088 | 1.61 |
| 1992 | 11.194 | (2.980) | 9.30 | 1.587 | 2.994 | 2.59 |
| 1991 | 8.565 | .050 | 6.95 | 2.284 | 2.156 | 3.93 |
| AVE. | 8.025 | .444 | 6.48 | 3.544 | 2.956 | 4.49 |

SOURCE: R.L. Polk and Co., as cited in *Automotive News* (2001).

The vehicle scrappage rates in Table B-3 show a certain amount of year-to-year variability; but on average during the 1990s, approximately 6.5 percent of the auto fleet was scrapped each year. For trucks, the average annual scrappage rate was about 4.5 percent during this decade. Unfortunately, we have not been able to

locate data on the ages of vehicles when scrapped; so it is not possible to directly relate scrappage rates to average vehicle age. Generally, one would assume that the preponderance of scrapped vehicles are older; but even a relatively a new vehicle may be involved in a crash that results in it being scrapped.

**Table B-4. Median age of vehicles operating in the U.S. (in years)**

| Year | Autos | Trucks |
|---|---|---|
| 2000 | 8.3 | 6.9 |
| 1999 | 8.3 | 7.2 |
| 1998 | 8.3 | 7.6 |
| 1997 | 8.1 | 7.8 |
| 1996 | 7.9 | 7.7 |
| 1995 | 7.7 | 7.6 |
| 1994 | 7.5 | 7.5 |
| 1993 | 7.3 | 7.5 |
| 1992 | 7.0 | 7.2 |
| 1991 | 6.7 | 6.8 |
| 1990 | 6.5 | 6.5 |
| 1985 | 6.9 | 7.6 |
| 1980 | 6.0 | 6.3 |
| 1975 | 5.4 | 5.8 |
| 1970 | 4.9 | 5.9 |

SOURCE: R.L. Polk and Co., as cited in BTS (2001, Table 1-22).

Table B-5 presents a rough forecast of new auto and truck sales, as well as the numbers of autos and trucks to be scrapped, for the years 2005–2025. We must stress that this forecast ignores economic cycles (which are nearly impossible to forecast beyond a few quarters), and that no attempt is made to speculate on the extent to which consumer preferences will change with regard to the mix of auto

and light truck sales. In short, the forecast in Table B-5 assumes that current trends will continue.

**Table B-5. Rough estimate of new vehicle sales and scrappage, 2005–2025 (millions of units)**

| Year | New auto sales | Autos scrapped | New truck sales | Trucks scrapped |
|---|---|---|---|---|
| 2005 | 8.5 | 8.0 | 9.0 | 6.2 |
| 2010 | 8.5 | 8.0 | 8.8 | 6.1 |
| 2015 | 9.0 | 8.5 | 9.1 | 6.2 |
| 2020 | 9.0 | 8.5 | 9.2 | 6.3 |
| 2025 | 9.0 | 8.5 | 9.2 | 6.3 |

For purposes of illustration, let us assume that all new vehicles sold in 2005 and later will be equipped with the on-board computer necessary to implement the new approach to assessing road user charges. Based on the sales and scrappage figures in Table B-5, in Table B-6 we present estimates for the total numbers of autos in the fleet, the percentage of vehicles sold in 2005 or later years, the resulting number of autos equipped with the on-board computer, and the number of autos not so equipped.

There are two important assumptions contained in the values displayed in Table B-6:

- Of the autos operating on public roadways, 66.6 percent will be over five years old, 37.3 percent will be over 10 years old, 16.8 percent will be over 15 years old, and 5.6 percent will be over 20 years old. These values were derived from Schmoyer (2000, as cited in Davis 2000, Table 6.9), who has estimated survival rates over a 30-year time frame for 1990-model-year vehicles. If anything, his rates are a bit pessimistic for our purposes because autos generally are more durable today than they were in 1990.
- The nearly constant figures for new auto sales and scrappage in Table B-5 will apply.

The rough forecast in Table B-6 implies that if, beginning in 2005, all new autos sold were equipped with the on-board computer necessary to implement the new approach, by 2015 almost two-thirds of the autos in operation would be so equipped; by 2025 almost 95 percent of autos would be capable of supporting the new approach. While we stress that this forecast is only an approximation, it is important to remember that even sophisticated forecasts seldom are very precise beyond a few years into the future. The purpose of the forecast is not to provide

definitive figures on future auto sales or scrappage rates but rather to illustrate a plausible rate at which the auto fleet would become equipped with on-board computers if new autos sold beginning in 2005 featured these computers.

**Table B-6. Rough forecasts of autos in use and autos sold, 2005–2025 (millions of units)**

| Year | Total autos in use | Percent autos year 2005 or newer | Number of autos year 2005 or newer | Number of autos year 2004 or older |
|---|---|---|---|---|
| 2005 | 130.2 | 6.5 | 8.5 | 121.7 |
| 2010 | 130.7 | 33.4 | 43.7 | 87.0 |
| 2015 | 131.2 | 62.7 | 82.3 | 48.9 |
| 2020 | 131.7 | 83.2 | 109.6 | 22.1 |
| 2025 | 132.2 | 94.4 | 124.8 | 7.4 |

Table B-7 provides an analogous forecast for trucks. The vehicle survival data from Schmoyer (2000, as cited in Davis 2000, Table 6.10) are for light trucks; and because no specific data are available for heavy trucks, we use the same rates for them. Given that 86.2 percent of all trucks are personal vehicles (Davis 2000, Table 6.4), this generalization is not likely to introduce significant error. Based on our earlier discussion of the comparatively frequent turnover of heavy truck power units by TL freight firms, however, high-mileage units probably are operated by these firms for shorter durations. Quite likely, these units subsequently are sold to lower-mileage users, such as construction firms and farmers, and are thus kept in use longer.

Of the trucks operating on public roadways, 68.7 percent will be over five years old, 41.2 percent will be over 10 years old, 21.0 percent will be over 15 years old, and 8.4 percent will be over 20 years old. To forecast the total trucks in use, we applied an average 3.6 percent annual growth rate, which is conservative relative to the 4.4 percent annual growth rate observed in the 1990s. Our reasoning is that the precipitous growth in light trucks of that decade is unlikely to continue at the same rate. Nonetheless, the 3.6 percent annual growth rate does imply a major growth in trucks, more than doubling the total number from 2005 to 2025.

### Vehicle Replacement Rate Summary

The purpose of this analysis has been to estimate the rate at which autos and trucks are likely to turnover. This rate is important to phasing in the new approach to assessing road user charges because it gives an indication of how quickly the vehicle fleet would enable the states to convert to the new approach. Using the best

available data, we have generated estimates of new vehicle sales and scrappage rates, which allow the growth of the fleet to be estimated. Using vehicle survival data by vehicle age, we have estimated the percentage of new vehicles that would be sold after a designated year, in this case 2005. We conclude that in the 20 years following implementation of the new approach (when new vehicles would begin to be equipped with the necessary on-board computer system), the percentage of vehicles so equipped would steadily rise. By the twentieth year, about 95 percent of autos and 91 percent of trucks would be capable of supporting the new approach.

