ITS Personal Data Needs: How Much Do We Really Need to Know?

Final Report

Prepared by:

Frank Douma
Thomas Garry

Humphrey School of Public Affairs
University of Minnesota

Stephen Simon

Law School
University of Minnesota

CTS 12-21

Technical Report Documentation Page

1. Report No.	2.	3. Recipients Accession No.	
CTS 12-21			
4. Title and Subtitle ITS Personal Data Needs: How Much Do We Really Need to Know?		5. Report Date July 2012 6.	
7. Author(s) Frank Douma, Thomas Garry, and Stephen Simon		8. Performing Organization Report No.	
9. Performing Organization Name and Address State and Local Policy Program Humphrey School of Public Affairs University of Minnesota 301 19th Avenue South Minneapolis, Minnesota 55455		10. Project/Task/Work Unit No. CTS Project #2011065 11. Contract (C) or Grant (G) No.	
12. Sponsoring Organization Name and Address Intelligent Transportation Systems Institute University of Minnesota 200 Transportation and Safety Building 511 Washington Ave. SE Minneapolis, Minnesota 55455		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code	
15. Supplementary Notes http://www.its.umn.edu/Publications/ResearchReports/			
16. Abstract (Limit: 250 words) The recent spread of geolocation technology in intelligent transportation systems (ITS) raises difficult and important policy questions about locational privacy. However, much of the current public discussion on locational privacy and ITS appears at risk of becoming increasingly disconnected. In one camp are privacy advocates and others who oppose the spread of ITS locational technology on privacy grounds. In the other camp are technologists and the ITS industry who generally view privacy issues as a secondary matter. The net result is that the ITS privacy debate often involves two sides talking past each other, with too little energy spent on finding potential common ground. This disconnect in part results from a lack of basic clarity, on both sides, about just what the needs and interests of those involved in the ITS privacy issue are and how they relate to the betterment of the transportation system. This report sheds new light on the ITS privacy debate by identifying just who is involved in the ITS privacy problem and what their goals are with respect to privacy and ITS data. The analysis identifies the types of locational data and the methods for obtaining it that create privacy conflicts and, in turn, recommends general approaches for both policymakers and industry practitioners to better manage these conflicts. The report represents a first effort in mapping the interests of participants in the ITS privacy debate.			
17. Document Analysis/Descriptors Intelligent transportation systems, Privacy, Laws, Regulation, Locational privacy, Personally identifiable information, Stakeholder analysis, ITS developers, ITS data users, ITS data collectors, Analysis, Developers		18. Availability Statement No restrictions. Document available from: National Technical Information Services, Alexandria, Virginia 22312	
19. Security Class (this report) Unclassified	20. Security Class (this page) Unclassified	21. No. of Pages 78	22. Price

ITS Personal Data Needs: How Much Do We Really Need to Know?

Final Report

Prepared by:

Frank Douma
Thomas Garry

Humphrey School of Public Affairs
University of Minnesota

Stephen Simon

Law School
University of Minnesota

July 2012

Published by:

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

Acknowledgments

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

We would like to extend thanks to Max Donath and Sarah Aue-Palodichuk for their support in this and previous research projects. We would also like to thank all those that participated in the panel of experts for this project, including: Tom Bamonte, Steven Bayless, Andrew Blumberg, Mike Walz, Lee Tien, and Barbara Wendling. Finally, we would like to extend our gratitude to Dorothy Glancy of the Santa Clara Law School for insightful reviews and commentary.

A version of this article first appeared in the Winter 2012 issue of the Transportation Law Journal from the University of Denver Sturm College of Law: Thomas Garry, Frank Douma, and Stephen Simon, "Intelligent Transportation Systems: Personal Data Needs and Privacy Law" 39(3) Transportation Law Journal 97 (2012).

Table of Contents

Chapter 1. Introduction **1**

Chapter 2. Background **3**

A. The Nature of Intelligent Transportation Systems (ITS). 3
B. Summary of Privacy Law for ITS. 3
C. What is Personally Identifiable Locational Information? 6

Chapter 3. Methodology **9**

Chapter 4. Participant Analysis **13**

A. ITS Developers. 13
B. Transportation Users: Subjects of Data Collection. 15
C. Government as an Institutional Participant (But Not as a Collector or User of Data). 21
D. Data Users and Collectors. 23
E. Secondary Data Users. 33

Chapter 5. Conclusions **37**

A. Policymakers Cannot Expect to Find One-Off, Grand Solutions. 37
B. The Use of PILI for Purposes Not Directly Beneficial to the Transportation System May Warrant Different Policy Treatment. 42
C. ITS Developers Will Play a Central Role in Addressing Privacy Concerns. 44
D. Many Conflicts between Participants on Privacy Issues are Not Zero-Sum. 45

Chapter 6. Summary Recommendations. **53**

References **55**

Appendix A Toolbox for Identifying Privacy Issues

Appendix B Taxonomy of Privacy Expectations and Legal Protections

List of Tables

Table 3.1 Participants and Constituent Groups..... 10

Table 5.1 Mitigating Privacy Conflicts between Participants Over the Collection and Use of PILI. 46

List of Figures

Figure 5.1 Web of Interests in the ITS Privacy Debate 39

Executive Summary

The last decade has seen a dramatic spread of geolocation technology in intelligent transportation systems (ITS). Yet the speed at which ITS and locational technology is developing is outpacing progress on addressing the difficult locational privacy questions raised by these technologies. Moreover, much of the current public discussion on locational privacy and ITS appears at risk of becoming increasingly disconnected. In one camp are privacy advocates and others who oppose the spread of ITS locational technology on privacy grounds. In the other camp are technologists and the ITS industry who generally view privacy issues as a secondary matter, dwarfed by the impressive and tangible benefits these technologies bring to the transportation system. The net result of this disconnect is that the ITS privacy debate often involves two sides talking past each other, with too little energy spent on finding potential common ground, where privacy concerns can be addressed while allowing the data collection that ITS locational technology needs to function.

This disconnect in part results from a lack of basic clarity, on both sides, about just what the needs, goals and interests of those involved in the ITS privacy issue are and how they relate to the betterment of the transportation system. To address this disconnect, this report sheds new light on the ITS privacy debate by identifying just who is involved in the ITS privacy problem and what their goals are with respect to privacy and ITS data. The analysis identifies the types of locational data and the methods for obtaining it that create such conflicts and, in turn, the analysis recommends general approaches for both policymakers and industry practitioners to better manage these conflicts. In sum, the report represents a first effort in mapping and assessing the interests in the ITS privacy debate.

The analysis shows that there is no simple divide among participants in the ITS privacy debate, between those who favor privacy protections and those who favor the ability to collect and use personally identifiable locational data (PILI). Rather, the analysis indicates the debate involves a web of interlaced interests among participants, some conflicting and some congruent. This debate structure results not only from a diverse set of participants but also from the piecemeal nature of American privacy law and the variety of transportation settings in which PILI is collected by ITS.

The positions of participants in the debate vary with circumstances (e.g., where, when, how the data is collected) and over time, given how fast technology and society's privacy expectations are changing. As a result, finding policy solutions to the ITS privacy debate becomes a more nuanced and iterative endeavor: Is the collection of PILI necessary in a certain setting? Are there non-PILI alternatives? If PILI has to be collected, how should it be handled? Do the answers to these questions change over time?

For policymakers, this means that for the foreseeable future policy approaches to the ITS privacy problem will necessarily be sector and context specific. Attempts at broad, single-shot solutions will likely be undermined by the mix of heterogeneous participant interests, new technologies and shifting privacy norms.

When tackled at this smaller scale, the ITS-privacy debate reveals a number of potential avenues, or tools, for finding common ground for at least some of the most significant participant conflicts: those between transportation users and data collectors and users. These tools for common ground include:

Rules

- Time limits on data retention. This involves purging PILI in its entirety from databases, or at least removing its personally identifiable elements, after some defined period of time.
- Prohibition on secondary uses of data unrelated to the primary use or not consented to by the subject of the data collection.

Technology Architecture

- "Privacy-by-design" techniques that use ITS architecture to increase the privacy of PILI or avoid collecting PILI altogether, while still providing the needed level of data utility for identified end users.

Industry Practice

- The practice of not collecting PILI where data needs can be met with non-PILI. This is particularly applicable where non-PILI is sufficient and the additional costs of collecting PILI, in terms of its protection, production for law enforcement and litigation and the risks to reputation from data breaches, are considered.
- Implement privacy policies that call for: (i) the use of best practices for internal data management and security; and (ii) the use of clear privacy notices, where applicable so transportation users can make informed decisions about sharing PILI and which, in turn, encourages market differentiation among private-sector data collectors and ITS developers.

Chapter 1. Introduction

The last decade has seen a dramatic spread in geolocation technology. Global positioning systems (GPS) technology, for example, is now commonplace in cellular phones, cars, bicycle computers, and even runners' watches. The ability of this technology to collect, easily and inexpensively, vast amounts of personally identifiable information about individuals' travel behavior is raising difficult, important and controversial questions about locational privacy: When can an individual's locational information be electronically gathered and by whom? Once collected, for what purposes can that data be used? With whom can it be shared? How long should the data be retained? When can law enforcement access it? (1)

The prominence and significance of these questions are no more apparent than in the transportation context. The application of geolocation technology in intelligent transportation systems (ITS) already provide a number of means by which vehicles, and in some circumstances occupants, can be electronically identified and tracked as they move about the transportation network. Furthermore, these means can only be expected to increase as locational technology develops and its potential applications for ITS expand.

Yet the speed at which ITS and locational technology is developing is outpacing progress on addressing these difficult privacy questions. (2) Moreover, much of the current public discussion on locational privacy and ITS appears at risk of becoming increasingly disconnected. In one camp are privacy advocates and others who oppose the spread of ITS locational technology on privacy grounds. They have raised questions in the courts and alarm among politicians and the general public about the threat such technologies present to privacy "rights". This has resulted in court decisions, political controversies and electoral messages that have in some cases prohibited the deployment of ITS technologies, and even the removal of some technologies after deployment. (3)

In the other camp are technologists and the ITS industry who generally view privacy issues as a secondary matter, dwarfed by the impressive and tangible benefits these technologies bring to the transportation system. As a result, those on this side of the debate often give too little attention to privacy concerns, both in how they design ITS locational technology and in communicating with the public about what data their devices collect and for what purposes.

The net result of this disconnect is that the ITS privacy debate often involves two sides talking past each other, with too little energy spent on finding common ground, where privacy concerns can be addressed while allowing the data collection that ITS locational technology needs to function. This lack of articulated common ground creates uncertainty for the ITS community as whole, and particularly for technology developers as they are pushed by privacy advocates to avoid making products that can collect sensitive locational information and pulled by new technological developments that increase the ability to collect that data.

In part the disconnect stems from the increasingly murky legal setting in which this debate takes places. Rapid technological change is upsetting what had once been relatively stable legal doctrines and categories used to discuss and manage conflicts over privacy. (4) The resulting legal uncertainty makes it difficult to find even a common conceptual framework and language

under which the two sides can meet, let alone set clear lines about what locational information deserves legal protection and what does not. (5)

Related to this legal uncertainty, the disconnect also results from a lack of basic clarity, on both sides, about just what the needs, goals and interests of those involved in the ITS privacy issue are and how they relate to the betterment of the transportation system. That is, just what are the data needs for locational technology that further the objectives of ITS and to what extent do they really conflict with the legitimate privacy expectations of transportation users?

It is this second source of the disconnect that is the focus of this report. This report will seek to shed new light on the ITS privacy debate by identifying just who is involved in the ITS privacy problem and what their goals are with respect to privacy and ITS data. The analysis will identify the types of locational data and the methods for obtaining it that create such conflicts and, in turn, recommend general approaches for both policymakers and industry practitioners to better manage these conflicts; that is, the report will try to find some much needed common ground in the ITS privacy debate.

The report will proceed in six chapters. The second chapter will lay the groundwork for the analysis by providing: a short description of ITS; a brief primer on privacy law as it relates to transportation; and a discussion of what type of locational information is at issue in the ITS privacy problem. The third chapter will contain a description of the methodology used for the analysis of the participants in the ITS privacy problem. The next chapter will contain the participant analysis itself. The fifth chapter will provide some conclusions that follow from the analysis. The final chapter will set forth some general recommendations for policymakers and the ITS industry.

Chapter 2. Background

A. The Nature of Intelligent Transportation Systems (ITS).

ITS is a broad, often generic term used to refer to generally any electronic and communication technologies used in the transportation system. (6) In the context of privacy issues, ITS nearly always refers to technologies related to ground vehicular transportation. In this report, the discussion will be limited to ITS as it relates to non-public ground transportation.

The type of technologies involved with ITS are wide ranging and include both in-vehicle telematics and roadside data collection devices. (7) Current examples include: vehicle toll tag transponders that automatically identify vehicles for the electronic payment of tolls; roadside systems to measure traffic volume, speed and congestion; roadside and vehicle mounted cameras that aid law enforcement; and in-vehicle systems that warn drives of dangerous situations and provide information on route choices.

Though ITS technologies are deployed and operated by both the private and public sectors, the core rationale for ITS is generally a public one: to improve the safety, efficiency, cost effectiveness, sustainability and reliability of the transportation system. (8) Moreover, ITS often involves a large amount of coordination and cooperation between the public and private sectors. ITS technologies are developed in the private sector but generally need to be integrated in some fashion with the government's transportation regulatory system as well as the transportation infrastructure, which is typically (though certainly not always) planned, paid for and managed by the public sector.

ITS technologies implicate privacy issues because by their nature they are generally dependent on locational data. That is, to be useful, these systems typically need to collect data on when and where vehicles are. While this data often includes little or no information about individual vehicles and transportation users, many ITS applications collect some degree of vehicle and/or user specific locational data.

B. Summary of Privacy Law for ITS.

Unlike the Europe Union or other countries deploying ITS, the United States does not have a comprehensive legal regime that protects privacy. Instead, the concept of an individual's "right to privacy" has arisen piecemeal, at both the federal and state levels, through court cases and legislation of limited scope. Furthermore, privacy rights are not fixed, but evolving as society's privacy expectations, technology and the law itself changes. Previous research by the lead author of this report has detailed and analyzed U.S. privacy law in the transportation context and its implications for ITS. (9) The main points of this research are:

1 Sources of Privacy Protection.

- The U.S. Constitution, specifically Supreme Court case law on the Fourth, Ninth and Fourteenth Amendments, is a core source of American privacy law. With respect to the transportation context, case law on the Fourth Amendment is the most relevant. The basic test for whether a person has a protected privacy interest under the Fourth

Amendment comes from the 1967 U.S. Supreme Court case, *Katz v. United States*. (10) Under *Katz*, a reasonable expectation of privacy exists when: (i) a person has an expectation of privacy, and (ii) society deems the expectation to be reasonable. Clarifying in a later case, the Supreme Court stated "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."(11)

- Rapid technological change, however, is bringing the legitimacy of the *Katz* test into question. The Supreme Court itself has acknowledged that the second part of the *Katz* test, the "societal expectation" prong, is nearly unworkable, as technology is advancing so rapidly that it is almost impossible for a court to determine the corresponding societal expectation of privacy.(12) Reflecting this to some extent, the Court in a recent Fourth Amendment case on GPS tracking by law enforcement decided the case using an analysis framework other than the *Katz* test, though without necessarily rejecting the primacy of *Katz*.(13)
- While U.S. constitutional law is the most influential and does much to shape privacy law generally, its direct applicability for ITS is limited to the context of criminal investigations and government employment.
- A number of existing federal laws create privacy protections, albeit in relatively discrete areas. Very few of these laws have direct relevance for ITS. Among those that do, the most relevant are the *Driver's Privacy Protection Act of 1994*, which protects personal information collected by departments of motor vehicles, and the *Privacy Act of 1974*, which regulates how the federal governments handles the personally identifiable information it collects.(14) In addition, the Federal Trade Commission, under Section 5 of the *Federal Trade Commission Act*, has become active in regulating companies' privacy notices to consumers about how they collect and use consumer data, including locational data.(15)
- Though there are currently no federal laws that specifically protect an individual's locational information, there are a number of proposed laws that seek to do so. These include the bipartisan *Geolocational Privacy and Surveillance Act* which would require law enforcement to get a warrant before using locational technology to track individuals' location; and the *Location Privacy Protection Act of 2011* which make it presumptively illegal for non-government entities to collect an individual's locational information absent consent.(16) These proposed laws reflect the level of political interest and public concern over locational privacy issues.
- Federal law sets the floor of privacy protection upon which states have the ability to build their own privacy regulations. As a result, the extent to which privacy is protected beyond the federal level varies across states. Some state courts have interpreted their state constitutions in a way that expands the privacy rights of their citizens beyond those prescribed by federal constitution. Similarly, some states statutorily extend privacy protections beyond those afforded by federal law. But like federal law, state statues generally approach privacy in a piecemeal, area-by-area fashion.
- There are not many state laws specifically addressing privacy and transportation technologies. Most laws only address specific technologies whose use is either unpopular with the public, such as automated speed enforcement, or where there is a perceived potential for abuse.