**Table B-7. Rough forecasts of trucks in use and trucks sold, 2005–2025 (millions of units)**

| Year | Total trucks in use | Percent trucks year 2005 or newer | Number of trucks year 2005 or newer | Number of trucks year 2004 or older |
|---|---|---|---|---|
| 2005 | 85.6 | 10.2 | 8.7 | 76.9 |
| 2010 | 102.7 | 31.3 | 2.1 | 70.6 |
| 2015 | 123.1 | 58.8 | 72.4 | 50.7 |
| 2020 | 147.6 | 79.0 | 166.6 | 19.0 |
| 2025 | 177.0 | 91.4 | 161.8 | 15.2 |

## PHASE-IN POLICY ISSUES

The foregoing analysis suggests that if the appropriate on-board equipment were to be included in all motor vehicles manufactured after some date, a growing number of vehicles would be capable of supporting the new approach to assessing road user charges, reaching over 90 percent within 20 years. A public policy question thus emerges: at what point should conventional vehicles powered by engines that burn gasoline or diesel fuel be assessed user charges via the new approach in lieu of motor fuel taxes?

### Charging Conventional Fuel-Burning Vehicles

At least three different policy directions could be taken with regard to transitioning from the motor fuel tax to the new approach, including:

- Apply the new approach only to vehicles powered by alternatives to traditional gasoline- or diesel fuel-burning internal-combustion engines.
- As new vehicles, however they are powered, are manufactured with the on-board equipment needed to support the new approach, assess user charges to them using the new approach.

- Charge vehicles powered by alternative propulsion systems using the new approach, and wait until a large enough proportion of gasoline- and diesel-powered vehicles have the necessary on-board equipment before switching them to the new approach.

To be sure, the most pressing issue related to phasing in the new approach as it applies to conventional gasoline- and diesel-powered vehicles is how to handle the payment of the motor fuel tax. On the one hand, it would be grossly unfair for conventional vehicles to pay both the fuel tax and a per-mile user charge. On the other hand, care must be taken to prevent fraudulent non-payment of the motor fuel tax by operators of conventional vehicles. This implies that as the new approach is phased in, it will be essential for the refueling pump to be able to positively identify those vehicles that are being assessed per-mile user charges via the new approach.

We recommend that the third policy direction above be taken. As time passes and an increasing proportion of refueling pumps become equipped with the necessary features to make the needed positive identification, it will make sense to move to widespread implementation of the new approach. Until then, vehicles with alternative propulsion systems can be assessed user charges via the new approach, using the procedures discussed in Chapter 6.

At some point in the future (e.g., 20 years after all new vehicles are equipped), states could completely phase out motor fuel taxes. Owners of the comparatively few remaining older, unequipped vehicles could be asked to indicate the odometer reading annually at the time the vehicle's registration is renewed. While it is likely that some owners of these older vehicles would understate the mileage traveled by their vehicles during the previous year, a relatively small number of vehicles would be involved. Coupled with the general tendency for older vehicles to be driven comparatively few miles, the loss in revenue probably would not be substantial.

**Identifying Conventional Vehicles with On-Board Equipment**

More research is needed on how best to make the positive identification at the refueling pump as to which vehicles are being assessed road user charges with the new approach. One option is for a small sensor on the pump nozzle to make contact with a sensor near the vehicle's refueling receptacle. The vehicle's sensor would be tied into the on-board computer. As noted above, it would be essential for the vehicle/refueling pump communication to be sufficiently secure and reliable to avoid fraudulent non-payment of motor fuel taxes. The refueling pump, for example, could be tied into the collection center, which could validate the vehicle identification number and confirm that the vehicle is being assessed road user charges via in the new approach.

We have shown that an extended period of time will be needed for over 90 percent of all operational vehicles to feature the on-board equipment necessary for road user charges to be assessed with the new approach. Thus, it is realistic to suppose that the new approach will need to operate side by side with the motor fuel tax for a number of years. A corollary is that it will take many years for the vast majority of

refueling pumps to be equipped with the type of sensor just discussed, just as the gradual switch to pay-at-the-pump technology has. It will be important to make reasonable provisions for operators of vehicles participating in the new approach who must purchase fuel at refueling stations unable to discern whether or not the vehicle should be assessed the motor fuel tax.

One possible way to address the issue of appropriate payment of the motor fuel tax is for vehicles that feature the on-board equipment needed to support the new approach to have a simple fuel-flow meter incorporated into their refueling receptacle and tied into the on-board computer. The on-board computer would thus have information as to (1) the number of gallons of fuel transferred and (2) the polygon in which the fuel was purchased. A small data file stored in the on-board computer could contain the applicable motor fuel tax rates for all jurisdictions. Through a simple computation, the on-board computer could store a credit for road user charges (i.e., fuel taxes) paid. This credit would be applied against the total per-mile user charge due to that jurisdiction.

In the event that such a vehicle were to purchase fuel in one jurisdiction but travel few miles there and many more in other jurisdictions, it would be possible to have a negative balance owed to the jurisdiction where the fuel was purchased. The collection center could easily resolve this circumstance by in effect transferring revenue from one jurisdiction to another, not unlike interstate fuel tax pay-back agreements that are now in place with respect to heavy vehicles.

The main point to be made is that there are possible solutions to the problem of ensuring fairness in motor fuel tax payments as a growing proportion of the vehicles in operation become equipped with the features necessary to support the new approach. It is essential that both the vehicle operator and the states in which travel has occurred be treated fairly, and the methods just discussed is among the possible means for ensuring that is the case.

**REFERENCES**

*Automotive News*. 2001. *2001 Market Data Book*. Available at http://www.autonews.com

Bureau of Transportation Statistics (BTS). 2001. *National Transportation Statistics*. BTS01-01. U.S. Department of Transportation. Washington, DC: U.S. Government Printing Office.

Davis, Stacy C. 2000. *Transportation Energy Data Book: Edition 20*. Oak Ridge, TN: Oak Ridge National Laboratory for the U.S. Department of Energy.

Schmoyer, Richard L. 2000. Unpublished study on scrappage rates. Oak Ridge, TN: Oak Ridge National Laboratory.

U.S. Census Bureau. 1999. *Statistical Abstract of the United States: 1999*. (119th edition). Washington, DC.

# APPENDIX C
# SECURITY, PRIVACY, AND ROBUSTNESS REQUIREMENTS

Given the important privacy considerations related to the new approach to assessing road user charges and the large amounts of revenue at stake for various levels of government, the system will need to meet stringent privacy, security, and robustness standards. This appendix builds on Chapter 5 to set forth a set of security, privacy and robustness requirements for the new approach and to specify a preliminary privacy/security architecture that demonstrates the technical feasibility of meeting these requirements. This architecture defines basic security and privacy mechanisms that should be incorporated into the design and implementation of the system to ensure integrity and robustness and to provide adequate protection of personal information.

The term security as it is used here relates to protection against threats (both malicious and accidental) to intended system operation. Of particular concern are potential attempts to subvert or defraud the system to avoid payment of charges or to disrupt the overall ability of the system to function effectively. As explained in Chapter 5, the central security issues for the new approach to assessing road user charges are as follows:

- Protection against deliberate or accidental tampering with the accurate collection, processing, and storage of road-use data by the on-board system, ranging from efforts to disable or falsify GPS/GIS data to complete disablement of the system.
- Protection against reporting (uploading) of altered or fraudulent data or efforts to prevent the reporting of data.
- Resistance to “hacking” attacks intended to disrupt system operation.