- State privacy torts, such as intrusion upon solitude, public disclosure of private facts, "false light" publicity, and misappropriation of likeness, provide an additional source of privacy protection. These torts, though, do not usually create a cause of action on the public streets, and have not yet been successfully applied in any cases involving ITS technologies. (17)

2 Implications of Privacy Law for ITS.

The tangled and unsettled nature of privacy law in the U.S. means its application to ITS is often jurisdiction, technology and context specific. Nevertheless, several principles can be stated.

- The less personally identifiable the information an ITS application collects, the less likely the application will encounter legal restrictions that will dictate how that information is collected and used. When the data collected identifies specific vehicles or otherwise includes personally identifiable information, legal issues regarding consent, access, ownership and protection of information are often triggered.
- When an ITS application collects personally identifiable information about an individual, consent to obtain that data generally should be obtained from that individual. Voluntary consent (opt-in) is one way in which consent can be given. Voluntary consent generally requires individuals to manifest willingness to have their personal information collected and must be informed of some specific aspects about the information being collected. The other form of consent is to imply consent (opt-out). Courts have found implied consent to be sufficient when the governments' interests' in preventing injury, property damage, and loss of life on roadways are served by the practice. However presumed or implied consent usually must allow for individuals to opt-out of such programs and requires that members of the public be made reasonably aware of to what they are tacitly consenting.(18)
- Current law typically places much greater restrictions on the collection and use of personally identifiable data by the public sector, than by the private sector. Thus, who is collecting and/or using the information gathered by an ITS application, often dictates the level of privacy protections triggered.

To help synthesize how privacy law applies to ITS, the previous research by the lead author of this report developed an ITS and Privacy Toolbox and Taxonomy, which are included as Appendices 1 and 2 to this report. The Toolbox and Taxonomy summarize the level of restrictions that correspond with different kinds of information being collected.(19) Together they illustrate two basic principles regarding the intersection of ITS and privacy law: (i) "[t]he more personal the nature of the information that is collected, the greater the number of privacy considerations exist"; and (ii) "the proposed purpose for collecting personal information also triggers different levels of privacy considerations, as information collection for the administrative purposes of roadway safety and efficiency will raise less of a legal expectation of privacy, compared to when ITS information is being gathered for criminal and law enforcement purposes".(20)

C. What is Personally Identifiable Locational Information?

As this summary indicates, much of privacy law analysis in the ITS context is underpinned by the distinction between anonymous and personally identifiably data; the latter implicates privacy interests under the law while the former does not. This report will refer to information that implicates privacy interests as *personally identifiable locational information* (PILI).

Generally, PILI is considered data that could be used to identify an individual (e.g., license plate number) as being at a particular location at a particular time. Conversely, anonymous locational information, or non-PILI, cannot be tied back to a specific individual. Examples include information from traffic counters or devises that only detect the presences of vehicles in order to control traffic flows, without identifying the vehicle.

As a practical matter, much ITS information is likely to fall within a spectrum of PILI and non-PILI, as opposed to within a strict category of anonymous or personally identifiable. Moreover, data administrators regularly try to convert PILI they have collected into non-PILI by manipulating it to remove identifiers that could link the data to specific individuals, as collecting and using PILI is in many instances not the primary purpose of ITS applications.

However, the efficacy of these de-identifying or anonymizing practices in terms of privacy protection, as well as the very distinction between PILI and non-PILI, are coming into increasing question. Recent advances in re-identification techniques – the process by which seemingly anonymous data is linked with other information in order to associate it with specific individuals – have become surprisingly effective and as a result have significantly eroded the difference between PILI and non-PILI. (21) What had previously thought to be anonymous information can now be combined with other data to connect it with a specific individual.

This blurring of the line between PILI and non-PILI is principally driven by three factors unlikely to abate in the near future: (i) enormous growth in low-cost data processing and storage capabilities that has widely expand the opportunities for aggregating and integrating data from multiple sources; (ii) targeted advertising and homeland security are creating powerful incentives to obtain and utilized personalized data in both the public and private sectors; and (iii) the increasing availability of publicly available information about individuals is changing notions of acceptable levels of anonymity among the public.(22)

The diminishing distinction between PILI and non-PILI creates a conceptual problem for privacy law: how to differentiate between which information warrants protection and that which does not. There is clearly a difference-in-kind in terms of privacy concerns between a dataset with traffic counts and one with license plate numbers. The problem is how to draw a conceptual line between the two that has generally applicability, in light of re-identification technology.

This report is not the forum for attempting to resolve this conceptual problem. The Federal Trade Commission (FTC) in a recent study confronted this problem in the context of consumer privacy and proposed that an inexact but workable line can be drawn between data that can be *reasonably* linked to a specific individual, computer or device, including through processes of re-identification, and data that cannot be so linked.(23) This report will borrow from the FTC's framework and define PILI collected from ITS applications to mean: locational data that can be

reasonably connected to a specific individual, device or vehicle, and non-PILI as locational data that cannot be reasonably connected to any individual, device or vehicle.

Chapter 3. Methodology

The first objective of this report is to bring clarity to the ITS privacy debate by identifying: (i) who is involved in the creation, collection, use and regulation of PILI data from ITS sources; (ii) what are their respective goals; (iii) what restraints, if any, are there on achieving their interests; and (iv) where their interests may come in to actual conflict. This is largely a descriptive analysis, in effect an assessment of the current state of affairs with respect to ITS and privacy. This type of study is a basic element in any policy analysis. Surprisingly though, it appears there have been no published analysis of this sort with respect to ITS and privacy. (24)

In many ways, this analysis is similar to a stakeholder analysis in that it involves identifying those institutions, entities, groups and types of individuals that have a stake in some matter, and their interests and preferences with respect to that matter.(25) This report, however, is not what is typically thought of as a stakeholder analysis in that does not assess the relative power each group has over influencing outcomes or policy with respect to the subject issues, and does not prioritize any group's involvement in the ITS and privacy issue. Further, the analysis here does not address the role, interests and power of advocacy groups (e.g., privacy advocacy groups or ITS industry trade organizations); the positions of these groups are, for the type of analysis here, treated as derivative of their constituents' views. In this regard, this report is less a stakeholder analysis and more of what may be called a "participant analysis"; that is, it examines who are the direct, "on the ground" participants in the ITS privacy problem.

For purposes of this analysis, a "participant" was defined broadly to capture parties that have a direct role in the ITS privacy issue, not just those involved in ITS data collection and use. Doing so expanded the list of participants to include the government (in its regulatory capacity), as well as transportation users who are the subjects of ITS data.

In identifying participants and their interests for this report, input was sought from a panel of experts in relevant fields including ITS, telecommunications technology, transportation and privacy law. Specifically, initial drafts of the analysis were circulated among these experts, who in turn provided commentary that resulted in extensive revisions to the analysis.

One of the basic issues on which a number of experts commented was how to best organize the discussion of participants. Because public and private actors are treated different under privacy law, using the public-private distinction as the main organizing framework seemed useful and logical. However, feedback from panelists and the content of the analysis itself suggested that the public-private distinction was secondary, and that more instructive was a first-order grouping of participants based on their functional role with respect to ITS data collection, use and policy development. Table 1 lists the participants identified and the categories in which they were organized. The analysis in the following Chapter 4 will follow the organizational structure shown in Table 1.

Table 3.1 Participants and Constituent Groups

	Participant Groups	Participant Sub-Groups	Examples
A.	ITS Developers	Firms without a direct relationship with transportation users.	Firm in the ITS technology and application supply chain firms (e.g., hardware and software developers)
		Firms with a relationship with transportation users.	Auto-Manufacturers
B.	Transportation Users (Subjects of ITS Data Collection)	Individuals	Vehicle Owners, Drivers, Passengers
		Commercial Firms	Freight Haulers; Commercial Bus Lines; Taxi Firms
C.	Government (not as data collector or user)	Role as Protector of Privacy	Legislatures; Courts; Regulatory Agencies (e.g., Federal Trade Commission)
		Role as Facilitator of Economic Development	Legislatures; Regulatory Agencies (e.g., economic development agencies)
		Role as Regulator	Legislatures; Regulatory Agencies (e.g., consumer protection agencies)
D.	Data Collectors & Users	Private Sector	Subscription-Based ITS Providers (e.g., in-vehicle navigation services); Car Rental Companies; Employers; Auto Insurance Companies; Market and Traffic Analysis Firms
		Public Sector/Government	Operators of Transportation Systems; Law Enforcement; Public-Sector Employers

	Participant Groups	Participant Sub-Groups	Examples
		Quasi-Public	Tollway Authorities
E.	Secondary Data Users	Marketers	Geo-locational advertisers
		Litigants	Civil Plaintiffs and Defendants; Criminal Defendants; Private Investigators

Chapter 4. Participant Analysis

A. ITS Developers.

ITS developers are the private-sector firms that design and produce the devices, networks and software that collect and manage ITS locational data. As private-sector actors, their goals with respect to ITS are driven principally by profit and market considerations. For these participants, ITS represents a marketplace for new products and services, and to the extent that ITS expands these firms stand to gain.

With respect to PILI, as a general matter, the basic interest of these firms is that the fewer restrictions on collecting and using PILI the better. More opportunities to collect PILI and more opportunities to use PILI translate into increased demand for their products. Underlying this interest is the principle in information technology that the more personally identifiable information a set of data contains, the greater utility it has for an end user -- as well as the inverse, the more anonymous information in a dataset, the less utility it has. (26) Thus, all other things being equal, products that collect and use PILI represent a larger potential market for developers, than those that collect non-PILI.

But all other things are not equal. A number of factors constrain this basic interest of ITS developers. These factors include:

1 Lack of market demand for PILI collecting products in a given setting due, for example, to: public opposition to the collection and use of PILI: the additional costs or risks associated with protecting and sharing PILI; or privacy laws prohibit the collecting of PILI.
2 Strategic positioning by the firm in response to whether they think addressing privacy considerations with their products will be beneficial for them in the market or in public discussions on privacy (e.g., can proactive steps be taken to forestall public policies that limit data collection).
3 The firm's business and marketing model have incorporated principles of corporate responsibility with respect to privacy.

The relative influence of these constraining forces for a given firm is to some extent a function of whether that firm sells their products directly to the subjects of ITS data collection. For example, a company that makes tracking devices for car rental companies will likely have a different perspective on PILI, as compared to an auto-manufacturer building a GPS-equipped vehicle that is sold directly to the public. Accordingly, the analysis here is split between these two types of firms.

1 Firms without a Direct Relationship with the Subjects of ITS Data Collection.

These are private-sector firm in the ITS supply chain (e.g., hardware and software developers). Typically, they do not themselves collect data and therefore do not have any direct relationship with transportation users. Neither do they generally use the data themselves. Thus, their position on PILI is largely shaped by the nature of their clients (i.e., the party to whom they are selling their ITS products) and their clients' position on the need for PILI. That is, the extent to

which these firms will or will not design their products to collect PILI or include privacy enhancing features is largely driven by whether there is client demand for doing so. For instance, a firm that makes transponders for an automated toll road will incorporate privacy enhancing technology within those devices to the extent the operator of the toll road wants them and, practically speaking, can pass their additional cost on to road users.

2 Firms with a Relationship with the Subjects of ITS Data Collection.

There are a number of kinds of ITS developers that sell their products directly to the subjects of ITS data collection. Auto-manufactures are an example in that they include ITS technology as value added features in their vehicles.

These developers have additional considerations that arise from their direct relationship with the subjects of data collection. These include:

1 They may be both a developer of technology as well as a collector and user of PILI. Thus, their interest in PILI is more direct, both in terms of the risks and benefits in collecting and using such information.
2 These firms must navigate and manage consumer expectations about privacy with regard to their products, particularly as these expectations and the related economic costs (e.g., costs of data security) change over time. They must do so in order to earn or maintain consumer trust, both with respect to their firm generally and privacy specifically. This is particularly the case where ITS technology is secondary to a firm's principal business. The main business of auto-manufactures, for instance, is selling cars. They do not want privacy concerns generated by the inclusion of ITS features in their vehicles to harm their overall brand. Accordingly, these types of firms must weigh the commercial opportunities that greater levels of PILI collection allow against the risks doing so presents to consumer trust.

Regardless of whether they have a direct relationship with the subjects of data collection or not, ITS developers are an essential pivot point in the ITS privacy debate because of their ability to build privacy enhancing features directly into devices. Early ITS devices often relied on generic, off-the-shelf, technology. However, now many ITS applications employ technologies specifically designed for ITS applications. This presents opportunities to engineer privacy considerations into ITS architectures from the outset, so-called "privacy by design".

The key aim of privacy-by-design is to use engineering to limit the potential to connect locational data with an individual, while also maximizing the informational value of the data for end users. Further, in privacy-by-design, privacy considerations and data protection are built into the ITS architectures from the outset, as opposed to as an afterthought and add-ons after systems are in place already. Examples include: (i) cryptography methods that increase the anonymity of tollway transponder data but still permit the tollway authority to allocate toll charges to individual vehicles; and (ii) the separation of the processing of identity and locational information from in-vehicle GPS units so that no one entity has both locational and vehicle identity data.(27)

Privacy-by-design is, however, not a win-win silver bullet. Building privacy-enhancing features into ITS applications can make the applications more expensive. More importantly, as advances in re-identification technology and relational databases have shown, even when identifying information is removed, data can still yield PILI when combined with other information sets. Privacy-by-design can thus mitigate ITS privacy concerns, but not necessarily solve them.

For developers themselves, to the extent they can show privacy-by-design technologies improve privacy protection but preserve locational data utility, they can reduce the restraint privacy concerns puts on their market. Thus, privacy-by-design can advances developers' own economic interests and do so in a manner that furthers privacy considerations. (28)

An increasing cognizance among ITS developers of privacy considerations is evident in the efforts by trade groups and other industry organizations to develop industry-wide privacy principles, and otherwise take steps to self-regulate with respect privacy.(29) This reflects recognition among some portions of the industry that if the public's privacy concerns with respect to PILI are left unaddressed, particularly in the design and development stages, such concerns could be a significant impediment to the deployment of ITS markets over the long term. In this respect, the presumed preference of developers for the ability to collect and use PILI may be secondary to a desire to avoid unfavorable public policies and public sentiment with regard to PILI data collection.

B. Transportation Users: Subjects of Data Collection.

Two kinds of groups are the subjects of PILI collection by ITS applications: individuals and private commercial firms.

1 Individuals.

Individuals are the subjects of ITS data collections as vehicle owners, drivers, and passengers. As transportation end users, their goals with respect to ITS are to secure the improvements it can bring to the transportation system: increased mobility, reduced congestion, improved safety, and more efficient use of resources.

With regard to PILI, individuals have two basic kinds of interests. First, they have a strong interest in the protection of PILI for privacy reasons. Significant harms can result from the unauthorized collection, use and sharing of a person's PILI. These harms can be wide-ranging in nature, including; economic; dignitary; reputational; political, loss of civil liberties; and sometimes even physical harms (e.g., as a result of stalking). Moreover, these harms to individuals are also harms to society as a whole, in that can impede or have a chilling effect on socially beneficial behavior and otherwise have a negative effect on civil society.

Second, in addition to this harm-avoidance or privacy-protection interest, individuals also have an interest in securing the benefits that can be obtained from sharing their PILI. Advances in locational technology have, in effect, made PILI a valuable asset for individuals, which they can trade for services and conveniences. Pay-as-you-drive car insurance and GPS navigational guidance are just two of the many examples that illustrate this dynamic.