In this appendix, we address the first two of these issues. It is not intended to minimize the importance of hacking and large-scale cyber-attacks as significant security threats. Indeed, the new approach to assessing road user charges must expect to be an irresistible target for a wide range of attacks intended to disrupt its operation; and, without proper safeguards, such attacks could seriously undermine the effectiveness of the system. However, the nature of this type of threat is quite different from that of efforts aimed at fraud or avoidance of payment.

Privacy in this context relates to minimizing the potential that the new approach to assessing road user charges in collecting potentially sensitive personal information could be used for purposes other than road user charge assessment. System requirements associated with privacy include:

- prevention of unauthorized access to user data stored in the on-board system,
- prevention of eavesdropping by third parties during uploading of data, and
- minimization of the extent to which collected data could be related to specific events or to the actions of an individual user (e.g., to place a user at a specific location at a specific time).

Finally, robustness relates to the overall reliability of the system and its resistance to various malfunction and/or failure scenarios. Clearly robustness and security issues have considerable overlap because various types of deliberate attempts at system disablement must be considered as potential threats against system integrity. Sometimes the same mechanisms can be used to guard against both deliberate and accidental threats. Robustness concerns, however, extend beyond the realm of security to include component or subsystem failures.

## REQUIREMENTS

As in any complex system design activity, it is prudent to begin by stating security/privacy/reliability issues as a set of specific requirements that must be individually and collectively addressed during system development. The requirements listed below constitute only the subset of overall system requirements that are derived directly from security, privacy, and robustness considerations. It must be noted that many other requirements among the broader set of overall system requirements will have some additional bearing on these areas.

### Security Requirements

There are 12 basic and essential requirements to adequately protect the security of the on-board data processing and storage necessary for the new approach to function properly:

- **S1.** Each vehicle participating in the new approach to assessing road user charges shall be uniquely identified by a non-forgeable identifier that can be tied to its current vehicle registration. This identifier shall provide a verifiable means of associating reported charges with a particular registered vehicle.
- **S2.** The on-board system shall be designed and packaged to be resistant to tampering that would reveal any closely held internal information (e.g., private encryption keys) and to prevent modification or subversion of any processing algorithms or stored data.
- **S3.** There shall be no secret information resident in the on-board system of a vehicle that could, if compromised via tampering or reverse engineering, be useful for any breach of system security extending beyond corruption of usage data for that vehicle.
- **S4.** All data collected and reported by the system shall be corroborated via an independent, tamper-resistant odometer reading.

- **S5.** The on-board system shall detect the accidental or purposeful disablement of GPS signal reception and report this to the collection center. During any such disablement, the on-board system shall continue to collect and report odometer-based data.
- **S6.** All data reported to the collection center shall be protected from tampering or alteration by any outside entity during the upload process.
- **S7.** It shall not be possible for any outside entity (i.e., any entity other than the authorized on-board system of a vehicle) to fraudulently report data on behalf of a vehicle.
- **S8.** In the event of temporary disruption of data-reporting mechanisms, the on-board system shall retain collected data until it can be successfully uploaded.
- **S9.** Temporary disruption of data-reporting mechanisms should not result in the loss of reported data, or the duplicate reporting of data, in a manner that is undetectable by the collection center.
- **S10.** The collection center shall detect any temporary disablement or failure of the on-board system that results in gaps in collected data.
- **S11.** The collection center shall detect the long-term disablement or failure of an in-vehicle system manifested by an absence of reported data.
- **S12.** The on-board system shall be able to validate the source and integrity of any information downloaded to the vehicle (e.g., rate schedule updates).

**Robustness Requirements**

To ensure system robustness, there are three key requirements:

- **R1.** The on-board system shall retain stored data through temporary loss of system power (e.g., due to disconnection of the power source).
- **R2.** The on-board system should detect any internal malfunction manifested by an unacceptable discrepancy between reported GPS/GIS data versus independent odometer data and report this malfunction to the user through some sort of in-vehicle indication.
- **R3.** The on-board system should detect malfunction of its data-reporting (upload) subsystem as manifested by inability to successfully report collected data and report this malfunction to the user through an in-vehicle indication.

**Additional Data Storage and Communication Requirements**

Four additional requirements further address data storage on board the vehicle and communication between the vehicle and the collection center:

- **P1.** Collected and reported usage data shall be maintained only at the minimum level of detail required for the assessment of road user charges.

- **P2.** Data stored in the on-board system shall be protected from access by any outside entity other than the authorized collection center.
- **P3.** During reporting (upload) to the collection center, user data shall be protected from all forms of external eavesdropping.
- **P4.** Users (vehicles) should be protected from theft-of-identity (i.e., ploys to fraudulently misdirect road use charges to another user).

## SYSTEM ARCHITECTURE

The security and privacy architecture should employ a combination of public-key (asymmetric) and secret, private-key (symmetric) encryption techniques to validate the source and authenticity of data. Non-forgeable vehicle identification (requirement S1) and secure reporting of data (requirements S6, S7) can be achieved via the use of an asymmetric encryption technique such as the Rivest-Shamir-Adleman (RSA) algorithm (Rivest 1978). Public-key encryption utilizes a privately held, secret key and a corresponding public key that is derived from the private key via a "one-way" function (Stinson 1995). Because the private key cannot be computed from the public key, the public key can be freely distributed without compromising the private key. A message encrypted using the public key can only be decrypted by the holder of the private key. Conversely, a message encrypted using the private key can be decrypted by any entity using the public key. Public-key encryption can be used both to protect the privacy of data and to validate the source and integrity of data.

Each manufactured on-board computer will be assigned a deeply embedded private key. As per requirement S2, the on-board system should be designed so as to make it prohibitively expensive for an external entity to discover the identity of this key. This could be done, for instance, by "burning" the key into an integrated circuit chip at the time of manufacture. It is not necessary to ensure that it would be completely impossible to discover the identity of this private key, only that the cost and complexity of doing so would be considerable. The corresponding public key will serve as the publicly known identifier for the on-board computer, and ultimately for the vehicle in which the computer is installed. Once the public key has been determined, no external record of any type should be maintained of the private key's identity. At the time of vehicle registration, the public key of the on-board system will be registered with the collection center. This key will serve as the unique, non-forgeable identifier for the vehicle (requirements S1, P4). Because the private key is the only piece of secret data held in the on-board computer (the encryption algorithms themselves do not need to be secretly held), reverse-engineering of an on-board computer could at most breach the security of transactions involving a single vehicle. Hence, requirement S3 is met.

All message transmissions from the vehicle to the collection center or any other external entity by the on-board computer should be digitally "signed" using the on-board computer's private key. The digital signature process will work as follows: The on-board computer will format the plain text (unencrypted message), including

its public key, to announce its identity to the collection center. The on-board computer will then digitally sign the message using its private key. The digital signature technique involves computing a "hash function" of the plain text message and then encrypting this hash function value using the private key (Stinson 1995, Stallings 1999). This encrypted hash value is appended to the transmitted message as a signature. The collection center will decrypt the received signature using the sender's public key and compare it to a locally computed hash function of the plain text message. Note that a match between the locally computed hash value and the one obtained from the decrypted signature ensures both the identity of the sender (because only the holder of the private key could have encrypted the signature) and the integrity of the message (because any modification to the message would have altered the computed hash value and resulted in a mismatch with the signature). This addresses requirements S6 and S7.