In the context of ITS, both these interests (harm-avoidance and benefit-securing) are retrained by a number of factors. These restraints include:

- To the extent the two interests are in opposition, they restrain each other. That is, the harm-avoidance interest can weigh against the benefit-securing interest, and vice-versa. Sharing PILI to gain some benefit may increase the risk that an individual can suffer a privacy related harm related to information.
- Either of these interests can be restrained by ITS architecture. An ITS application that requires an individual's PILI may provide a valuable benefit to a transportation user, but it may not allow for the secure sharing of that PILI.
- Individuals' cognitive biases limit their ability to pursue their harm-prevention interest. (30) Research shows that people often overly discount future privacy risks in exchange for immediate benefits. This is due to a number of factors, including that: protecting privacy is typically a secondary consideration for individuals that arises in the context of some other primary objective; and PILI is often collected in small increments and individuals often do not perceive a significant privacy threat with respect to each incremental piece of such data, but in the aggregate such data can amount to a significant privacy invasion. (31)
- The pursuit of these interests can be restrained by the law, particularly with regard to the harm-prevention interests. The law may not protect PILI from unauthorized collection or use, or it may not require an adequate or sufficiently clear notice of the privacy risks involved with sharing PILI in a given circumstance.

There is a complicated interplay among these interests and restraints that shapes how individual behave with respect to their PILI.

Most individuals having a strong stated preference for maintaining the privacy of their movement and travel habits. For individuals, when the government engages in the collection of PILI, it raises longstanding concerns about widespread government surveillance and overbearing scrutiny of private lives for law enforcement or political purposes. When private sector firms collect the data, individuals have concerns about unaccountable private parties knowing 'too much' about them, as well as to whom such information may eventually be sold.

However, most individuals' stated preferences do not match their actions. (32) Studies indicate an apparent dichotomy between individuals' stated privacy preferences and their actual behavior. (33) Research shows that "individuals are willing to trade privacy for convenience or to bargain the release of personal information in exchange for relatively small rewards."(34) In short, individuals say they value their privacy much more than they do in practice.

As a result, it is difficult to determine or measure what individuals' actual privacy preferences are for their PILI in many situations. Furthermore, individuals' privacy preferences, whatever they are, are not static. They can shift rapidly over time as changes in technology, the law, and government and corporate behavior influence social norms about privacy. (35)

Despite these complexities, the characteristics of some categories of individuals in the ITS context do lead them to have objective differences in the relative weight they put on privacy protection. These differences stem from the basic characteristics of the individuals in each

category, the way certain ITS technology benefits or interacts with them, and how the law treats them.

a. Vehicle Owners

Many types of ITS technology only gather information that is tied to a specific vehicle (e.g., via licenses plate numbers) rather than an individual driver or occupant. (36) Through vehicle registration databases, this vehicle locational data can be positively linked to the owner of the vehicle. It can as also be used to infer the possible driver of the vehicle. Consequently, such vehicle data is PILI.

This ability to positively identify the owner but not necessarily the driver is unimportant in some circumstances as the owner and driver/passengers may be treated as one-in-the-same. Toll collectors, for example, do not necessarily care who is driving a given car on their roadway. Similarly, in the case of automated traffic enforcement systems (e.g., red-light cameras) owners are sometimes held liable, as a matter of law, for the offense regardless of who is driving the car.(37)

There are, however, circumstances where this owner-driver distinction is important, most notably in the case of criminal law enforcement. Courts have placed limits on the extent to which vehicle owners can be held vicariously liable for acts committed by a user of their car.(38) Further, in criminal and civil cases, evidence from ITS networks that a particular car was at a given location at a certain time is only circumstantial evidence that the owner herself was there. Accordingly, all other things being equal, vehicle owners as a group have a different and lesser privacy-protection interest in their vehicle's locational data, as compared to drivers' interest in their locational data. The privacy-protection interest of owners is lesser because of the legal and practical limits on what actions by an unidentified driver can be attributed to a vehicle's owner. (39)

b. Drivers

In the ITS context, individual drivers have the strongest interests in their PILI, both in terms of privacy protection and in benefit gaining. ITS devices that can positively identify and locate individual drivers at a particular moment in time (e.g., roadside face recognition cameras, in-vehicle biometric devices) pose the greatest potential to undermine their interest in privacy protection.

Moreover, the capacity of ITS applications to compile large amounts of PILI, in electronic form, presents a more significant privacy risk than information about a discrete or individual trip. Such aggregate data enables the drawing of intimate picture of a person's life, creating the capacity to tell third parties "where that individual works, sleeps, worships and recreates with others."(40) In turn, though, such detailed PILI also has the greatest value to drivers in terms of the ability to exchange it for ITS benefits and services.

i. Sub-Categories of Drivers.

There are several sub-categories of drivers that, given their circumstances, may have a lesser interest in their PILI than drivers generally, or otherwise warrant special consideration. These include:

Employees. ITS technology provides the means for employers to monitor in detail the travel behavior of their employees.(41) This may, for example, occur when employees are utilizing employer-provided vehicles (e.g., sales people), and thus provide employers the opportunity to track their employees both while in the course of performing their duties as well as outside their employment. In turn, such information may then be available to third parties, including law enforcement. Given the typically inferior bargaining position of most employees, vis-à-vis their employer, the privacy-protection interest of employees, with respect to PILI, warrants special consideration.

In addition, the collection of the PILI of public employees, such as police officers, probation officers, agency administrators and judges, may raise distinctive concerns as such data may be considered public records, subject to freedom of information requests. Accordingly, public employees may have distinct interests with respect to the collection of their PILI by their employers.

Minor-Age Drivers. Many states have graduated drivers license (GDL) programs for young drivers. (42) These programs place restrictions on teenage licenses, such as curfews and limits on the number and kinds of passengers, in an effort to lower the risks new drivers present. In-vehicle devices are being developed to monitor teen driver compliance with GDL restrictions, as well as to discourage unsafe driving practices and monitor compliance with traffic laws.(43) These devices, either by-design or as a necessary by-product, have the potential to collect PILI that would be valuable to law enforcement, insurance companies and other third parties. Such devices strongly implicate the privacy-protection interests of young drivers, particularly to the extent such devices become a legal or de facto requirement (e.g., insurers require them) for minors to enter GDL programs. They also raise special privacy issues for non-GDL drivers of the same vehicle to the extent the GDL monitoring devices are not or cannot be disabled for other drivers. However, such privacy costs may be justified to the extent such devices improve teenage driver safety. (44)

Senior Drivers. Like teenagers, older individuals are in a higher-risk class of drivers. ITS technology is being developed to address the age-related functional limitations that contribute to seniors being more risky drivers. Some of these technologies, such as intersection crash avoidance systems that seek to reduce the disproportionate involvement of seniors in intersection crashes, use real-time vehicle location and traffic signal information to warn senior drivers of potential crash situations.(45) Again, the data collected by these systems may be valuable to law enforcement or third parties, and raises privacy protection concerns specific to seniors, particularly to the extent any such system becomes a condition for seniors to have a license or to be insurable.

c. Passengers

Drivers are not the only occupants of vehicles who can have their identity and location captured by ITS technology. Voice command systems and in-vehicle cameras can be used to identify vehicle passengers. (46) As with drivers, such technologies trigger a heightened level of privacy concerns because they collect PILI with which passengers may be readily identified. Further, in certain circumstances such as when passengers are in a vehicle that is not their own or with which they are not familiar, passengers may have an even greater privacy interest than drivers in that they may have no knowledge or reason to know their PILI is being captured.

2 Commercial Firms.

Private-sector businesses that own and operate commercial vehicles are also the subject of ITS applications that collect PILI. For these companies, ITS has the potential to bring a wide range of benefits by improving the flow of information among their vehicles, company managers and the transportation system. This improved flow of information can raise productivity, reduce administrative costs and increase profits. (47)

Many of the same types of ITS applications that can collect PILI about individuals also collect PILI about commercial vehicles (e.g., tollway tag transponders, GPS navigation services). However, there are also two additional ways in which PILI about commercial vehicles can be collected, that do not apply to individuals: compliance with vehicle regulatory regimes; and vehicle fleet management systems.(48)

a. Data from Regulatory Compliance

Companies that own and operate commercial vehicle owners are generally subject to a number of state and federal regulations that do not apply to drivers and owners of passenger vehicles. These regulations stem from the nature of commercial vehicles: their weight and size, the cargo or number of passengers they carry, the borders they cross, etc.

The administration of some of these regulations and compliance with them by businesses can often be facilitated and improved by ITS technology. An example of this is electronic clearance technology that automates the inspection process of freight haulers at weigh stations and border crossings. Such systems involve in-vehicle transponders and roadside technologies for vehicle identification and weighing.

Generally, both the regulator and regulated benefit from the collection of PILI through these technologies.(49) Typically such systems only automate existing regulatory processes; that is, they only generate locational information regulators already gather through manual collection processes.(50) However, the greater reliability and coverage of the automated collection process and the immediate digital format of the information, raises concerns for regulated firms that such information could be used by the parties collecting the data for tracking individual vehicles and other secondary purposes, including speed enforcement.(51)

b. Data from Internal Management Systems.

Many businesses that operate commercial vehicles have internal management systems that employ ITS applications to track the movement and location of their vehicles. These systems allow businesses to do things like better control and assess fuel usage, plan delivery schedules and evaluate driver performance. Businesses typically take measures to protect this information from outside parties, for a number of practical and business reasons (e.g., employee safety, protection of trade secrets etc.). Some firms, however, sell the locational data from their fleets to third parties, such as traffic-reporting services, but only after it has been anonymized.

Regardless of how it is generated, commercial firms generally have the same general interests in PILI that individuals do. They have an interest in (i) protecting it from unauthorized uses (i.e., harm avoidance); and (ii) employing it for certain benefits or services. However, the nature of these interests for businesses, in comparison to those of individuals, differs in two important respects.

First, unlike individuals, the privacy-protection interest for businesses is also driven by concerns about competitors accessing their PILI. (52) Some businesses consider the movement and position of their company vehicles to have value in their industry. Within the trucking industry, for example, a competitive advantage can be gained if the positioning and routing of a firm's fleet is optimized relative to the geographic flows of freight.(53) As a result, many freight movers view their shipping routes and vehicle positions as trade secrets. Similarly, business people across many industries do not want their travel behavior in company vehicles to be captured and disclosed to competitors, lest they reveal information about who their potential new customers or takeover targets are.(54) Thus, any ITS technology that can identify and track individual vehicles raises the concern that competitors may gain access to such information.(55) However, some businesses, such as commercial bus services, may see competitive advantages in the dissemination of their PILI and thus may take different stances on locational privacy.

Second, with respect to their benefit-seeking interest, businesses want ITS technologies to improve and streamline the commercial vehicle regulatory regimes to which they are subject. This interest can provide a significant impetus to the spread of ITS technology, as the example of electronic clearance technology above illustrates.

The restraints on commercial firms' interests in PILI are also similar to the restraints on individuals' interests, but again with two notable exceptions. First, the interest of businesses in protecting their PILI from competitors falls within the protections afforded by trade secret laws. As a result, this interest, unlike many aspects of the harm-avoidance interest of individuals, is generally covered by a well-developed area of the law. Second, companies, when weighing the advantages and disadvantages of sharing their PILI, generally speaking, do not suffer from the same cognitive biases that individuals do.

Beyond these descriptive differences between individuals and commercial firms as the subjects of PILI data collection, it is also important to separate businesses because they represent a powerful political constituency, who may use their influence to attempt to shape the ITS privacy debate (and any resulting regulations) in ways that differ from the interests of individual drivers.

This role of businesses in the privacy debate, though, is complicated by the variability of concerns about ITS privacy across industries.

Furthermore, commercial firms are distinctly important to ITS privacy issues because, as a practical matter, they are often in the best position to be early adopters of ITS technology. To the extent they view ITS applications as possibly creating privacy problems for them down the road, they may be reluctant to embrace and drive the development of ITS technologies. For example, many businesses likely want to avoid ITS applications that involve the sharing of PILI with government planners or vehicle regulators, unless they can be assured that such information will not end up being used for other purposes, such as law enforcement, or being made publicly available through freedom of information act requests.

C. Government as an Institutional Participant (But Not as a Collector or User of Data).

The government has a clear stake in whether PILI can be collected and, if it is collected, to whom it is available and for what purposes. It likewise has strong stake in the development of ITS for the benefits it brings to the transportation system. However, the government's perspective on these issues is not uniform. It varies depending on the level of government being discussed, whether federal, state or local. It also varies across the number of roles government has, from that of a collector and user of ITS data for law enforcement and transportation planning, to that of being an institutional defender of privacy. In this section, the focus is on the government's interests when it is not involved in collecting or using ITS data, and the perspectives this generates on PILI and ITS generally.

1 Government Institutional Interests in Privacy.

The federal and state governments, through their judicial and legislative capacities, play a central role in defining the formal privacy rights on which many of the privacy concerns about the collection of PILI are based. (56) In this respect, the government has a strong institutional interest in the protection of these rights and the prevention of harms resulting from the violation of these rights. Similarly, government has a political interest in being responsive to the public's concerns about protecting PILI, particularly as technological changes alter privacy expectations and necessitate the redefining of formal privacy rights to fit contemporary circumstances.

In comparison to the federal government, state governments are by their nature often more responsive to constituent and advocacy groups' demands, and thus can be expected to be the place where concerns over privacy and PILI are most likely to find legislative expression.(57)

2 Facilitator of Economic Development.

In promoting public welfare, the government regularly acts to encourage economic development and innovation. At the federal level, this involves using public policy to promote the economic competitiveness of the U.S. relative to other countries. Many ITS applications clearly have the potential to increase economic efficiency and output, for example, by reducing traffic congestion. (58)

Some commentators and ITS industry representatives have expressed concern that the U.S. has fallen behind other countries in the development and deployment of ITS, and that this is having a negative impact on the economic well-being of the U.S. (59) Accordingly, to the extent that privacy concerns over the collection of PILI are an impediment for ITS in the U.S., relative to other countries, the federal government has an interest in lessening those impediments. In the same vein, to the degree that disparate state privacy laws create obstacles for ITS, the federal government has a stake in establishing a measure of legal uniformity across states with respect to the handling of PILI.

At the state level, one of the principal drivers of government decision making is the state's economic competiveness, relative to other states as well as internationally. Hence, to the extent that the development and deployment of a given ITS technology is viewed as improving a state's economic performance, this will weigh against a state taking measures to limit the use of that technology on the basis of privacy considerations.

Similarly, economic competitiveness is an important consideration for local government, and the quality and nature of the transportation system in a given local area plays a central role in its economic competiveness relative to other areas. Given the potential of ITS to reduce congestion and otherwise improve transportation systems in a cost-effective manner, local governments can generally be expected to lean against restricting ITS due to concerns over PILI.

3 Regulatory Activities.

Federal and state governments are the central regulators of economic life in the U.S. Through their regulatory and administrative activities, they promotes certain public policies, such as fairness, consumer safety, competitive markets, pollution control, efficient tax collection, the free flow of information and so on. ITS has the potential to help the government pursue a number of these objectives more effectively and efficiently by, for instance, improving public safety by reducing the number of car accidents through better vehicle and infrastructure designs.

Given the advantages ITS collection brings to achieving a number of various policy objectives, government as regulator now regularly confronts issues at the intersection of privacy and ITS. Recent examples include: the Federal Trade Commission being asked to investigate whether an ITS data collector is adequately disclosing their locational data collection and use practices to consumers; (60) the National Highway Traffic Safety Administration issuing rules regarding whether car manufactures must include event data records (more commonly known as black boxes) in all new cars and what type of information these devices will record; (61) and the U.S. Department of Transportation's research into usage-based vehicle taxes that may involve the measurement of distance travelled with in-vehicle GPS and telematic devices. (62)

In its regulatory capacities, the government often has to balance competing public policy objectives. Its role is no different in the case of ITS and privacy. The government as regulator will frequently need to weigh how privacy considerations should shape and limit the use of ITS technology that collects PILI in particular circumstances. From this perspective, the government cannot generally be presumed to favor or disfavor the collection of PILI, but rather can be seen as a key player in mediating the relationship between privacy and ITS.

D. Data Users and Collectors.

This category of participant consists of those actors involved in the collection and use of PILI from ITS. They operate ITS technology, and then manage, store and use the resulting PILI. Participants in this category may be involved, to different degrees, in the collection or use of PILI from ITS, but to some extent they do both. (Participants that are only involved in the use of PILI are discussed in the following section.)

Participants in this section will be organized based on whether they are private, public or quasi-public actors. This is a useful arrangement given that privacy law treats collectors and users of PILI somewhat differently depending on which of these sub-categories they fall into. Moreover, the purposes for which these participants collect and use PILI are, to some extent, distinguishable along these lines.

1 Private-Sector Participants.

For private-sector data collectors and users, their goals with respect to ITS are principally driven by economic considerations. In broad terms, these firms gather and use, or want to have the ability to gather and use, PILI because it improves their bottom line. It can reduce costs, through improved decision-making. It can also generate profits, either through the firm's own use of the data or by selling it to other parties.

The private sector's involvement in the collection and use of PILI from ITS is rapidly evolving. The data has a wide range of applications and there are a variety of private firms that can benefit from it. The strength of each firm's interest in PILI varies depending on their industry and their data needs. Some of the most notable current PILI collectors and users include the following.

a. Subscription-Based ITS Providers

Subscription-Based ITS providers are companies that collect PILI from the vehicles of owners with whom they have a contractual relationship to provide some service related to that data. Examples include companies like OnStar, which provides vehicle communication services such as stolen vehicle tracking, automated crash response, and navigation guidance. These companies have a direct economic interest in PILI as its collection and use is a core part of their business.

Outside of fraud and consumer disclosure requirements, there are generally no existing legal constraints on the PILI these companies can collect. (63) In principal they could try and collect as much PILI information as is technologically and commercially feasible. In practice, though, these firms have considerations beyond the law that restrain their collection of PILI. These include (i) the cost and time involved in protecting the data from security breaches or having to produce it for law enforcement or civil litigants; (ii) principles of corporate responsibility; and (iii) the privacy preferences of their customers and the public at large, given that the use of their services is voluntary and they are presumably seeking a wide a customer base as possible. (64)

This dynamic reflects the policy position that the market can best determine the extent to which PILI should be protected: consumer choice, profit incentives and cost considerations will drive firms towards an optimal level of privacy protection. In this light, when determining the extent

to collect and use PILI, subscription-based participants can be understood as weighing (a) the privacy preferences of their users (and prospective users) and the cost of collecting, managing and protecting PILI, against (b) the commercial advantages that can be gained from PILI.(65)

To the extent this calculus results in companies self-imposing restraints on their collection and use of PILI, this may be evidenced by the customer contracts or their privacy policies. Privacy policies, generally speaking, are an organization's statement about how it collects, uses, protects and shares a customer or client's data. (66) For the most part, private-sector companies are not required to have privacy policies, apart from select circumstances.(67) Compared to consumer contracts, privacy policies tend to be more specific about a company's privacy practices, but the policies are typically not legally binding.

Nevertheless, privacy policies can play an important role in enhancing privacy. They can create certain expectations among customers which companies may feel compelled to honor in order to maintain customer trust and market competitiveness. In this regard, the policies can promote transparency and competition among companies on privacy issues.(68) Moreover, to the extent companies engage in a deliberative process to develop their privacy policies, doing so can help identify where privacy-enhancing steps can be cost beneficial, such as improving internal data security to reduce the risk of costly data breaches.

b. Car Rental Companies

Many businesses that operate commercial vehicles have internal management systems that employ ITS to track the movement and location of their vehicles. These companies have a strong economic interest in the collection of this data for the purpose of improving the ability to manage their assets. The PILI collected by these businesses raises privacy concerns for three groups: the employees of these businesses who drive the vehicles (discussed above with respect to individuals in Section 2.A); the company itself to the extent the data can be accessed by third parties (discussed above with respect to commercial transportation users in Section 2.B); and third-party drivers of these vehicles. Car rental companies are those businesses that let third-party drivers use their vehicles, and they are the subject of this subsection.

Car rental companies have found a number of uses for GPS and telematic technology in their vehicles. These uses mainly involve the monitoring compliance with and, in some instances, enforcement of rental contracts. Examples include:

- Geographic restrictions. Rental companies often place geographic restrictions on a vehicle's use. When a customer drives a vehicle across a restricted boundary, in-vehicle GPS and telematic devices can alert the rental company. The company can then disable the vehicle using a remote ignition interlock that prevents the vehicle from being started, or more commonly, use the telematic systems to calculate distance penalties.(69)
- Ensuring use by only the authorized driver. Car rental agreements typically only authorize named individuals to drive the rented vehicle. Some rental companies, when they suspect unauthorized use, will monitor the car's movements to check whether it is being driven in areas where they would expect the authorized driver to be, such as where they work or live, or where they indicated they were going to travel. (70) If the vehicle is not there, the company may take measures to disable and recover the vehicle.

Each of these uses, at a minimum, requires that the rental company be able to track the location of individual vehicles. In this respect, car rental companies can be viewed as having a legitimate business interest in the ability to collect and use PILI from their ITS systems; doing so helps manage and protect their vehicles.

An open question is whether car rental companies should get the consent of their customers to collect this data, or at least disclose their PILI collection practices. Unlike subscription-based ITS providers, PILI collection is not part-and-parcel of the service rental companies provide their customers. The data's principle purpose is for the protection of the car rental companies' property.

Currently, there is no clear consensus within the rental car industry on whether the collection and use of PILI should be disclosed to customers. (71) Some disclose to encourage compliance with the rental contract while others do not for, among other reasons, fear customers may disable the equipment.(72) To the extent the industry does not have a recognized disclosure practice, this limits the argument that consumer choice can be used to manage privacy issues.

The industry does have considerations that restrain its collection of PILI beyond consumer choice. One is liability exposure for the conduct of rental car drivers.(73) Given that rental companies have the ability to monitor speed and location, they want to avoid scenarios where they have a responsibility to disable vehicles or inform the authorities when drivers are known to be engaging in reckless or suspected unlawful behavior. Another consideration is the expense of responding to requests for this data from law enforcement and civil litigants.

In addition, a few states have imposed legal constraints on the collection of PILI by car rental companies. This has been principally driven by consumer concerns about abuse.(74) New York and California, for example, now prohibit the use of tracking devices by rental companies, except for limited purposes, such as the loss of a vehicle.(75) These laws represent one of the few instances where the collection of PILI has been legally restricted for a particular industry.

c. Employers

Private-sector employers now regularly outfit their company vehicles with GPS and telematic devices. (76) Employers do so to increase the productivity and safety of their employees and vehicles, as well as to encourage responsible behavior among employees. Freight companies, for example, can use real-time locational data from their fleet to coordinate vehicles over the course of a day as pick-up and delivery needs change, and many different kinds of employers can use locational data to crosscheck employee timesheets with vehicle movements.

The locational information collected by employers is necessarily PILI. Employers typically know which employee is driving which of their vehicles. Moreover, for locational information to be of value to employers, it must be personally identifiable. Accordingly, employers can be seen as having a legitimate interest in being able to gather, for bona fide business reasons, the PILI of their employees while they are in company-owned vehicles.

While employers find a number of benefits in outfitting their vehicles with location monitoring devices, employees can see it as overly intrusive surveillance of their activities and invasion of their privacy, particularly to the extent they are monitored during non-work periods. The

employer-employee relationship is the subject of much government regulation, but currently there are no federal or state laws that prohibit private employers from using locational monitoring devices in their company-owned vehicles.(77) At least one state, though, has a law requiring an employee's consent before such devices can be used.(78)

State privacy laws and common law tort principles may place limits on private employers use of tracking devices, especially with respect to off-duty monitoring.(79) However, because of the relatively recent deployment of these technologies, there have been few reported cases so far applying privacy laws or tort principles to employee locational tracking.(80) In the cases that have been reported, courts have generally given preference to employer's interest in the protection and productivity of their vehicles, over the privacy interests of employees.(81) Nevertheless, given the lack of legal certainty, the practice among many private companies now is to seek the consent of their employees and to develop written polices about when the location of employees can be monitored and for what purposes. (82) Furthermore, employers may be subject to union contracts that place limits on when they can collect PILI about their union employers.

d. Insurance Companies

The ability to collect PILI is having a significant impact on how auto insurers underwrite drivers. Conventional car insurance typically assess the risk of drivers based a number of generic risk profiles, including age, sex, location and type of car, along with driving history. These categories are based upon risk averages and, generally, over or underestimate the risk of a given driver. PILI about an individual driver allows insurers to create a more accurate risk profile of that driver and, in turn, better match the price of coverage to the actual risk presented. This rationale creates a strong business interest in PILI for insurance companies. A societal interest is also served by insurance companies having this data, as it allows them to more fairly price an individual driver's risk to the transportation system.

The simplest form of this new type of insurance, often generically referred to as usage-based insurance, is based on the amount of miles actually driven.(83) More sophisticated forms include additional variables to gain a more complete risk profile, such as: elapsed driving time; duration of driving periods; when during the day or night a car is driven; where the car is driven; the driver's acceleration and braking patterns; and driving at excessive speeds (e.g., over 80 mph).(84) Some forms of usage-based insurance are targeted at the parents of teenage drivers and offer features that alert parents if their teenager has violated certain conditions, including curfew, geographic and speed restrictions, or whether they have not arrived at school within a certain time. (85)

Usage-based insurance appeals to consumers because it offers the possibility of lower rates. To take of advantage of it, though, drivers have to outfit their cars with telematic devices to record and transmit information about their driving behavior to insurers. For insurers, the ITS data they collect must be personally identifiable -- they need to be able to link driving behavior to a particular driver, or at least a particular vehicle.

However, for some forms of usage-based insurance, locational information is not necessary. And some insurers have begun to differentiate themselves in the marketplace based on whether

they require locational tracking for their usage-based insurance. An executive from Progressive Insurance Group described his company's position on privacy and locational tracking this way:

"The most sensitive [privacy] issue is location tracking. . . . We've been at this for quite some time, and we've concluded there are arguments on the benefits of location, but concluded we didn't need it for purposes of rating risk."(86)

In this regard, insurance companies can be understood as viewing consumer choice as the best manager of privacy issues, given that the type of insurance a consumer purchases is voluntary and the market can offer insurance options that do not require PILI. In line with this, insurers can be expected to disfavor public policies that place restrictions on the collection and use PILI, as that may restrict current and future market opportunities.(87)

On the other hand, auto insurance is highly regulated at the state level. These existing regulatory platforms could be used to address concerns about the secondary uses of PILI collected by insurance companies, as well as require that the market provides products that do not require PILI so that those policies that do require PILI remain effectively opt-in.

e. Market and Traffic Analysis Firms

Market and traffic analysis firms are interested in ITS information because it can help them understand consumer travel behavior and the traffic characteristics around particular locations.(88) This information, for instance, can improve decision-making with regard to real estate valuation and the siting of businesses and buildings. While this type of location data has long been collected by such firms through travel surveys and traffic counters, ITS technology increases the volume, scope and accuracy of this information.(89)

ITS applications that collect PILI increase the granularity, and thus utility, of traffic data, improving the modeling of origin-destination patterns and the behavior of particular kinds of travelers in given areas. Further, some applications that collect PILI for traffic and market analysis purposes, such as GPS-equipped vehicles, have the potential to collect data less expensively than applications that collect non-PILI.(90)

However, despite the advantages of PILI, many of this industry’s data needs can be met through anonymous geodemographic data sets. Measuring the amount and timing of traffic flows does not require PILI. (91) Thus, while collecting and using PILI does provide a marginal benefit for these stakeholders, non-PILI is often an adequate substitute or equivalent for these participants.

f. Operators of Transportation Systems (e.g., Government Contractors)

In an effort to save money and improve efficiency, governments regularly outsource the operation of transportation services and infrastructure management to private sector companies. As a result, some private-sector firms collect PILI data on behalf of the government or in the process of carrying out what has been traditionally thought of as a government service. Examples include private firms that operate speed cameras that identify vehicles for purposes of enforcing traffic regulations. (92)

Such private companies have an obvious interest, principally economic, in the collection and use of PILI. This interest though is circumscribed, in that it is essentially derivative of the government's interest in that data. That is, the contractor's interest in collecting and using the PILI does not extend beyond the legitimacy of the government's own interest in that data. (93) For example, a company operating red-light cameras on behalf of a local jurisdiction does not have a legitimate interest in using the data it collects for purposes other than enforcing the traffic rules.

A conceivable exception to this lies when the contractor is purposefully given some degree of ownership of the PILI it collects on the government's behalf. This could arise when the government engages a contractor to collect PILI for it, and part of the payment to the contractor for doing so is a concession to use the PILI for some other purposes, such as advertising. Such a scenario would raise difficult policy questions about the obligations of the contractor with respect to such data.

2 Public-Sector Participants.

Public-sectors entities collect and use PILI from ITS sources. They do so in three main capacities: (a) as managers of transportation systems; (b) as law enforcement; and (c) as employers.

a. Manager of Transportation Systems

In their role as managers of public transportation systems, the government has its most widespread involvement in the collection and use of PILI from ITS. This involvement mostly occurs at the state, regional and local levels of government, through a mix of actors: state-level agencies (e.g., departments of transportation, departments of motor vehicles [DMVs]), metropolitan planning organizations, as well as regional, county and city agencies.

Traffic monitoring and transportation planning are two of the principal activities for which these actors use ITS data. The very purpose of many ITS applications are to provide information to the public sector about traffic flows and infrastructure use. Such data increases the efficiency and safety of transportation systems, by enabling and improving such things as: the modeling and management of traffic congestion; analyzing future infrastructure needs; performing safety analysis using driver and vehicle behavior characteristics; and monitoring air quality and its relationship to traffic patterns.(94) This information generally comes from infrastructure based technology (as opposed to vehicle based) and measure things like vehicle counts, travel times, road speeds, and route patterns. (95) While much of this data is location specific, it is not personally identifiable in that the devices do not identify individual vehicles or drivers. Accordingly, for most traffic monitoring and transportation planning activities, anonymous information is sufficient.

However, these activities are not completely shielded from the ITS privacy debate. Technological developments, such collecting data from in-vehicle GPS units, raise the prospect of more accurate and fine-grained travel data for traffic monitoring and transportation planning, as well as less expensive data collection.(96) But these technologies also involve collecting PILI, raising the attendant privacy issues.(97)

For some other purposes, transportation agencies already regularly collect PILI. These are generally cases in which for some reason individual vehicles need to be identified at particular locations in the transportation system. Examples include identifying commercial vehicles at weigh stations and border crossings and identifying vehicles using roads subject to usage charges (e.g., tollways, HOT lanes, congestion pricing). Identification of this nature is typically done through the detection of in-vehicle devices by roadside systems, and the use of cameras or video technology to capture license plates. This type of information is personally identifiable in that the vehicle locational data can be linked to customer accounts, including credit card and vehicle registration information, in order to process usage charges.(98) Technical steps are often taken to try and minimize the extent to which this information can be personally identifiable, for instance by stripping data pieces of unique identifiers.(99) In addition, sometimes there are legal or policy requirements that PILI be purged from databases after a defined period. But these measures are not always successful in completely anonymizing or protecting the data and, in any event, they create additional costs for agencies. (100)

As a general legal matter, the privacy concerns with the government's collection of this type of PILI are mitigated by the fact that transportation users voluntarily elect to use the roadways these ITS applications monitor (and, if applicable, voluntarily install the relevant in-vehicle devices). Thus they ostensibly consent to such data collection. However, this consent-based solution to the privacy problem has several vulnerabilities. First, to the extent the sharing of PILI becomes a *de facto* requirement for driving, the notion of voluntary consent may no longer be a viable remedy to the privacy problem. Second, there remains some uncertainty about the secondary, non-ITS related uses to which this data can be put (i.e., uses not necessarily implicitly or explicitly consented to). Warrants, subpoenas, as well as freedom of information acts, provide potential avenues of access to this information by secondary uses. (101)

Despite these privacy complications, as road user taxes and congestion pricing systems gain more acceptance as policy tools and sources of government revenue, there will likely be greater demand for public-sector actors to collect this type of PILI.