The digital signature technique itself does not provide any protection from external eavesdropping because the message body is in plain text form. To provide privacy of uploaded data (requirement P3), an additional encryption step is needed. Note that the on-board computer's private key is of no use for this operation. A complementary scheme can be used, however, wherein the collection center maintains its own private key and advertises a corresponding public key for use by on-board computers. On-board computers can then utilize the collection center's public key to encrypt messages prior to upload. Once encrypted, these messages can be decrypted only by the collection center and hence cannot be eavesdropped upon by any other entity. The on-board computer will first sign messages using its private key and then encrypt them using the collection center's private key.

The encryption scheme described above has two shortcomings: First, the computational complexity of public key encryption is quite high (several orders of magnitude higher than standard secret-key encryption/decryption schemes). Second, breaking the private key of the collection center would allow a malicious entity to eavesdrop on data uploads by any vehicle, making the breaking of this encryption key a potentially high-value target. The first concern is particularly problematic because the processing power of the on-board computer will necessarily be limited.

To mitigate both of these problems, we propose an alternative encryption architecture. Specifically, the collection center should use public-key encryption only for the purpose of disseminating unique, temporary, symmetric encryption keys to on-board systems (Adams 1997). These keys will be randomly generated by the collection center and will be valid for a limited time duration (e.g., a week). All protected uploads and downloads between the on-board computer and the collection center will utilize an efficient symmetric encryption scheme based upon these temporary keys. An on-board computer can request a new temporary key at any time via a simple dialogue with the collection center. Because the secure distribution of these temporary keys could utilize asymmetric encryption using the on-board computer's public key, there will be no globally vulnerable keys to worry about. Also, because the temporary key stored in an on-board computer will be

valid only for data transfer to and from that particular computer, requirement S3 is maintained.

However, in order for the on-board computer to authenticate and validate key dissemination messages from the collection center, a signature mechanism is needed. A public-key system should be used for this purpose. Specifically, the collection center should maintain a private signature key with a corresponding public key known to computers on board vehicles. This public key can be made available via a standard trusted certificate server like those commonly used in Internet security applications. This will permit the collection center to change its private key periodically to devalue attempts to acquire this key. The collection center can use this private key to sign messages exactly as described earlier for the on-board computers.

A further optimization is possible to reduce the overhead of message signature. Once symmetric, secret keys are established between an on-board computer and the collection center. These keys can be used for both digital signature (using a Message Authentication Code (MAC) technique that is both more computationally efficient and more secure than RSA-based digital signature) and encryption (Davies 1989). Thus, signature and encryption using asymmetric keys would be necessary only for purposes of disseminating temporary private keys.

**Data Upload Protocols**

The integrity of data upload from a vehicle's on-board computer to the collection center must be maintained despite a variety of communications-related problems. Requirements S8 and S9 speak to the need for reliable and accurate data upload. Because data transfers are subject to interruption at any time, the system must carefully guard against the possible loss or corruption of data due to a loss of connectivity during the upload process. Equally problematic would be the acceptance of duplicate data by the collection center resulting in an overcharge.

Internet protocols almost certainly will be used as the basis for the data communications infrastructure of the new system because developing an alternative infrastructure would be prohibitively expensive and time consuming. Because the transport layer, TCP, of the Internet provides reliable, sequenced message delivery, it is tempting to assume that all reliability issues related to data upload can be solved simply by utilizing TCP services. Unfortunately, this is a false hope for two reasons (Tanenbaum 1996): (1) TCP services do not tolerate the loss of the transport connection that potentially could occur, and (2) TCP is not designed to operate in the presence of non-robust links.

For the reasons noted above, it is advisable to utilize connectionless (UDP) service for all data uploads. This means that data destined for upload from the on-board computer to the collection center must be formatted into individual packets, which are then separately given to the network layer for delivery to the collection center. Each of these packets is independently subject to loss or corruption in the network.

A robust protocol is needed to invoke the retransmission of messages that fail to successfully reach the collection center.

A fairly straightforward Automatic Repeat Request (ARQ) protocol can be used for this purpose (Tanenbaum 1996). Such protocols are widely used in data communications applications. Each packet sent by the on-board computer should be identified by a unique "sequence number" that differentiates the packet from any other packet generated by a given on-board computer. Upon successful receipt of a packet, the collection center should respond with a positive acknowledgment (ACK) specifying the sequence number of the received packet. The on-board computer must retain a copy of any transmitted packet until a positive acknowledgment is received.

While the above protocol is somewhat unsophisticated, it is highly robust in dealing with all types of network disruptions. However, there are several special considerations in applying the ARQ protocol to this application. First, special care must be taken in determining the sequence numbers used to identify data packets. In typical ARQ applications, packet numbers are sequentially generated from some form of counter. If the sender experiences a temporary outage or software crash, the counter must sometimes be initialized to some pseudo-random initial value, resulting in a gap in the sequential numbering. In this application, it is important that sequential numbering never be lost so that the collection center can always identify gaps in reported data (requirement S10). This requires that special consideration be taken in design of the sequence numbering mechanisms used by the on-board system. A simple solution would be to record sequence numbers to nonvolatile storage.

A second consideration is the unbounded nature of the upload protocol. In fact, the problem of insuring reliable upload of data is an instance of the "Two Generals Problem" (Gray 1979), which is proven to have no bounded solution. What this theoretical result means in practical terms is that while it can be assured that any packet will eventually be successfully uploaded, the amount of time required for successful upload cannot be bounded. Therefore, under extended periods of particularly harsh link conditions, the on-board system might need to retain data packets for an arbitrarily long period of time (requirement S8). Because new data is continuously being accrued and on-board storage capacity is necessarily limited, there is a limit to the capacity of the on-board system to tolerate disruptions in the data upload process. There is no magic solution to this problem other than to provide as much storage as is feasible in the on-board computer, to use this storage as efficiently as possible, and to manage the data upload process so as to take maximum advantage of favorable link conditions. In the event that data is lost due to exhaustion of on-board storage, the system design must ensure that the collection center will always be aware of this fact (requirement S10). This is easily accommodated in the upload protocols by including a provision for the reporting of "lost" packets.

### Additional Architectural Considerations

Requirements S5, R2, and R3 dictate that the on-board system architecture must possess the ability to detect subsystem failures affecting the GPS receiver, the independent odometer, and the data-reporting subsystem (smart card link). A detected malfunction should be reported to the vehicle user through some form of in-vehicle indication. This serves two purposes: (1) to alert the user to seek system repair in the case of a non-malicious failure and (2) in the case of a deliberate disablement of a subsystem, to warn the user that the disablement has been detected.

The detection of subsystem malfunctions is, for the most part, straightforward. Loss of signals from GPS satellites should be detectable within the GPS/GIS subsystem itself. Other forms of GIS/GPS or odometer malfunction can be detected by monitoring any discrepancies between vehicle mileage data reported by the two subsystems. Malfunction or disablement of the data-reporting (upload) subsystem can be detected by failure to successfully upload data over a given time interval. This interval should be chosen to minimize false alarms due to external network unavailability but should be short enough to avoid substantial loss of data. The collection center can easily detect disablement or malfunction of the on-board system (as per requirements S10, S11) through anomalies in reported data or long-term absence of reporting activity.

Requirement R1 dictates that all collected data resident in the on-board system be stored in some form of non-volatile storage to protect it from failure scenarios involving loss of power to the on-board system. This may pose a severe restriction because non-volatile read/write storage (e.g., flash memory) is slower, less dense, and more costly that regular (volatile) dynamic random-access memory (RAM). This issue requires further study and experimentation. An alternative approach would be to relax requirement R1 to permit limited loss of data in loss-of-power situations.