State DMVs are another area in which the government already handles personally identifiable data related to transportation. The information they collect includes vehicle ownership information and the social security numbers, photographs, addresses, and medical information of drivers. DMVs use this information to perform their vehicle and driver licensing functions.

DMV data is relevant for ITS as it is often used to link ITS locational data to a specific vehicle owner or driver, for purposes of charging usage fees or identifying who has committed a traffic offense. For example, a license-plate reader camera will capture the license plate number of a vehicle that has run a red light. The license plate number is then run through the DMV database to match it with the vehicle owner and obtain the owner's address for citation purposes.

Importantly, the DMV information that connects ITS locational data to a particular individual is protected by the *Driver's Privacy Protection Act* (DPPA). (102) As a result, this DMV identification information can only be used for select purposes, such as processing traffic violations, without the consent of the person who is the subject of the data.(103) Thus, to the extent DMV information is needed to convert ITS locational data into PILI, the DPPA functions as privacy bulwark. Notably, it does so without undermining the effectiveness of ITS

applications, such as automated enforcement. In this regard, the DPPA may be a model for erecting other privacy walls at strategic places in ITS architecture, where locational information can be held separate from identification information.

b. Law Enforcement

Law enforcement is a core function of the government. It has a strong interest in the effective and efficient prevention and investigation of possible legal violations, as well as the prosecution of actual violations. PILI is often directly relevant to these undertakings, from tracking the movements of suspected criminals to identifying the driver of a speeding vehicle. ITS technology dramatically increases the availability, reliability and scope of such information, as well as the ease with which the government can acquire it.

Countervailing the government's strong interest in PILI for law enforcement is the privacy interests of transportation users. The government's use of their PILI for law enforcement can result in legal sanctions, loss of liberty and a chilling effect on otherwise legal and socially beneficial behavior.

It is for these weighty reasons that the government's collection of PILI faces the highest level of legal scrutiny. The government's ability to acquire, use and internally share PILI about individuals for law enforcement purposes is constrained by principles of the federal and state constitutions, and a number of federal and state statutes.(104)

However, most of the laws and court cases relevant for ITS in this regard were written well before the advent of many ITS technologies. As a result, just how these constraints apply to the collection of PILI from ITS in particular circumstances is currently a matter of some uncertainty. Moreover, this uncertainty may remain for some period as technological changes rapidly alter the practicalities of the collection and use of PILI by law enforcement. (105)

This uncertainty, when combined with the strong interest the government has in using PILI for law enforcement, means it is likely that government (in its law enforcement role) can be expected to push to define these constraints in a manner that allows it the greatest possible flexibility in obtaining and using PILI from ITS. (106) Specifically, this means such things as a greater ability to employ private firms as surrogate data collectors. (107)

One of the most active areas of policy debate, at the state and local level, has been the use of ITS to enforce traffic safety laws. Often referred to as automated enforcement, this involves using roadside cameras to identify vehicles, and sometimes the drivers, that have committed a traffic offense, such as exceeding a posted speed limit or driving through a red light.

The government's interest in the use of automated enforcement is principally twofold: (i) increase public safety through more effective enforcement of traffic laws; and (ii) reduce the cost of enforcement through the use of technology. This latter rationale is particular strong for local governments as they spend a relatively significant amount of their resources on traffic enforcement.

The privacy interests implicated in the use of target automated enforcement are less than in use of ITS by the government for mass surveillance. Automated enforcement systems are generally

designed so that the cameras are only activated when a violation is detected; that is, the cameras do not indiscriminately capture everything in view. (108)

Nevertheless, automated enforcement allows the government to collect significant amounts of PILI about transportation users, which has the potential for uses beyond traffic enforcement. This concern, in part, has led in some instances to public resistance to the use of ITS to enforce traffic laws.(109) And in response, several states have passed laws prohibiting automated enforcement and others have passed laws limiting its use.(110) Moreover, the use of automated enforcement to enforce more than minor traffic offenses faces constitutional limitations.(111)

Despite these countervailing factors, the fiscal and administrative attractiveness of using ITS to enforce traffic rules means that it will likely continue to remain a relevant objective for state and local governments and a key issue in the ITS privacy debate.

c. As Employer

The government employs a large number of people and, just as with private-sector employers, it has a strong interest in the productivity and behavior of its employees and in the protection of its property. And also like private-sector employers, the government installs GPS and other telematic devices on its vehicles. In doing so, the government confronts many of the same employee privacy considerations discussed above with respect to private employers.

The government as an employer, though, is subject to additional legal constraints that do not apply to private employers. Most notably of these are the privacy protections afforded by the Fourth Amendment, as well as state constitutional equivalents, which apply to the government when it acts as an employer.(112) These protections limit when and how the government can collect information about its employees, including PILI from vehicles.(113) In addition, public-sector employers are subject to statutes that limit the extent to which they can share data they have collected about their employees with other parts of the government.(114)

Thus, while public-sector employers, as a general matter, have the same interest in collecting PILI about their employees as private employers do about their employers, the government's ability to do so faces more legal restraints.

3 Quasi-Public Entities

Recent years have seen an increase in organizations that perform public functions but do not fit clearly in the mold of public-sector actors.(115) These so-called quasi-public entities take on a variety of forms, but their commonality is that they perform what would generally be referred to as public functions, such as operating bus systems or carrying out regulatory responsibilities.

Typically these organizations are formed pursuant to legislation and are controlled by government-appointed boards.(116) They are not fully public in that they are independent of the legislature and executive branches, and generally do not depend on state general funds for their operation.(117) They are, however, not fully private because they are run by government appointed officials and are often endowed with powers to collect fees and revenues in the course of performing traditional public functions.(118) These types of quasi-public entities are often found managing transportation infrastructure systems such as toll roads.

There are also other types of quasi-public entities that result from partnerships between public bodies and private firms. These organizations may not be specifically authorized by legislation and may be managed by both government officials and industry representatives, and thus may have more of a private character to them then the type of organizations discussed above. These types of entities can often be found in the transportation sector where industry and the public sector want to formalize their cooperation in the delivery of some nominally public service or function. A notable example is Heavy Vehicle Licenses Plate, Inc., or HELP, Inc. (119) This is a non-profit organization operated by government transportation officials and representatives of the trucking industry. (120) Its mission is to develop, deploy and manage ITS systems in the trucking industry that allow for automated compliance with commercial vehicle regulations, such as weigh stations, driver log requirements, cargo inspections, and controlled-access to certain types of facilities.

The rationale of quasi-public entities is that the can deliver public services more effectively and efficiently than traditional public organizations. This can be due to their ability to self-finance and operate without legislative oversight; their freedom from civil service and contract bidding requirements; their ability to geographically bridge traditional jurisdictional boundaries; or their capacity to directly involve industry in decision-making.(121)

These quasi-public organizations have a high relevance for ITS in that they often build and operate transportation facilities that may benefit from ITS technology or, in the case of organizations like HELP, Inc., they bring industry and government together on using ITS technology to improve the regulatory compliance process. In this regard, the objectives of many of these organizations are aligned with the mission of ITS -- to improve the transportation system.

Because these organizations are typically mission specific, their interest in collecting and using PILI is generally limited to the extent that having PILI serves that mission. For example, the collection of PILI by a tollway authority to efficiently charge drivers for tollway use furthers the objective of efficiently operating the tollway. On the other hand, the use of the PILI for some secondary purpose, such as sharing it with unrelated organizations or for advertising, does not follow from that mission.

To the extent these organizations collect and use PILI, their legal obligation with respect to that data is sometimes unclear. Their quasi-public status complicates the analysis of what statutory and constitutional restrictions they are subject to, in both their collection practices and secondary uses of the data. The question in effect is whether they are treated as public or private sector entities. For example: Is their data subject to freedom of information requests? (122) Does law enforcement need to have a warrant to access information from them? Can they share or sell their information with private firms?

This ambiguity creates uncertainty, but also opportunities for innovation. (123) For example, with regard to those quasi-public entities created by statute, the legislature can specifically prescribe the obligations that a particular entity has with respect to collecting and using PILI, as opposed to the more complicated task of creating statutory privacy obligations that apply across the government as a whole or to a specific agency that has a wide set of responsibilities.

Examples of this can be seen with statutorily created tollway authorities whose authorizing statutes detail what they may and may not do with the PILI they collect.(124)

E. Secondary Data Users.

This final category consists of participants who use PILI from ITS sources but are not involved in its collection. The interest of these participants in PILI, and ITS generally, are distinguishable from those participants that both collect and use PILI. As a general matter, these participants do not have a direct stake in improving the transportation system through ITS. For them, ITS is principally only a source of locational data.

The two main types of participants in this category are marketers (advertisers) and civil litigants. They are sometimes referred to as secondary data uses since their use of PILI is often outside the primary purpose for which the data was original collected. (125)

1 Marketers.

PILI from ITS sources have considerable value for marketers. (126) Consumer locational information is what one commentator has described as the third pillar of the "holy trinity" of advertising data (after demographic data and information about the day/time someone is viewing something).(127) PILI allows marketers to identify when and where consumers travel and how far they are willing to travel for certain purchases. In turn, it allows marketers to develop sophisticated models of consumer behavior on which advertising strategies can be built.

Further, when PILI data comes from an in-vehicle ITS device that permits two-way communication, marketers have the ability to target and customize their efforts towards particular customers, with a specific offer at a specific time and at a specific place. This creates a valuable opportunity to influence desirable consumers at the moment they are most likely to make the decision of where to stop for gas, coffee, etc. (128) Moreover, it provides the potential for marketers to "manage" the traffic to a particular business over the course of the day, by increasing location-based incentives efforts at those times when demand is low. (129)

Marketers may also aggregate this locational data with other non-ITS data, such as data on age, gender, income, and lifestyle to further refine targeted advertisements, with those messages then delivered through a number of possible media. For example, advertisers may send emails to consumers with advertisements or sale information, with those materials tailored based on each consumer's travel history (e.g., what stores they like to visit, when they go to those stores, etc.). All of this is part of the broader shift in marketing, from mass advertising to targeted approaches based on consumer-specific data. (130)

Beyond fraud or other deceptive trade practices, marketers generally have no legal restraints on their use of PILI. They do face some restrictions on the medium of their marketing using PILI. For example, there are legal limits on marketing via emails or faxes. (131) However, these restrictions do not in and of themselves regulate the use of PILI. The most significant restraint marketers may face is negative consumer reactions to advertisements using PILI based on the consumer's privacy concerns.

Most marketers do not collect ITS locational data themselves; rather they purchase it from a data collector such as vehicle navigational services. Marketing is thus typically a secondary use of ITS data. This raises the problematic issue of the extent to which the subjects of the data have, explicitly or implicitly, consented to the use of their PILI by marketers. Where there is no such consent, marketers cannot be said, from both a privacy and transportation-system perspective, to have a strong interest in the data.

While marketers are generally a secondary user of data, they do often provide a critical source of revenue for ITS data collectors. (132) As a result, the type of data that marketers want and what they are willing to pay for it, influences the decisions by data collectors about what locational information they will obtain and store, and the extent to which that information is personally identifiable.

For many marketing purposes, locational data does not need to contain PILI to have considerable value; anonymized data is often sufficient. Marketers can still advertise products and services to an individual based on his or her travel patterns, even if they do not know who that person is. Nevertheless, PILI is clearly more valuable to marketers than non-PILI, as it allows them to relate an individual consumer to a specific travel pattern and allows them to link a given customer's travel behavior to other consumer information, thus permitting even further targeting of advertising efforts.

Generally speaking then marketers can be understood as preferring the availability to obtain PILI. However, this is not an all or nothing preference, as it is for car rental companies for example. Decoupling identity from locational information does not entirely negate the value of ITS data to marketers. Marketers can still gain considerable value from anonymized and aggregate data.

2 Litigants.

When a party's travel behavior or location at a particular time is relevant in litigation, litigants are increasingly seeking to use information gathered from ITS systems as evidence. Examples include divorce cases where the travel habits of one of the parties may be used as evidence of infidelity, or in car accident cases where information about the speed and position of a vehicle at a particular moment may help reconstruct the accident. (133) By definition what is sought in these cases is PILI; otherwise the information would likely not be of value to the seeking party.

The question in the context of litigation is not whether PILI should be collected -- it already has been -- but whether the information should be available in the litigation discovery process. If the data is public information this question has already been answered. If, however, the data is non-public this becomes an open question.

There are three distinct interests in this question. First is the party who is seeking such information. They presumptively favor the discoverability of such information. Second is the party whose locational information is at issue. They presumably disfavor the discoverability of such information, otherwise they would consent to its discovery. And third is the holder of such information in cases where it is a non-party to the litigation. These non-party holders are typically ITS data collectors. They presumably disfavor the discoverability of such information

for a number of reason: producing such information for litigation is burdensome and costly; it creates an expectation that they must archive such information; disclosure may conflict with existing contractual or policy commitments they may have to the party whose locational information is at issue; and disclosure may deter the use of their service by prospective customers.(134) Non-party holders may be either public or private-sector parties and this will influence the strength of their interest in disclosing the information, as well as legal responsibilities they may have in not-disclosing the information.

The legal rules of discovery mediate these competing interests, determining whether the information should be available to the party seeking it in a given case.(135) While the general rules of discovery are well established, their application to ITS information is not. As a general matter, in litigation among private parties such information will likely be available if it is relevant to the dispute -- absent a specific statue or common law principle that prohibits the discover of particular types of information.(136) Courts do have the discretion to assess, in a given case, whether privacy interests should limit the discovery of certain kinds of information or whether the burden of its production outweighs the benefits of the information to the case.(137) As a general rule of thumb, though, if the location of a party is directly relevant to the dispute in the case, it is likely that the court will permit the discovery of the information.(138)

Given the wide range of litigation scenarios in which a driver or a vehicle's locational information may be relevant, it is difficult to identify singular participant positions for likely litigants with respect to the privacy aspects of such information. For a given participant, in some cases the discoverability of such information may be advantageous while in others it may not. Insurance companies, for example, may favor the discoverability of such inform when they represent the plaintiff, but not when they are defending liability claims.

The participants with the clearest interest in this context are the non-party holders of PILI. As a generally matter, they will have a strong preference for the non-discoverability of such information for the reasons discussed above. In this respect, to the extent PILI from ITS sources is discoverable, it creates a strong incentive for collectors to anonymize the data they collect in order to reduce its potential as evidence in litigation, or do avoid collecting PILI altogether. (139) For the same reason, they may limit the time they keep the data, purging it from their systems after a certain period. (140)

There are certain professional groups who also have an interest in the availability of PILI from ITS sources in court cases. Plaintiff and criminal defense attorneys, for instance, have an interest in the availability of PILI data. But again the circumstances of the particularly case will dictate whether they favor its discoverability in that case. Vehicle forensic experts who analyze vehicle data recorders and private investigators, on the other hand, may have a consistent interest in the availability and discoverability of PILI data as it creates demand for their business.

It is noteworthy, though, that many of the interests litigants have in using PILI from ITS sources are unrelated to the purposes of ITS. That is, the furtherance of their interests in using PILI generally does not benefit the transportation system. An exception to this may be that PILI from ITS sources may assist in the adjudication of traffic accident disputes.

Chapter 5. Conclusions

The participant analysis points to four main conclusions about the actors involved in the ITS privacy debate, the dynamics among them and possible approaches to moving the debate forward: A) given the heterogeneity of the interests involved and rapid technology change, policymakers cannot expect to find one-off, grand solutions to the ITS privacy problem; B) the use of PILI for purposes not directly beneficial to the transportation system may warrant different policy treatment; C) ITS developers will play a central role in addressing privacy concerns; and D) a number of conflicts between participants on privacy issues are not zero-sum, and thus there exists potential areas for common ground between them. Each of these conclusions will be addressed in turn here.

A. Policymakers Cannot Expect to Find One-Off, Grand Solutions.

The participant analysis reveals that the ITS privacy debate involves a latticework of conflicting and congruent interests. This structure means there are few clear and stable divisions in the debate where policymakers can draw broad, hard and fast lines about when, where and how PILI should be protected. This dynamic is driven by three features of the debate: (i) the debate involves few black-white participant positions; (ii) individual participants have multiple interests that are sometimes themselves in tension; and (iii) there is uncertainty in the very structure of the ITS privacy debate.