## CONCLUSIONS

This appendix has defined a set of security, privacy, and robustness requirements for the new approach to assessing road user charges and outlined architectural approaches to address them. The requirements dictate secure storage and reporting of data while preventing unauthorized eavesdropping. They further dictate that the on-board system of any vehicle not hold any secret keys, algorithms, or other information that, if compromised, could be used for any purpose beyond reporting the data for that specific vehicle. Central to meeting these requirements is the use of modern, public-key cryptography, with a unique private key deeply embedded in each on-board computer at the time of manufacture. This secret key will allow authentication and validation of all data uploads from a vehicle using digital signature techniques and will also permit secure download of temporary encryption keys for efficient encryption of data to ensure privacy from eavesdropping.

Several additional security, privacy, and robustness issues have been addressed, including detection and reporting of subsystem malfunctions or deliberate attempts

at disablement, and temporary loss-of-power by the on-board system. In total, the proposed architectural features demonstrate the feasibility of addressing system security, privacy, and robustness requirements using straightforward and proven approaches. The overall conclusion is that these issues should not pose any fundamental obstacles to the successful deployment of the new approach to assessing road user charges.

**REFERENCES**


Adams, C. 1997. "Constructing Symmetric Ciphers Using the CAST Design Procedure." *Designs, Codes and Cryptography*, Vol. 12, No 3 (November), pp. 283–316.

Davies, D., and W. Price. 1989. *Security for Computer Networks*. New York, NY: John Wiley and Sons.

Gray, Jim. 1978. "Notes on Data Base Operating Systems." Operating Systems, An Advanced Course*, Lecture Notes in Computer Science*, Vol. 60. Heidelberg, Germany: Springer Verlag, pp. 393–481.

Rivest, R.L., A. Shamir, and A. Adleman. 1978. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." *Communications of the ACM*, Volume 21, No. 2, pp. 120–126.

Stallings, Wiliam. 1999. *Cryptography and Network Security—Principles and Practice*. Englewood Cliffs, NJ: Prentice Hall.

Stinson, Douglas. 1995. *Cryptography, Theory and Practice*. Boca Raton, FL: CRC Press.

Tanenbaum, Andrew. 1996. *Communication Networks*. Englewood Cliffs, NJ: Prentice Hall.

available data, we have generated estimates of new vehicle sales and scrappage rates, which allow the growth of the fleet to be estimated. Using vehicle survival data by vehicle age, we have estimated the percentage of new vehicles that would be sold after a designated year, in this case 2005. We conclude that in the 20 years following implementation of the new approach (when new vehicles would begin to be equipped with the necessary on-board computer system), the percentage of vehicles so equipped would steadily rise. By the twentieth year, about 95 percent of autos and 91 percent of trucks would be capable of supporting the new approach.

**Table B-7. Rough forecasts of trucks in use and trucks sold, 2005–2025 (millions of units)**

| Year | Total trucks in use | Percent trucks year 2005 or newer | Number of trucks year 2005 or newer | Number of trucks year 2004 or older |
|---|---|---|---|---|
| 2005 | 85.6 | 10.2 | 8.7 | 76.9 |
| 2010 | 102.7 | 31.3 | 2.1 | 70.6 |
| 2015 | 123.1 | 58.8 | 72.4 | 50.7 |
| 2020 | 147.6 | 79.0 | 166.6 | 19.0 |
| 2025 | 177.0 | 91.4 | 161.8 | 15.2 |

## PHASE-IN POLICY ISSUES

The foregoing analysis suggests that if the appropriate on-board equipment were to be included in all motor vehicles manufactured after some date, a growing number of vehicles would be capable of supporting the new approach to assessing road user charges, reaching over 90 percent within 20 years. A public policy question thus emerges: at what point should conventional vehicles powered by engines that burn gasoline or diesel fuel be assessed user charges via the new approach in lieu of motor fuel taxes?

At least three different policy directions could be taken with regard to transitioning from the motor fuel tax to the new approach, including:

- Apply the new approach only to vehicles powered by alternatives to traditional gasoline- or diesel fuel-burning internal-combustion engines.
- As new vehicles, however they are powered, are manufactured with the on-board equipment needed to support the new approach, assess user charges to them using the new approach.

- Charge vehicles powered by alternative propulsion systems using the new approach, and wait until a large enough proportion of gasoline- and diesel-powered vehicles have the necessary on-board equipment before switching them to the new approach.

### Charging Conventional Fuel-Burning Vehicles

To be sure, the most pressing issue related to phasing in the new approach as it applies to conventional gasoline- and diesel-powered vehicles is how to handle the payment of the motor fuel tax. On the one hand, it would be grossly unfair for conventional vehicles to pay both the fuel tax and a per-mile user charge. On the other hand, care must be taken to prevent fraudulent non-payment of the motor fuel tax by operators of conventional vehicles. This implies that as the new approach is phased in, it will be essential for the refueling pump to be able to positively identify those vehicles that are being assessed per-mile user charges via the new approach.

We recommend that the third policy direction above be taken. As time passes and an increasing proportion of refueling pumps become equipped with the necessary features to make the needed positive identification, it will make sense to move to widespread implementation of the new approach. Until then, vehicles with alternative propulsion systems can be assessed user charges via the new approach, using the procedures discussed in Chapter 6.

At some point in the future (e.g., 20 years after all new vehicles are equipped), states could completely phase out motor fuel taxes. Owners of the comparatively few remaining older, unequipped vehicles could be asked to indicate the odometer reading annually at the time the vehicle's registration is renewed. While it is possible that some owners of these older vehicles would understate the mileage traveled by their vehicles during the previous year, a relatively small number of vehicles would be involved. Coupled with the general tendency for older vehicles to be driven comparatively few miles, the loss in revenue probably would not be substantial.

### Identifying Conventional Vehicles with On-Board Equipment

More research is needed on how best to make a positive identification at the refueling pump as to which vehicles are being assessed road user charges with the new approach. One option is for a small sensor on the pump nozzle to make contact with a sensor near the vehicle's refueling receptacle. The vehicle's sensor would be tied into the on-board computer. As noted above, it would be essential for the vehicle/refueling pump communication to be sufficiently secure and reliable to avoid fraudulent non-payment of motor fuel taxes. The refueling pump, for example, could be tied into the collection center, which could validate the vehicle identification number and confirm that the vehicle is being assessed road user charges via in the new approach.

We have shown that an extended period of time will be needed for over 90 percent of all operational vehicles to feature the on-board equipment necessary for road

user charges to be assessed with the new approach. Thus, it is realistic to suppose that the new approach will need to operate side by side with the motor fuel tax for a number of years. A corollary is that it will take many years for the vast majority of refueling pumps to be equipped with the type of sensor just discussed, just as the gradual switch to pay-at-the-pump technology has. It will be important to make reasonable provisions for operators of vehicles participating in the new approach who must purchase fuel at refueling stations unable to discern whether or not the vehicle should be assessed the motor fuel tax.