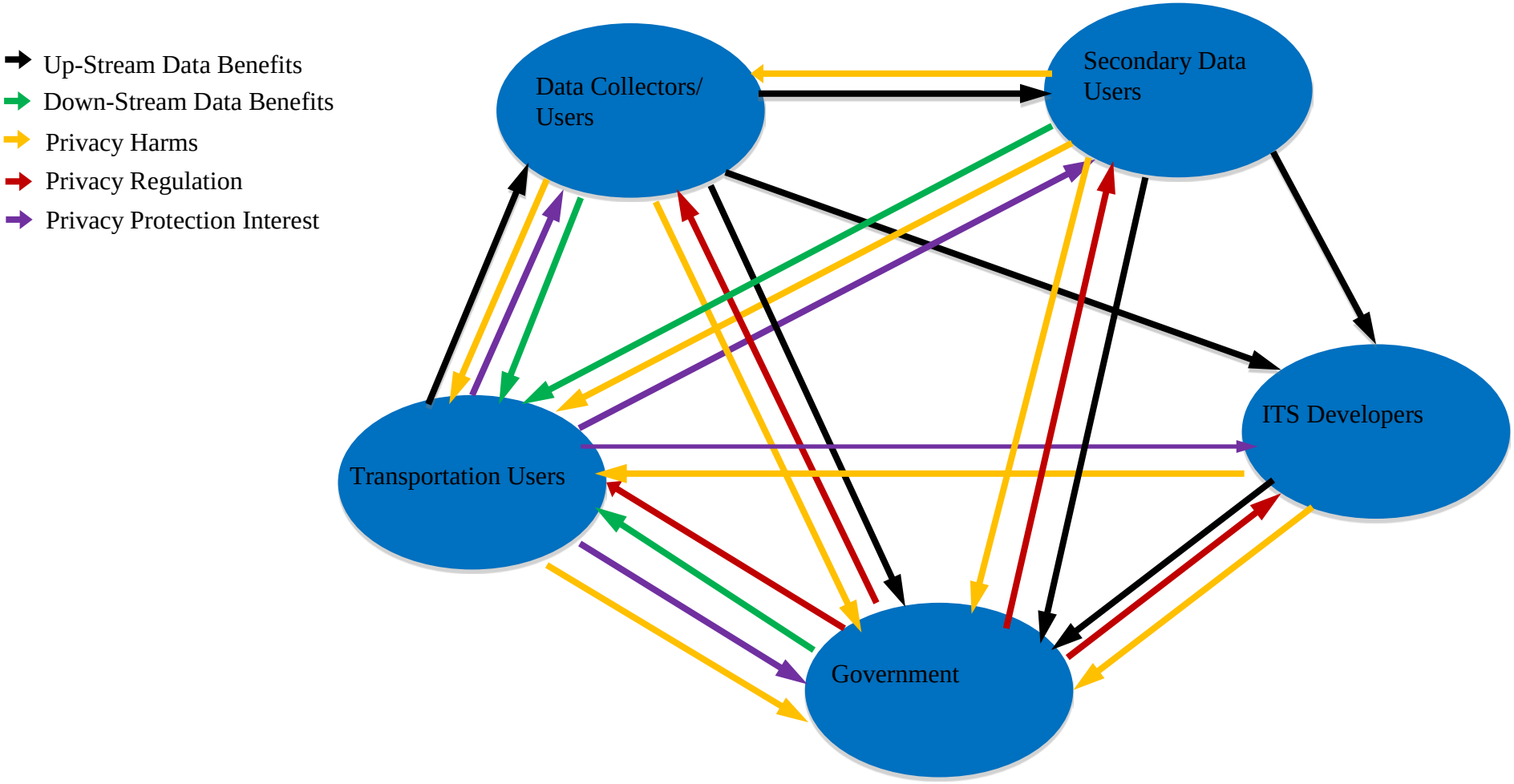
(i) *Few Black and White Participant Positions*. Among participants, there is no clear divide between a pro-privacy camp and a pro-collection/use camp. Rather, participant views are collectively more nuanced and multifarious. For example, it cannot be said that transportation users are simply pro-privacy and that data collectors/users are anti-privacy. Individuals exhibit a willingness to share their PILI in exchange for real benefits across a variety of circumstances (e.g., GPS navigation guidance, electronic tolling). There are limits to this willingness, albeit unclear, and open questions as to what extent the sharing is fully informed. Nevertheless, this widespread sharing of PILI by transportation users reflects that, for them, the protection of PILI does equate with not sharing PILI.

Similarly, for most participants that are collectors or users of PILI, more PILI is not necessarily better for their interests. Both in the private and public sector, PILI can have significant disadvantages in terms of greater costs for its protection, management, and possible production for law enforcement or litigants. The relative advantages and disadvantages of collecting and using more or less PILI vary across a wide range of actors. This makes it difficult to find blocs of PILI collectors and users, across industries, whose interests are clearly aligned over a single privacy enhancing policy. An exception to this generalization may be the large number of PILI collectors and users that would favor limitations on when they must produce data for litigation, when they are a non-party to the case.

The multifaceted and heterogeneous nature of participant interests and the number of different participants involved makes the ITS privacy debate difficult to map and navigate. On the other hand, it creates multiple pivot points in the debate where participants can match

or leverage their interests with other participants in seemingly unexpected ways to find solutions to the privacy problem. In this respect, it is better to see the ITS privacy debate not as having two competing sides, but rather as having a web of interlaced interests, with participants having both competing and congruent interests with respect to each other. Figure 1 shows a schematic drawing of this web.

Figure 5.1 Web of Interests in the ITS Privacy Debate



	Data Collectors/Users	Data Users	Transportation Users	Government	ITS Developers
Description	Private and public actors that both collect and use PILI from ITS.	Actors that use PILI from ITS, but do not collect it themselves.	Individual and commercial subjects of PILI collected from ITS.	Political, economic and regulatory role of government (not including role in collecting/using PILI)	Firms in the ITS technology and application supply chain
Examples	Tollway Authorities Car Rental Co.'s Employers Trans. Agencies	Marketers Litigants	Vehicle Owners Vehicle Drivers Vehicle Passengers	Legislatures Courts Regulatory Agencies	Hardware developers Software developers. Auto-Manufacturers

(ii) *Individual Participants Have Multiple Interests that are Often in Tension*. As this web analogy suggests, many participants have interests in PILI that pull them in different directions to one degree or another with regard to privacy. This is not only evidenced in the tension between the harm-prevention and benefit-pursuing interest of individuals or the cost-benefit analysis of data collectors and users, but also with the government. Regulatory and transportation agencies, for example, are pushed and pulled to various extents by the goals of protecting transportation-user privacy, improving the safety and efficiency of the transportation system through PILI-collecting ITS, and encouraging the economic benefits that come with increasing the flow of information in the transportation network. The tensions between these interests can be found both among regulatory agencies and within individual agencies.

These internally competing interests mean participant positions are likely to move, to some degree, over time as the balance between these interests shifts. Such shifts will be driven by technological, cultural and economic changes, forcing participants to recalculate the perceived benefits and risks associated with each interest. This suggests that the future of the ITS privacy debate will be marked less by the consolidation of participant positions and more by uncertainty as to what the relative strength of each participant's interests are.

(iii) There is Uncertainty in the Very Structure of the ITS Privacy Debate. The unsettled nature of the ITS privacy debate is reflected not only in changeability of participant interests but also the basic categories of the debate. As outlined at the outset of this report, the foundational categories of PILI and non-PILI themselves have become unstable due to technologies changes and shifting social norms about locational privacy and anonymity. Re-identification technology is turning what was once thought to be non-PILI into PILI. (141) Likewise, technological changes and privacy debates occurring largely outside the transportation sector (e.g., smart phones with GPS units, Facebook, etc.) are challenging traditional categories of what constitutes acceptable levels of locational anonymity. In the not too distant future, it is conceivable that the sharing of PILI may become so ubiquitous outside the transportation system, that the public may have far different expectations about the sharing of PILI within the transportation system than they currently do. (142) The public may in fact come to expect from the transportation system the benefits that may come with sharing large amounts of PILI. In other words, several foundational assumptions about privacy protection policy are in a period of seismic change.

Similarly, the divide between private and public-sector participants is being challenged. The law treats these participants differently with respect to their collection and use of PILI from ITS. Yet, in the context of the transportation system, the roles played by public and private actors are become increasingly blurred. It can no longer simply be assumed that given elements of the transportation system will be either managed or financed by the public sector. This reflects the historical trend, both within and without the transportation arena, of the lessening of the divide between private and public actors. It also reflects the fiscal challenges that the traditional public sector faces. Privately owned, as well as privately financed, transportation infrastructure is now commonplace as governments seek to reduce costs and find other sources of revenue.

> For ITS, this raises difficult questions about what privacy responsibilities does the private sector have when it collects PILI for a traditional public purpose and who owns the economic value of that data. Private-sector firms already operate ITS applications that collect PILI on behalf of the public sector, even in areas once thought the core domains of the public sector, such as law enforcement (e.g., red-light cameras).(143)
>
> Moreover, it raises the prospect that resource-strapped public-sector actors may use the economic value of PILI collected by ITS sources, to help pay for the cost of the transportation system. Scenarios can now be envisioned where ITS applications that exclusively serve and benefit the public transportation system are operated by private-sector companies and paid for by the value those companies can extract from the PILI collected by those applications. For example, an ITS service provider could be contracted by a public agency to install ITS infrastructure along a section of public roadway for some public transportation purpose, with the payment for doing so coming from the value the provider can gain from using the PILI collected by that infrastructure (e.g., through marketing or market analysis uses). In such scenarios, the conventional categories for assessing what data should be protected become increasingly incomplete and problematic.

However, the heterogeneous and somewhat fluid nature of the ITS privacy debate does not mean it is simply an impenetrable jumble of interests for policymakers. The participant analysis, in fact, suggests a number of dichotomies to help policymakers organize the ITS privacy debate and, in turn, develop policies for what types of PILI should be protected and what types of actors should be able to collect PILI and for what uses. The dichotomies include:

- Collecting and using PILI for commercial versus non-commercial purposes;
- Collecting and using PILI for purposes related to the core rationale of ITS technology (i.e., improving the safety, efficiency and sustainability of the transportation system), as opposed to collecting for some other purpose;
- Collecting and using PILI for law enforcement versus non-law enforcement purposes;
- Primary versus secondary uses of PILI; and
- PILI whose collection and use has been consented to by the subject of the data, as opposed to not having been consented to; and
- Collected data that still is useful in terms of its original purpose, versus data that is no longer needed for its original purpose.

These categories in many ways correspond with those identified in Appendix B, the "Taxonomy of Privacy Expectations and Legal Protections." These categories can be useful for policymakers in thinking about potential regulatory frameworks regarding the protection and collection of PILI from ITS sources; ones that makes choices about when PILI is protected and when it is not. We offer an illustrative example:

Divide PILI between:

(1) data collected and used for purposes directly related to the core rationale for ITS technology (i.e., improving the safety, efficiency and sustainability of the transportation system) and for which express consent cannot be reasonably obtained (e.g., red-light cameras); and
(2) data collected and used for purposes unrelated to this transportation rationale, or for which consent can be reasonably obtained (e.g., toll tag transponders).

For data in the first category, PILI can be collected without the explicit consent of the transportation user. But for data in the second category, express consent is required. PILI collected in this first category may only be used and retained by the collecting party for as long as needed for its original purpose, and thereafter deleted in a transparent fashion. The data should not be available to any other third parties for uses beyond its original purpose. The use of the PILI in the second category, collected via the consent route, is handled by the terms of the consent.

Such an example framework is attractive in its simplicity. It is, nevertheless, problematic in its details as it leaves many thorny privacy issues unaddressed. How broadly can the justification of the core rationale for ITS technology be extended? Does it include law enforcement? Does it include collection by private actors? If data in the first category is to be deleted after some period, can it be retained beyond that period if it has been anonymized? Furthermore, what is the scope of the consent regime? To what degree must consent be informed and how is it manifested?

The point here, though, is not the specific merits of this proposal, but that these dichotomies, while useful in defining boundary positions, are also problematic in that they can lead to absolutist thinking and notions that there is a grand, one-off framework with hard and fast rules that will solve the ITS privacy problem. As the participant analysis shows, there are a number of competing and heterogeneous interests in the ITS privacy debate and the strengths and merits of those interests vary by industry, participant role in the transportation system, and circumstances. As a result, policy solutions to the ITS privacy problem, for the foreseeable future, will likely necessarily be industry and sector specific, rather than having general applicability across all of ITS.

Thus, to the extent there is a single "best" approach to addressing the ITS privacy problem, it will be one that is highly contextual and iterative, that asks: When is the collection of PILI necessary in a certain setting? Are there non-PILI alternatives, if PILI has to be collected? How should it be handled? These dichotomies listed can help frame these questions in a given circumstance, but they do not necessarily provide broad, generalized solutions.

B. The use of PILI for Purposes Not Directly Beneficial to the Transportation System May Warrant Different Policy Treatment.

While the participant analysis does not point to clear divides in the ITS-privacy debate, which policymakers can target for broad solutions, it does highlight that there are a number of uses of PILI from ITS that provide little directly benefit to the transportation system.

At its core, the rationale for ITS technology is the benefits it brings to the transportation system in terms of improved safety, efficiency and mobility. In many ways, this is what justifies the privacy risks associated with the collection of PILI.

In turn, though, where PILI from ITS is used for purposes not directly serving the transportation system, the rationale for permitting that data use, at least from a privacy perspective, is greatly diminished. In such cases, the remaining rationale for such data use is often simply the general economic benefits that come from the free flow of information.

In many circumstances, this remaining economic rationale may not outweigh the privacy risks associated with such data use. In addition, it may also not outweigh the negative spillover consequences such use of PILI may have in terms of the public opposition it engenders for ITS data collection generally.

These considerations can be most clearly seen in the use of PILI from ITS sources by marketing firms and litigants. In the case of marketing, the use of PILI to refine and target advertisements generally provides no direct benefit to the transportation system. And while the use of PILI by litigants can benefit the transportation system in the adjudication of transportation related disputes (e.g., car accidents), there are wide variety of circumstances where the use of PILI from ITS by litigants brings no benefit to the transportation system.

Moreover, the use of PILI from ITS by marketing firms and litigants can be a deterrent to the use or sharing of PILI for purposes that do benefit the transportation system. For example, individuals may be less likely to support mileage-based usage charge systems if they believe that the PILI needed to operate such systems results in unwanted advertisements or could be used against them in legal disputes.

This idea of separating out what uses of PILI do not serve the transportation system does not simply result in drawing lines between public and private-sector data users. There are a number of private-sector data users whose interest in PILI is beneficial to the transportation system. For example, the use of PILI by auto insurers to more accurately price the risks of individual drivers has transportation safety and efficiency benefits. Likewise, there are public sector uses of PILI that do not serve the transportation system. For instance, the use of PILI from ITS by law enforcement for non-transportation reasons (e.g., investigation of non-transportation related crimes) does not improve the operation of the transportation system, and also chills the use of ITS applications that do benefit the transportation system.

Accordingly, it is often difficult to identify, *a priori*, when a given use of PILI benefits the transportation systems and when it does not. Nevertheless, some of the initial efforts to regulate PILI from ITS can be understood as attempting to draw this line. For example, several states have enacted laws that prevent tollway authorities from selling the PILI they collect and limiting the circumstances in which it may be released to litigants involved in legal disputes. (144) That is, policymakers may find identifying where the use of PILI from ITS sources benefits the transportation system a useful tool for sifting out what data uses warrant regulation in particular contexts.

There is, though, a large caveat to this analysis. The analysis ignores the economic reality that uses of PILI, unrelated to the transportation system, sometimes drive and pay for the collection of the PILI in the first place. This is most notable in the marketing and advertising uses of PILI. The type of data that marketers and advertisers want and what they are willing to pay for it, influences the decisions by data collectors about what PILI information they will obtain and store. Accordingly, to the extent that secondary uses unrelated to the transportation system pay for or otherwise enable the operation of ITS applications that do serve the transportation system, labeling a particular use of PILI as unrelated to the transportation system may not be a useful criteria for determining what uses of PILI to permit.

C. ITS Developers Will Play a Central Role in Addressing Privacy Concerns.

The participant analysis points to there being three main methods for mediating the intersection of participant interests: (i) legal rules; (ii) an opt-in or market structure; and (iii) technological architecture.

The first two methods have been well identified and much discussed in the ITS privacy debate. Laws can be used to prohibit or dictate the fashion in which PILI can be collected, used and stored. Opt-in or market mechanisms rely on the subjects of data collection to choose what data they want to share and what data they want to protect. Both of these approaches have their disadvantages. Laws in the privacy context can often be clumsy and inefficient, either too broad or too narrow to tackle the heterogeneous nature of the privacy problem. Opt-in or market mechanisms are undermined by the often enormous information asymmetries between the collector/user of the data and the one sharing that data.

The third approach has received less attention. It involves designing ITS applications to tackle privacy in the very nature of how they operate, so-called privacy-by-design. The key objective here is to design applications that do not collect PILI, but try to provide the same level of data utility that identified users need. (145) Examples of this approach include using advanced cryptography to eliminate the connection between an individual's locational information and the individual before it is collected in a database, while at the same time not eliminating the unique locational qualities of that information.

There are limits to privacy-by-design. (146) First, building privacy-enhancing features into ITS applications can make those applications more expensive, particularly to the extent they are added in later in the design process. Second, as the advances in re-identification technology and relational databases have shown, engineered fixed are not necessarily guaranteed long-term privacy solutions. Nevertheless, privacy-by-design represents one of the promising tools to help mediate the conflicts between transportation users and data collectors and users.

Furthermore, the prospect of the privacy-by-design approach brings technology developers to the fore in the privacy debate and makes them a central player. In this role, developers are no longer simply reactive to privacy concerns but one of the drivers in resolving them.

D. Many Conflicts between Participants on Privacy Issues are Not Zero-Sum.

Not surprisingly, the participant analysis reflects that the principle conflicts over privacy are between transportation users and the collectors and users of PILI. However, the analysis also shows that the relationship between these two sets of participants is a complicated one. While their interests with respect to PILI are conflicting in certain aspects, they are congruent in others. Moreover, the analysis shows there are multiple opportunities, or possible measures that can be taken, to maximize these congruent interests and minimize the conflicting interests. Table 2 outlines this dynamic with respect to several of the relationships between transportation users and the collectors/users of PILI from ITS.

Table 5.1 Mitigating Privacy Conflicts between Participants Over the Collection and Use of PILI.

	Participants	Congruent Interests	Conflicting Interests	Measures to Maximize Congruent Interests /Minimize Conflicting Interests
1	Transportation Users	• Improved the efficiency and cost-effectiveness of the transportation system.	• Prevent privacy-harms resulting from sharing PILI, including the sharing of the data with third parties, including law enforcement.	Rules • Time limits on data retention. • Prohibition on secondary uses of data. Technology Architecture • Offer opt-out option by accommodating pre-paid usage credits purchased anonymously. • Only collect data on vehicles, not drivers or vehicle occupants
	Operators of Transportation Systems	• Identifying vehicles with ITS to impose usage charges in order to better manage the traffic system (e.g., toll charges, HOT lanes, congestion pricing). • Collecting PILI creates risks and expense, including having to produce data for litigation and law enforcement.	• PILI is needed to manage customer accounts to process usage charges (e.g., credit card, vehicle registration information). • Money that can be made by selling data to secondary users.	
2	Transportation Users	• Want technologies that improve transportation safety, efficiency, and mobility with minimal loss of locational privacy.	• Prevent privacy-harms resulting from sharing PILI, including the sharing of the data with third parties, including law enforcement.	Rules • Increased privacy notice requirements will favor developers who include privacy-enhancing features. Technology Architecture

	Participants	Congruent Interests	Conflicting Interests	Measures to Maximize Congruent Interests /Minimize Conflicting Interests
	ITS developers	• Want to expand market for ITS technologies. • Competitive advantage in marketplace for those developers that include privacy-enhancing features in their products.	• Product design driven by client needs and PILI has greater utility for clients than non-PILI. • Incorporating privacy enhancing in products features is more expensive.	• Potential for "privacy-by-design" products that use ITS architecture to protect privacy of PILI or avoiding collecting PILI.
3	Transportation Users	• Vehicle tracking reduce costs for car rental companies, which in turn reduces rental costs for consumers.	• Privacy harms that may result if PILI transferred to third parties or law enforcement, or otherwise used for some secondary purpose. • Privacy expectation of no PILI being collected by the car rental company.	Rules • Time limits on data retention. • Prohibition on secondary uses of data or using data for uses unrelated to rental contract enforcement. • Data collection must be conspicuously disclosed in rental contracts. Doing so may allow market to price different data collection practices among car rental companies. • Car rental companies prohibited

	Participants	Congruent Interests	Conflicting Interests	Measures to Maximize Congruent Interests /Minimize Conflicting Interests
				from collecting PILI, as there are other means for adequately protecting their interests in contract enforcement.
	Car rental companies	• Vehicle tracking reduces costs through improved contract enforcement and increased efficiencies in vehicle fleet management. • Collecting PILI creates risks and expense, including having to produce data for litigation and law enforcement, or an obligation to inform law enforcement of suspected unlawful activities by drivers.	• Money that can be made by selling data to secondary users. • PILI can be used by car rental companies for purposes other than rental contract enforcement. • Disclosure of tracking devices to consumers may increase likelihood devices are removed or damaged by consumers.	Technology Architecture • Data retention/transmission only begins when certain conditions are triggered (e.g., vehicle goes outside geographic limits or vehicle is not returned).
4	Transportation Users	• Permitting the collection of PILI lowers insurance premiums.	• Privacy harms that may result if PILI transferred to third parties or law enforcement, or otherwise used for some secondary purpose.	Rules • Time limits on data retention. • Prohibition on secondary uses of data or using data for uses unrelated to underwriting. • Data collection and retention practices must be conspicuously disclosed in insurance agreement, to allow market differentiation of
	Auto-	• More accurate	• Money that can be	

	Participants	Congruent Interests	Conflicting Interests	Measures to Maximize Congruent Interests /Minimize Conflicting Interests
	Insurance Companies	underwriting of drivers. • Market advantage if insurer can underwrite usage based insurance without collecting locational data. • Collecting PILI creates risks and expense, including having to produce data for litigation or law enforcement.	made by selling data to secondary users. • PILI can be used by insurers for purposes other than underwriting decision-making.	practices with respect to PILI. • Insurers are already highly regulated and thus may be more receptive to regulations of PILI practices. Technology Architecture • Data collected does not need to include location information to underwrite all forms of usage-based insurance. Thus, ITS devices that collect data relevant for measuring usage (e.g., miles travelled, excessive speeds) but not location.
5	Transportation users	• Improved design and management of the transportation system and its traffic flows.	• Increased privacy expectations with respect to PILI collected because they are unaware data is being collected.	Rules • Prohibit the collection of PILI since most data needs can be met with non-PILI. Technology Architecture • Potential for "privacy-by-design" products that use ITS architecture to protect privacy of PILI or avoiding collecting PILI, while providing the same data benefits. Industry Practice • Do not collect PILI since most data needs can be met with non-PILI.
	Market and Traffic Analysis	• Most data needs can be met through anonymous data sets. • PILI data only has marginal value. • Collecting PILI creates risks and expense, including	• Collecting PILI increase the granularity of the analysis, and thus has greater utility. • Money that can be made by selling data to secondary users.	

	Participants	Congruent Interests	Conflicting Interests	Measures to Maximize Congruent Interests /Minimize Conflicting Interests
		having to produce data for litigation and law enforcement.		

In short, the analysis suggests that for a number of the conflicts between transportation users and data collectors/users, there are several avenues for finding common ground. These solutions vary from the straightforward (not collecting PILI since it is not necessary for the user's data needs or its costs outweigh its benefits), to the regulatory (laws limiting how long data is held and whether it can be transferred), to the engineered (building privacy into the architecture of ITS applications). In other words, many of the ostensible conflicts within the ITS privacy debate are not entirely intractable; there are tools available to address and mitigate them.

The participant analysis does not of course paint an entirely optimistic picture. There are conflicts for which the extent of potential common ground are far less and for which there are no clear possible paths forward. For example, in-vehicle navigation services, whose business model to some extent relies on being able to sell PILI they collect from users, are dependent both on collecting PILI and being able to deploy it for secondary uses. Thus, a simple prohibition of secondary uses amounts to a one-sided solution. On the other hand, relying on notices and consumer choice to protect privacy is problematic, given the practical limitations on how well consumer consent mechanism can be considered fully informed.

Moreover, the value of PILI, economic and otherwise, to data collectors should not be underestimated. Despite the risks associated with it, for many data-collecting participants, PILI is viewed as an enormous asset, and for which the potential uses have yet to be fully identified. In other words, there's a perception among data collectors that the opportunity costs of not collect PILI, even if not fully known at this point, outweigh the current costs in terms of data protection, responding to subpoenas, reputation risk, etc. As a result, even where there is potential for common ground, getting data collectors to move there will often be no small undertaking.

Chapter 6. Summary Recommendations.

This report represents a first effort in mapping and assessing the participant interests in the debate about privacy and the locational data collected about transportation users by ITS technology. The participant analysis shows that there is no simple divide among participants, between those who favor privacy protections and those who favor the ability to collect and use personally identifiable locational data (PILI). Rather, the analysis indicates the ITS privacy debate involves a web of interlaced interests among participants, some conflicting and some congruent. This debate structure results not only from a diverse set of participants but also from the piecemeal nature of American privacy law and the variety of transportation settings in which PILI is collected by ITS.

Importantly though, participant positions in this debate are not entrenched or settled, due to forces both within and without the transportation arena. Most significant of these are rapid technology changes and shifting privacy norms. The confluence of these two forces is redefining what locational privacy means. Re-identification technology is, for instance, making locational data once thought anonymous, into personally identifiable. Similarly, the public now accepts as commonplace certain ITS applications that regularly collect PILI and put it in the hands of others.

The net result is that participant interests in the privacy debate are notable for their context dependence and changeability. Participant positions vary with circumstances (e.g., where, when, how the data is collected) and over time, given how fast technology and society's privacy expectations are changing. As a result, from a participant perspective, finding policy solutions to the ITS privacy debate becomes a more nuanced and iterative endeavor: Is the collection of PILI necessary in a certain setting? Are there non-PILI alternatives? If PILI has to be collected, how should it be handled? Do the answers to these questions change over time?

For policymakers, this means that for the foreseeable future policy approaches to the ITS privacy problem will necessarily be sector and context specific. Attempts at broad, single-shot solutions will be undermined by the mix of heterogeneous participant interests, new technologies and shifting privacy norms.

When tackled at this smaller scale, the ITS-privacy debate reveals a number of potential avenues, or tools, for finding common ground for at least some of the most significant participant conflicts: those between transportation users and data collectors and users. These tools for common ground include:

<u>Rules</u>

- Time limits on data retention. This involves purging PILI in its entirety from databases, or at least removing its personally identifiable elements, after some defined period of time.
- Prohibition on secondary uses of data unrelated to the primary use or not consented to by the subject of the data collection.
  Technology Architecture

- "Privacy-by-design" techniques that use ITS architecture to increase the privacy of PILI or avoid collecting PILI, while still providing the needed level of data utility for identified end users.
  Industry Practice
- The practice of not collecting PILI where data needs can be met with non-PILI. This is particularly applicable where non-PILI is sufficient and the additional costs of collecting PILI, in terms of its protection and production for law enforcement and litigation, are considered.
- Implement privacy policies that call for: (i) the use of best practices for internal data management and security; and (ii) the use of clear privacy notices, where applicable so transportation users can make informed decisions about sharing PILI and which, in turn, encourages market differentiation among private-sector data collectors and ITS developers.

These measures can maximize, to some degree, the congruent privacy-enhancing interests of participants who are otherwise seemingly in direct conflict over privacy. In effect then, these tools amount to ways to move the privacy-debate forward with respect to certain participant conflicts.

While the participant analysis shows there are opportunities for progress in select areas of the ITS privacy debate, it also shows that there are substantial obstacles overall. These obstacles are essentially driven by the inescapable tension between, one the one hand, the utility of PILI and the means to collect vast amounts of it cheaply and easily from ITS and, on the other hand, the harms that PILI can cause to both individuals and companies, given the permanence of such information and the ease with which it can be shared. This tension is unlikely to abate any time soon. Better managing the tension will require a legal framework that better reflects the reality of locational technologies, as well as an ITS architecture with increased privacy capabilities. But more importantly, it will require better tools for sifting out under what conditions the transportation user wants his or her privacy protected and under what conditions the user is willing to forego privacy for the benefits that come with sharing PILI.

References

1. There has been strong public reaction to news about the extent to which many types of mobile devices, and their applications, collect locational data, without the full consent or knowledge of the user. See, e.g., Julia Angwin and Jennifer Valentino-Devries "Apple, Google Collect User Data" *Wall Street Journal*, April 22, 2011, available at http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html (last accessed June 1, 2012).

2. This is no more apparent that with the U.S. Supreme court which stated in *City of Ontario v. Quon*, 130 S. Ct. 2619, at 2629 (2010) that "the judiciary risks error by elaborating too fully on the [constitutional] implications of emerging technology before its role in society has become clear. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."

3. See, e.g., Neely Tucker "Controversial speed cameras cause gear-grinding among irked drivers," *The Washington Post*, November 5, 2009, available at http://www.washingtonpost.com/wp-dyn/content/article/2009/11/04/AR2009110404747.html?referrer=emailarticle (last accessed June 1, 2012), discussing efforts in Arizona and elsewhere to repeal legislation enabling photo enforcement cameras; also Larry Copeland, "Traffic cameras divide nation's drivers," *USA Today*, May 13, 2010 http://www.usatoday.com/news/nation/2010-05-13-traffic-cameras_N.htm (last accessed June 1, 2012), listing states that have laws prohibiting photo enforcement, and also discussing public concerns relating to these technologies.

4. *City of Ontario v. Quon*, Reference 2.

5. This issue has been the subject of previous work by the lead author of this report. Frank Douma and Jordan Deckenbach, "The Challenge of ITS for the Law of Privacy," *Journal of Law, Technology, & Policy* 295, 325 (2009); Frank Douma and Sarah Aue, "ITS and Locational Privacy: Suggestions for Peaceful Coexistence," *Journal of Transportation, Law, Logistics and Policy Technology and Policy*, 2nd Qtr, 78(2), 89 (2011).

6. For a discussion of the history of ITS in the United States, see Dorothy J. Glancy, Privacy on the Open Road (The Twenty-Seventh Annual Law Review Symposium Privacy and Surveillance: Emerging Legal Issues) 30 *Ohio N.U. L. Rev*. 295 (2004).

7. U.S. Department of Transportation, RITA, "ITS List of FAQ's," available at http://www.its.dot.gov/faqs.htm, (last accessed June 1, 2012).

8. U.S. Department of Transportation, RITA, Reference 7.

9. Douma and Deckenbach, Reference 5; Douma and Aue, Reference 5.

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

11. *United States v. Knotts*, 460 U.S. 276 (1983).

12. *City of Ontario v. Quon*, Reference 2.

13. *United States v. Jones 132* S. Ct. 945 (2012).

14. *Driver's Privacy Protection Act of 1994*, 18 U.S.C. §§ 2721-25; *Privacy Act of 1974*, 5 USC Sec. 552a.

15. Section 5 of the *Federal Trade Commission Act (FTC Act)*, 15 U.S.C. §45(a), prohibits unfair or deceptive acts or practices in or affecting commerce.

16. H.R. 2168: *Geolocational Privacy and Surveillance Act*, available at http://www.govtrack.us/congress/billtext.xpd?bill=h112-2168; and S.1223: Location Privacy Protection Act of 2011 http://www.govtrack.us/congress/bill.xpd?bill=s112-1223 (last accessed June 1, 2012).

17. See e.g., Kendra Roseberg, "Location Surveillance By GPS: Balancing An Employer's Business Interest With Employee Privacy," 6 *Wash J.L. Tech. & Arts* 143 (2010).