**Fuel-flow meter.** One possible way to address the issue of appropriate payment of the motor fuel tax is for vehicles that feature the on-board equipment needed to support the new approach to have a simple in-vehicle system to monitor fuel intake during refueling. This system could consist of a fuel-flow meter incorporated into the vehicle's refueling receptacle and tied into the on-board computer or a digital level sensor in the fuel tank. (Many vehicles manufactured in recent years already have the ability to measure fuel intake.) The on-board computer would thus have information as to (1) the number of gallons of fuel transferred and (2) the polygon in which the fuel was purchased. A small data file stored in the on-board computer could contain the applicable motor fuel tax rates for all jurisdictions. Through a simple computation, the on-board computer could store a credit for road user charges (i.e., motor fuel taxes) paid. This credit would be applied against the total per-mile user charge due to that jurisdiction.

In the event that such a vehicle were to purchase fuel in one jurisdiction but travel few miles there and many more in other jurisdictions, it would be possible to have a negative balance owed to the jurisdiction where the fuel was purchased. The collection center could easily resolve this circumstance by in effect transferring revenue from one jurisdiction to another, not unlike interstate fuel tax pay-back agreements that are now in place with respect to heavy vehicles.

**Pump-based identifier.** An alternative solution to the phase-in problem would be to equip service stations that have old pumps with a simple device into which the smart card of a vehicle equipped to support the new approach could be inserted during payment. This device would validate the smart card and permit subtraction by the on-board computer of the motor fuel taxes assessed at the pump from the payment due. In this way, all road-use charges of vehicles equipped for the new approach would be assessed and apportioned correctly. The complexity of the device required at non-equipped service stations would be modest. There are, however, some potential security issues that must be addressed with regard to such a mechanism. For instance, it is possible that a customer might present the smart card taken from a vehicle that is equipped to support the new approach while paying for fuel purchased for a non-equipped vehicle in order to evade payment of motor fuel taxes.

This problem can be mitigated by attaching a very simple passive ID chip (like the ones used in card-based door locks and pet identification implants) to the nozzle of the pump to uniquely identify each non-equipped service station. This passive device could be easily attached to the pump nozzle, would cost only a few cents

per pump, and would require no wiring or other infrastructure at the pump. The in-vehicle system could include a sensor to read the ID chip during the refueling operation, and the on-board computer could record this ID along with the amount of fuel transferred. When the vehicle operator pays for the fuel, the station ID and other transaction details would be transferred to the smart card. Then, when the smart card is reinserted into the vehicle, the on-board computer could verify that the service station ID and fuel amount recorded on the smart card match those recorded by the on-board computer during the refueling operation. In the event that discrepancies in excess of a reasonable error tolerance are detected by the on-board system, charges for the evaded fuel tax could be added to the user charge stored in the on-board computer for the applicable jurisdiction.

The main point to be made is that there are possible solutions to the problem of ensuring fairness in motor fuel tax payments as a growing proportion of the vehicles in operation become equipped with the equipment necessary to support the new approach. It is essential that both the vehicle operator and the states in which travel has occurred be treated fairly, and the methods just discussed are among the possible means for ensuring that is the case.

**REFERENCES**

*Automotive News*. 2001. *2001 Market Data Book*. Available at http://www.autonews.com

Bureau of Transportation Statistics (BTS). 2001. *National Transportation Statistics*. BTS01-01. U.S. Department of Transportation. Washington, DC: U.S. Government Printing Office.

Davis, Stacy C. 2000. *Transportation Energy Data Book: Edition 20*. Oak Ridge, TN: Oak Ridge National Laboratory for the U.S. Department of Energy.

Schmoyer, Richard L. 2000. Unpublished study on scrappage rates. Oak Ridge, TN: Oak Ridge National Laboratory.

U.S. Census Bureau. 1999. *Statistical Abstract of the United States: 1999*. (119th edition). Washington, DC.

# APPENDIX C
# SECURITY, PRIVACY, AND ROBUSTNESS REQUIREMENTS

Given the important privacy considerations related to the new approach to assessing road user charges and the large amounts of revenue at stake for various levels of government, the system will need to meet stringent privacy, security, and robustness standards. This appendix builds on Chapter 5 to set forth a set of security, privacy and robustness requirements for the new approach and to specify a preliminary privacy/security architecture that demonstrates the technical feasibility of meeting these requirements. This architecture defines basic security and privacy mechanisms that should be incorporated into the design and implementation of the system to ensure integrity and robustness and to provide adequate protection of personal information.

The term security as it is used here relates to protection against threats (both malicious and accidental) to intended system operation. Of particular concern are potential attempts to subvert or defraud the system to avoid payment of charges or to disrupt the overall ability of the system to function effectively. As explained in Chapter 5, the central security issues for the new approach to assessing road user charges are as follows:

- Protection against deliberate or accidental tampering with the accurate collection, processing, and storage of road-use data by the on-board system, ranging from efforts to disable or falsify GPS/GIS data to complete disablement of the system.
- Protection against reporting (uploading) of altered or fraudulent data or efforts to prevent the reporting of data.
- Resistance to “hacking” attacks intended to disrupt system operation.

In this appendix, we address the first two of these issues. It is not intended to minimize the importance of hacking and large-scale cyber-attacks as significant security threats. Indeed, the new approach to assessing road user charges must expect to be an irresistible target for a wide range of attacks intended to disrupt its operation; and, without proper safeguards, such attacks could seriously undermine the effectiveness of the system. However, the nature of this type of threat is quite different from that of efforts aimed at fraud or avoidance of payment.

Privacy in this context relates to minimizing the potential that the new approach to assessing road user charges in collecting potentially sensitive personal information could be used for purposes other than road user charge assessment. System requirements associated with privacy include:

- prevention of unauthorized access to user data stored in the on-board system,
- prevention of eavesdropping by third parties during uploading of data, and
- minimization of the extent to which collected data could be related to specific events or to the actions of an individual user (e.g., to place a user at a specific location at a specific time).

Finally, robustness relates to the overall reliability of the system and its resistance to various malfunction and/or failure scenarios. Clearly robustness and security issues have considerable overlap because various types of deliberate attempts at system disablement must be considered as potential threats against system integrity. Sometimes the same mechanisms can be used to guard against both deliberate and accidental threats. Robustness concerns, however, extend beyond the realm of security to include component or subsystem failures.

## REQUIREMENTS

As in any complex system design activity, it is prudent to begin by stating security/privacy/reliability issues as a set of specific requirements that must be individually and collectively addressed during system development. The requirements listed below constitute only the subset of overall system requirements that are derived directly from security, privacy, and robustness considerations. It must be noted that many other requirements among the broader set of overall system requirements will have some additional bearing on these areas.

### Security Requirements

There are 12 basic and essential requirements to adequately protect the security of the on-board data processing and storage necessary for the new approach to function properly:

- **S1.** Each vehicle participating in the new approach to assessing road user charges shall be uniquely identified by a non-forgeable identifier that can be tied to its current vehicle registration. This identifier shall provide a verifiable means of associating reported charges with a particular registered vehicle.
- **S2.** The on-board system shall be designed and packaged to be resistant to tampering that would reveal any closely held internal information (e.g., private encryption keys) and to prevent modification or subversion of any processing algorithms or stored data.
- **S3.** There shall be no secret information resident in the on-board system of a vehicle that could, if compromised via tampering or reverse engineering, be useful for any breach of system security extending beyond corruption of usage data for that vehicle.
- **S4.** All data collected and reported by the system shall be corroborated via an independent, tamper-resistant odometer reading.

- **S5.** The on-board system shall detect the accidental or purposeful disablement of GPS signal reception and report this to the collection center. During any such disablement, the on-board system shall continue to collect and report odometer-based data.
- **S6.** All data reported to the collection center shall be protected from tampering or alteration by any outside entity during the upload process.
- **S7.** It shall not be possible for any outside entity (i.e., any entity other than the authorized on-board system of a vehicle) to fraudulently report data on behalf of a vehicle.
- **S8.** In the event of temporary disruption of data-reporting mechanisms, the on-board system shall retain collected data until it can be successfully uploaded.
- **S9.** Temporary disruption of data-reporting mechanisms should not result in the loss of reported data, or the duplicate reporting of data, in a manner that is undetectable by the collection center.
- **S10.** The collection center shall detect any temporary disablement or failure of the on-board system that results in gaps in collected data.
- **S11.** The collection center shall detect the long-term disablement or failure of an in-vehicle system manifested by an absence of reported data.
- **S12.** The on-board system shall be able to validate the source and integrity of any information downloaded to the vehicle (e.g., rate schedule updates).

**Robustness Requirements**

To ensure system robustness, there are three key requirements:

- **R1.** The on-board system shall retain stored data through temporary loss of system power (e.g., due to disconnection of the power source).
- **R2.** The on-board system should detect any internal malfunction manifested by an unacceptable discrepancy between reported GPS/GIS data versus independent odometer data and report this malfunction to the user through some sort of in-vehicle indication.
- **R3.** The on-board system should detect malfunction of its data-reporting (upload) subsystem as manifested by inability to successfully report collected data and report this malfunction to the user through an in-vehicle indication.

**Additional Data Storage and Communication Requirements**

Four additional requirements further address data storage on board the vehicle and communication between the vehicle and the collection center:

- **P1.** Collected and reported usage data shall be maintained only at the minimum level of detail required for the assessment of road user charges.

- **P2.** Data stored in the on-board system shall be protected from access by any outside entity other than the authorized collection center.
- **P3.** During reporting (upload) to the collection center, user data shall be protected from all forms of external eavesdropping.
- **P4.** Users (vehicles) should be protected from theft-of-identity (i.e., ploys to fraudulently misdirect road use charges to another user).

## SYSTEM ARCHITECTURE

The security and privacy architecture should employ a combination of public-key (asymmetric) and secret, private-key (symmetric) encryption techniques to validate the source and authenticity of data. Non-forgeable vehicle identification (requirement S1) and secure reporting of data (requirements S6, S7) can be achieved via the use of an asymmetric encryption technique such as the Rivest-Shamir-Adleman (RSA) algorithm (Rivest 1978). Public-key encryption utilizes a privately held, secret key and a corresponding public key that is derived from the private key via a "one-way" function (Stinson 1995). Because the private key cannot be computed from the public key, the public key can be freely distributed without compromising the private key. A message encrypted using the public key can only be decrypted by the holder of the private key. Conversely, a message encrypted using the private key can be decrypted by any entity using the public key. Public-key encryption can be used both to protect the privacy of data and to validate the source and integrity of data.

Each manufactured on-board computer will be assigned a deeply embedded private key. As per requirement S2, the on-board system should be designed so as to make it prohibitively expensive for an external entity to discover the identity of this key. This could be done, for instance, by "burning" the key into an integrated circuit chip at the time of manufacture. It is not necessary to ensure that it would be completely impossible to discover the identity of this private key, only that the cost and complexity of doing so would be considerable. The corresponding public key will serve as the publicly known identifier for the on-board computer, and ultimately for the vehicle in which the computer is installed. Once the public key has been determined, no external record of any type should be maintained of the private key's identity. At the time of vehicle registration, the public key of the on-board system will be registered with the collection center. This key will serve as the unique, non-forgeable identifier for the vehicle (requirements S1, P4). Because the private key is the only piece of secret data held in the on-board computer (the encryption algorithms themselves do not need to be secretly held), reverse-engineering of an on-board computer could at most breach the security of transactions involving a single vehicle. Hence, requirement S3 is met.

All message transmissions from the vehicle to the collection center or any other external entity by the on-board computer should be digitally "signed" using the on-board computer's private key. The digital signature process will work as follows: The on-board computer will format the plain text (unencrypted message), including

its public key, to announce its identity to the collection center. The on-board computer will then digitally sign the message using its private key. The digital signature technique involves computing a "hash function" of the plain text message and then encrypting this hash function value using the private key (Stinson 1995, Stallings 1999). This encrypted hash value is appended to the transmitted message as a signature. The collection center will decrypt the received signature using the sender's public key and compare it to a locally computed hash function of the plain text message. Note that a match between the locally computed hash value and the one obtained from the decrypted signature ensures both the identity of the sender (because only the holder of the private key could have encrypted the signature) and the integrity of the message (because any modification to the message would have altered the computed hash value and resulted in a mismatch with the signature). This addresses requirements S6 and S7.

The digital signature technique itself does not provide any protection from external eavesdropping because the message body is in plain text form. To provide privacy of uploaded data (requirement P3), an additional encryption step is needed. Note that the on-board computer's private key is of no use for this operation. A complementary scheme can be used, however, wherein the collection center maintains its own private key and advertises a corresponding public key for use by on-board computers. On-board computers can then utilize the collection center's public key to encrypt messages prior to upload. Once encrypted, these messages can be decrypted only by the collection center and hence cannot be eavesdropped upon by any other entity. The on-board computer will first sign messages using its private key and then encrypt them using the collection center's private key.

The encryption scheme described above has two shortcomings: First, the computational complexity of public key encryption is quite high (several orders of magnitude higher than standard secret-key encryption/decryption schemes). Second, breaking the private key of the collection center would allow a malicious entity to eavesdrop on data uploads by any vehicle, making the breaking of this encryption key a potentially high-value target. The first concern is particularly problematic because the processing power of the on-board computer will necessarily be limited.

To mitigate both of these problems, we propose an alternative encryption architecture. Specifically, the collection center should use public-key encryption only for the purpose of disseminating unique, temporary, symmetric encryption keys to on-board systems (Adams 1997). These keys will be randomly generated by the collection center and will be valid for a limited time duration (e.g., a week). All protected uploads and downloads between the on-board computer and the collection center will utilize an efficient symmetric encryption scheme based upon these temporary keys. An on-board computer can request a new temporary key at any time via a simple dialogue with the collection center. Because the secure distribution of these temporary keys could utilize asymmetric encryption using the on-board computer's public key, there will be no globally vulnerable keys to worry about. Also, because the temporary key stored in an on-board computer will be

valid only for data transfer to and from that particular computer, requirement S3 is maintained.

However, in order for the on-board computer to authenticate and validate key dissemination messages from the collection center, a signature mechanism is needed. A public-key system should be used for this purpose. Specifically, the collection center should maintain a private signature key with a corresponding public key known to computers on board vehicles. This public key can be made available via a standard trusted certificate server like those commonly used in Internet security applications. This will permit the collection center to change its private key periodically to devalue attempts to acquire this key. The collection center can use this private key to sign messages exactly as described earlier for the on-board computers.

A further optimization is possible to reduce the overhead of message signature. Once symmetric, secret keys are established between an on-board computer and the collection center. These keys can be used for both digital signature (using a Message Authentication Code (MAC) technique that is both more computationally efficient and more secure than RSA-based digital signature) and encryption (Davies 1989). Thus, signature and encryption using asymmetric keys would be necessary only for purposes of disseminating temporary private keys.

**Data Upload Protocols**

The integrity of data upload from a vehicle's on-board computer to the collection center must be maintained despite a variety of communications-related problems. Requirements S8 and S9 speak to the need for reliable and accurate data upload. Because data transfers are subject to interruption at any time, the system must carefully guard against the possible loss or corruption of data due to a loss of connectivity during the upload process. Equally problematic would be the acceptance of duplicate data by the collection center resulting in an overcharge.

Internet protocols almost certainly will be used as the basis for the data communications infrastructure of the new system because developing an alternative infrastructure would be prohibitively expensive and time consuming. Because the transport layer, TCP, of the Internet provides reliable, sequenced message delivery, it is tempting to assume that all reliability issues related to data upload can be solved simply by utilizing TCP services. Unfortunately, this is a false hope for two reasons (Tanenbaum 1996): (1) TCP services do not tolerate the loss of the transport connection that potentially could occur, and (2) TCP is not designed to operate in the presence of non-robust links.

For the reasons noted above, it is advisable to utilize connectionless (UDP) service for all data uploads. This means that data destined for upload from the on-board computer to the collection center must be formatted into individual packets, which are then separately given to the network layer for delivery to the collection center. Each of these packets is independently subject to loss or corruption in the network.

A robust protocol is needed to invoke the retransmission of messages that fail to successfully reach the collection center.

A fairly straightforward Automatic Repeat Request (ARQ) protocol can be used for this purpose (Tanenbaum 1996). Such protocols are widely used in data communications applications. Each packet sent by the on-board computer should be identified by a unique "sequence number" that differentiates the packet from any other packet generated by a given on-board computer. Upon successful receipt of a packet, the collection center should respond with a positive acknowledgment (ACK) specifying the sequence number of the received packet. The on-board computer must retain a copy of any transmitted packet until a positive acknowledgment is received.

While the above protocol is somewhat unsophisticated, it is highly robust in dealing with all types of network disruptions. However, there are several special considerations in applying the ARQ protocol to this application. First, special care must be taken in determining the sequence numbers used to identify data packets. In typical ARQ applications, packet numbers are sequentially generated from some form of counter. If the sender experiences a temporary outage or software crash, the counter must sometimes be initialized to some pseudo-random initial value, resulting in a gap in the sequential numbering. In this application, it is important that sequential numbering never be lost so that the collection center can always identify gaps in reported data (requirement S10). This requires that special consideration be taken in design of the sequence numbering mechanisms used by the on-board system. A simple solution would be to record sequence numbers to nonvolatile storage.

A second consideration is the unbounded nature of the upload protocol. In fact, the problem of insuring reliable upload of data is an instance of the "Two Generals Problem" (Gray 1979), which is proven to have no bounded solution. What this theoretical result means in practical terms is that while it can be assured that any packet will eventually be successfully uploaded, the amount of time required for successful upload cannot be bounded. Therefore, under extended periods of particularly harsh link conditions, the on-board system might need to retain data packets for an arbitrarily long period of time (requirement S8). Because new data is continuously being accrued and on-board storage capacity is necessarily limited, there is a limit to the capacity of the on-board system to tolerate disruptions in the data upload process. There is no magic solution to this problem other than to provide as much storage as is feasible in the on-board computer, to use this storage as efficiently as possible, and to manage the data upload process so as to take maximum advantage of favorable link conditions. In the event that data is lost due to exhaustion of on-board storage, the system design must ensure that the collection center will always be aware of this fact (requirement S10). This is easily accommodated in the upload protocols by including a provision for the reporting of "lost" packets.

### Additional Architectural Considerations

Requirements S5, R2, and R3 dictate that the on-board system architecture must possess the ability to detect subsystem failures affecting the GPS receiver, the independent odometer, and the data-reporting subsystem (smart card link). A detected malfunction should be reported to the vehicle user through some form of in-vehicle indication. This serves two purposes: (1) to alert the user to seek system repair in the case of a non-malicious failure and (2) in the case of a deliberate disablement of a subsystem, to warn the user that the disablement has been detected.

The detection of subsystem malfunctions is, for the most part, straightforward. Loss of signals from GPS satellites should be detectable within the GPS/GIS subsystem itself. Other forms of GIS/GPS or odometer malfunction can be detected by monitoring any discrepancies between vehicle mileage data reported by the two subsystems. Malfunction or disablement of the data-reporting (upload) subsystem can be detected by failure to successfully upload data over a given time interval. This interval should be chosen to minimize false alarms due to external network unavailability but should be short enough to avoid substantial loss of data. The collection center can easily detect disablement or malfunction of the on-board system (as per requirements S10, S11) through anomalies in reported data or long-term absence of reporting activity.

Requirement R1 dictates that all collected data resident in the on-board system be stored in some form of non-volatile storage to protect it from failure scenarios involving loss of power to the on-board system. This may pose a severe restriction because non-volatile read/write storage (e.g., flash memory) is slower, less dense, and more costly that regular (volatile) dynamic random-access memory (RAM). This issue requires further study and experimentation. An alternative approach would be to relax requirement R1 to permit limited loss of data in loss-of-power situations.

## CONCLUSIONS

This appendix has defined a set of security, privacy, and robustness requirements for the new approach to assessing road user charges and outlined architectural approaches to address them. The requirements dictate secure storage and reporting of data while preventing unauthorized eavesdropping. They further dictate that the on-board system of any vehicle not hold any secret keys, algorithms, or other information that, if compromised, could be used for any purpose beyond reporting the data for that specific vehicle. Central to meeting these requirements is the use of modern, public-key cryptography, with a unique private key deeply embedded in each on-board computer at the time of manufacture. This secret key will allow authentication and validation of all data uploads from a vehicle using digital signature techniques and will also permit secure download of temporary encryption keys for efficient encryption of data to ensure privacy from eavesdropping.

Several additional security, privacy, and robustness issues have been addressed, including detection and reporting of subsystem malfunctions or deliberate attempts

at disablement, and temporary loss-of-power by the on-board system. In total, the proposed architectural features demonstrate the feasibility of addressing system security, privacy, and robustness requirements using straightforward and proven approaches. The overall conclusion is that these issues should not pose any fundamental obstacles to the successful deployment of the new approach to assessing road user charges.

**REFERENCES**


Adams, C. 1997. "Constructing Symmetric Ciphers Using the CAST Design Procedure." *Designs, Codes and Cryptography*, Vol. 12, No 3 (November), pp. 283–316.

Davies, D., and W. Price. 1989. *Security for Computer Networks*. New York, NY: John Wiley and Sons.

Gray, Jim. 1978. "Notes on Data Base Operating Systems." Operating Systems, An Advanced Course*, Lecture Notes in Computer Science*, Vol. 60. Heidelberg, Germany: Springer Verlag, pp. 393–481.

Rivest, R.L., A. Shamir, and A. Adleman. 1978. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." *Communications of the ACM*, Volume 21, No. 2, pp. 120–126.

Stallings, Wiliam. 1999. *Cryptography and Network Security—Principles and Practice*. Englewood Cliffs, NJ: Prentice Hall.

Stinson, Douglas. 1995. *Cryptography, Theory and Practice*. Boca Raton, FL: CRC Press.

Tanenbaum, Andrew. 1996. *Communication Networks*. Englewood Cliffs, NJ: Prentice Hall.