18. This issue was covered in more depth in a recent report on online privacy from the U.S. Department of Commerce, National Telecommunications and Information Administration, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, (2010), available at http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf (last accessed June 1, 2012).

19. Douma and Deckenbach, Reference 5.

20. Douma and Deckenbach, Reference 5.

21. For a discussion, see Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," 57 *UCLA Law Review* 1701 (2010).

22. Federal Trade Commission (Bureau of Consumer Protection), *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (March 26, 2012), available at http://ftc.gov/os/2012/03/120326privacyreport.pdf (last accessed June 1, 2012).

23. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change,* Reference 22.

24. The closest to an existing participant analysis of ITS privacy issues is V. Briggs and C.M. Walton, *The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data.* Research Report SWUTC/00472840-00075-1, Southwest Region University Transportation Center, Austin, TX, 2000, available at http://swutc.tamu.edu/publications/technicalreports/472840-00075-1.pdf (last accessed June 1, 2012).

25. A. Friedman and S. Miles, *Stakeholders: Theory and Practice*, Oxford University Press: Oxford, 2006.

26. Ohm, Reference 21.

27. C. Cottrill, "Overview of Approaches to Privacy Preservation in Intelligent Transportation Systems and Vehicle Infrastructure Integration Initiative," *Transportation Research Record: Journal of the Transportation Research Board* Vol. 2129, pp. 9-15 (2009); Andrew J. Blumberg and Peter Eckersley, *On Locational Privacy, and How to Avoid Losing it Forever*, Electronic Frontier Foundation, available at https://www.eff.org/wp/locational-privacy Foundation (last accessed June 1, 2012).

28. Blumberg and Eckersley, Reference 27.

29. ITS America, "ITS America's Fair Information and Privacy Principles," ITS America (2011) http://www.itsa.org/images/mediacenter/itsaprivacyprinciples.pdf (last accessed June 1, 2012); Leslie Jacobson, "VII Privacy Policies Framework, Version 1.0.2," The Institutional Issues Subcommittee Of The National VII Coalition (February 16, 2007), available at http://www.nevadadot.com/uploadedFiles/privacy-policy.pdf (last accessed June 1, 2012).

30. See Alessandro Acquisti & Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy*, 3(1) 2005, 26-33, available at http://www.eecs.harvard.edu/cs199r/readings/acquisti.pdf (last access June 1, 2012).

31. Daniel J. Solove, "Essay: Fourth Amendment Pragmatism," 51 *B.C. L. Rev.* 1511 (2010).

32. Solove, Reference 31.

33. Acquisti and Grossklags, Reference 30.

34. Acquisti and Grossklags, Reference 30.

35. Solove, Reference 31.

36. Glancy, Reference 6.

37. For a list of whom state's with traffic law enforcement cameras and other automatic enforcement devices hold responsible for violations, *see* Insurance Institute For Highway Safety "Automatic Enforcement Laws," available at http://www.iihs.org/laws/automated_enforcement.aspx (last accessed October 13, 2011).

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

39. Douma and Deckenbach, Reference 5.

40. Douma and Deckenbach, Reference 5.

41. For a discussion, *see* Roseberg, Reference 17.

42. Governors Highway Safety Association, Graduated Driver Licensing Laws, February 2011, available at http://www.ghsa.org/html/stateinfo/laws/license_laws.html (last accessed June 1, 2012).

43. *See* e.g., Max Donath, Project Summary, *Smartphone Based Novice Teenage Driver Support System*, University of Minnesota Center for Transportation Studies (2011), available at http://www.its.umn.edu/Research/ProjectDetail.html?id=2009015 (last accessed June 1, 2012).

43. Shawn Brovold, Nic Ward, Max Donath, Stephen Simon, *Developing Driving Support Systems to Mitigate Behavioral Risk Patterns Among Teen Drivers*, University of Minnesota Center for Transportation Studies (2007), available at hhttp://www.its.umn.edu/Publications/ResearchReports/reportdetail.html?id=1422 (last accessed June 1, 2012).

43. Neil Lerner, James Jenness, Jeremiah Singer, Sheila Klauer, Suzanne Lee, Max Donath, Michael Manser, & Nicholas Ward, *An Exploration of Vehicle-Based Monitoring of Novice Teen Drivers: Final Report*, Report number DOT HS 811 333, (2010), available at http://www.nhtsa.gov/Research/Human+Factors/Teen+Drivers (last accessed June 1, 2012).

44. Douma and Aue, Reference 5.

45. Dawn C. Marshall, Robert B. Wallace, James C. Torner, and Michelle Birt Leeds, "Enhancing the Effectiveness of Safety Warning Systems for Older Drivers: Project Report" *National Advanced Driving Simulator, University of Iowa, Report prepared for*

the U.S. Department of Transportation (2010), available at http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2010/811417.pdf (last accessed June 1, 2012).

46. There are a number of products on the market that allow the video recording of a vehicle's passenger compartment, and thus the identification of passengers. *See e.g.*, DriveCam, Inc. company website, http://www.Drivecam.com (last accessed June 1, 2012).

47. U.S. Department of Transportation, RITA, Reference 7.

48. Briggs and Walton, Reference 24.

49. Briggs and Walton, Reference 24.

50. Briggs and Walton, Reference 24.

51. Briggs and Walton, Reference 24.

52. Ryan Fries, Mashrur A Chowdhury, and Mostafa Reisi Gahrooei, "Maintaining Privacy While Advancing Intelligent Transportation Systems Applications -- An Analysis," Proceedings of the Transportation Research Board Annual Meeting, January 23-27, 2011, Washington, D.C., available at http://www.siue.edu/~rfries/2011-TRB-Privacy%20with%20ITS.pdf (last accessed June 1, 2012).

53. Briggs and Walton, Reference 24.

54. R. Clarke, "How to Ensure that Privacy Concerns Don't Undermine e-Transport Investments," Presented at AIC e-Transport Conference, July 27-28, 2000 Melbourne Australia, available at http://www.rogerclarke.com/EC/eTP.html (last accessed June 1, 2012).

55. Fries, et al., Reference 52.

56. For a synopsis *see*, Douma and Deckenbach, Reference 5; Glancy, Reference 6.

57. See e.g., N.H. Rev. Stat. Ann. 236.130 (2006) (state statute limiting when state actors can use ITS technology to determine the ownership of a motor vehicle or the identity of a motor vehicle's occupants on public roads).

58. This may account, in part, for the large amount of funds and energy the U.S. Department of Transportation has spent on ITS research. Glancy, Reference 6.

59. Stephen Ezell, "Explaining International IT Application Leadership: Intelligent Transportation Systems," Information Technology and Innovation Foundation (December 2010), available at http://www.itif.org/publications/explaining-international-it-

application-leadership-intelligent-transportation-systems (last accessed June 1, 2012); IEEE-USA, "Position Statement: U.S. Economic Competitiveness and Intelligent Transportation Systems Technology," (February 12, 2010), available at http://www.ieeeusa.org/policy/positions/ITS.pdf (last accessed June 1, 2012).

60. Eric Engleman, "GM's OnStar Tracking Needs Probing: Senator," *Bloomberg News*, September 26, 2011, available at http://www.bloomberg.com/news/2011-09-26/gm-s-onstar-tracking-needs-probing-senator.html (last accessed June 1, 2012).

61. Keith Barry, "Automotive Black Boxes, Minus the Gray Area," *Wired.com*, May 23, 2011, available at http://www.wired.com/autopia/2011/05/automotive-black-boxes/ (last accessed October 13, 2011).

62. U. S. Department Of Transportation, Federal Highway Administration, *Privacy Impact Assessment: Mileage-Based Road User Charge System* (NEMBRUCS), May 29, 2009, available at http://www.dot.gov/pia/fhwa_nembrucs.htm (last accessed June 1, 2012).

63. For example, Section 5 of the Federal Trade Commission Act (15 USC 45) prohibits ''unfair or deceptive acts or practices" and most states have analogous consumer laws. Also, some states, including Maine, Colorado, California and New Hampshire, have, statutes that require disclosure of data tracking devices that are included in cars by auto manufactures. Cal. Veh. Code § 9951 (2003); Col. Rev. Stat 12-6-401 (2006); New Hampshire Revised Statutes Annotated, 357-G:1 (2006); Me. Rev. State Ann. 29-A 1972. Virginia has a statute that goes further and requires an owner's consent for any device that collects electronic information from a car, not just from those devices installed by an auto-manufacturer, except in selected circumstances. Va. Code Ann. § 46.2-1088.6.

64. With regarding to the extent of the data breach problem, see the Privacy Rights Clearinghouse which tracks the public reported data breaches since 2005. Privacy Rights Clearinghouse, "Chronology of Data Breaches Security Breaches 2005 – Present, available at http://www.privacyrights.org/data-breach (last accessed June 1, 2012).

65. Clarke, Reference 54.

66. The form and content of privacy policies vary, but there are widely-recognized concepts on which they typically built. See the Federal Trade Commission, "Fair Information Practice Principles" available at http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last accessed June 1, 2012).

67. For example, under federal law, financial institutions and health care service providers are required to have privacy policies. *Gramm–Leach–Bliley Act* 15 U.S.C. § 6801-6810; Health Insurance Portability and Accountability Act of 1996, Pub.L. 104-191. In addition, some states have broader laws requiring companies to have privacy

policies, most notably of these is California's "Shine the Light" law, CA Civil Code § 1798.83.

68. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, Reference 22.

69. Janie Ho, "GPS Keeping Tabs On Car Rentals" *CBS News*, February 11, 2009, available at http://www.cbsnews.com/stories/2004/03/06/eveningnews/main604461.shtml (last accessed June 1, 2012); Daryl Lubinsky, "GPS Tracking the Right Way: Disclosure, Fees and Recovery", *Auto Rental News*, September/October 2011, available at http://www.autorentalnews.com/Article/Story/2011/09/GPS-Tracking-the-Right-Way-Disclosure-Fees-and-Recovery/Page/3.aspx (last accessed June 1, 2012).

70. Lubinsky, Reference 69.

71. Lubinsky, Reference 69.

72. Lubinsky, Reference 69.

73. Lubinsky, Reference 69.

74. Leah Altaras, *Follow that Car! Legal issues arising from installation of tracking devices in leased consumer goods and equipment*, 3 Shidler J. L. Com. & Tech. 8 (Feb. 14, 2007), available at http://www.lctjournal.washington.edu/Vol3/a008Altaras.html (last accessed June 1, 2012); and Robert Lemos, "State puts brakes on GPS speeding fines," *CNET News*, July 2, 2001, available at http://news.cnet.com/State-puts-brakes-on-GPS-speeding-fines/2100-1040_3-269388.html (last accessed June 1, 2012).

75. Cal. Civ. Code § 1936(6)(o) (2002); Consolidated Laws of New York, General Business § 20 Article. 26 § 396-z (2006).

76. Roseberg, Reference 17.

77. Roseberg, Reference 17. An exception to this is when a collective bargaining agreement prevents an employer from using location-monitoring devices with respect to union employees, since collective bargaining agreements are covered by the National Labor Relations Act. 29 U.S.C. § 151–169

78. Conn. Gen. Stat. § 31-48d (2003).

79. Roseberg, Reference 17.

80. Roseberg, Reference 17.

81. Roseberg, Reference 17.

82. *See e.g.*, Mark Whitney, "The Impact of Emerging Technologies on Employee Privacy," *Legal Update: Morgan, Brown & Joy, LLP*, November 19, 2010, available at http://www.morganbrown.com/legal/legal_update.php?id=210#_edn38 (last accessed June 1, 2012); see also California Penal Code Section 637.7, which requires the employee's consent if the employee is the owner of the vehicle.

83. Carroll Lachnit, "Pay-As-You-Drive Insurance Goes Into High Gear," *Edmunds.com*, February 2, 2011, available at http://www.edmunds.com/auto-insurance/pay-as-you-drive-insurance-goes-into-high-gear.html (last accessed June 1, 2012).

84. Lachnit, Reference 83.

85. Safeco's Teensurance Safety Beacon, available at https://www.teensurance.com/beacon.aspx (last accessed June 1, 2012).

86. Safeco's Teensurance Safety Beacon, Reference 85.

87. Virginia is one of the few states to address the use of ITS data by auto insurers. It has a statute that prohibits insurers for treating consumer's differently, aside from setting different, if they refuse to provide the insurer ITS generated data. Va. Code Ann. § 38.2-2213.1

88. Briggs and Walton, Reference 24.

89. Briggs and Walton, Reference 24.

90. Baik How, Marco Gruteser , Ryan Herring , Jeff Ban A , Dan Work , Juan-carlos Herrera , Re Bayen , Murali Annavaram , and Quinn Jacobson, "Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring" *IEEE Transactions on Mobile Computing*, 2011, available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.144.7599 (last accessed June 1, 2012).

91. Briggs and Walton, Reference 24.

92. Travis Madsen and Phineas Baxandall, *Caution: Red Light Cameras Ahead; The Risks of Privatizing Traffic Law Enforcement and How to Protect the Public*, CALPIRG Education Fund (October 2011), available at http://www.calpirg.org/reports/cap/caution-red-light-cameras-ahead-risks-privatizing-traffic-law-enforcement-and-how (last accessed June 1, 2012).

93. This principle is reflected in certain privacy laws that the government actions are subject to, which provide that if a contractor is hired to perform an action covered by the privacy statute the contractor is subject to the privacy law to the same extent the

government would have been if it had performed that action. See e.g., *The Privacy Act Of 1974*, 5 U.S.C. § 552a(m)(1).

94. Briggs and Walton, Reference 24.

95. Briggs and Walton, Reference 24.

96. Baik How, et al., Reference 90.

97. Baik How, et al., Reference 90.

98. Douma and Deckenbach, Reference 5.

99. Fries, et al., Reference 52.

100. "California Legislature Passes Toll Road Privacy Bill" *TheNewspaper.com* (August 5, 2010), available at http://www.thenewspaper.com/news/32/3241.asp (last accessed June 1, 2012).

101. See e.g., *Wemhoff v. District of Columbia*, No. 04-CV-1310 , District Of Columbia Court Of Appeals, 887 A.2d 1004; 2005 D.C. App. LEXIS 645, November 9, 2005.

102. *Driver's Privacy Protection Act of 1994*, Reference 14.

103. *Driver's Privacy Protection Act of 1994*, Reference 14.

104. For a synopsis *see*, Douma and Deckenbach, Reference 5; Glancy, Reference 6.

105. *United States v. Jones*, Reference 13 (J. Alito, concurrence).

106. See e.g., Section 215 of the *Patriot Act*.

107. See e.g., *Company v. United States* (*In re United States*), 349 F.3d 1132 (9th Cir. Nev. 2003) (FBI could not require a telematic service provider to use their system to intercept in-vehicle conversations of a suspect because doing so would interference with the provider's service to the customer).

108. Insurance Institute For Highway Safety, "Summary of decisions concerning automated enforcement," available at http://www.iihs.org/laws/auto_enforce_cases.html (last accessed June 1, 2012).

109. See, e.g., Tucker, Reference 3; also Copeland, Reference 3.

110. *See* Insurance Institute For Highway Safety, "Automatic Enforcement Laws," Reference 37.

111. For a synopsis *see*, Douma and Deckenbach, Reference 5.

112. *City of Ontario v. Quon*, Reference 2.

113. See e.g., *Cunningham v. New York State Department of Labor*, N.Y. App. Div., 2011 NY Slip Op 08529, which held the government could permissible monitor an employee's travel in connection with an investigation of that employee's misconduct. A state agency was permitted to install a GPS device on an employee's vehicle for purposes investigating whether the employee was submitting false timesheets.

114. See e.g., *Privacy Act of 1974*, Reference 14.

115. Massachusetts Public Interest Research Group, "Out of the Shadows: Massachusetts Quasi-Public Agencies" (2010), available at http://www.masspirg.org/home/reports/report-archives/tax-amp-budget/tax-amp-budget3/out-of-the-shadows-massachusetts-quasi-public-agencies-and-the-need-for-budget-transparency (last accessed June 1, 2012).

116. Massachusetts Public Interest Research Group, Reference 115.

117. Massachusetts Public Interest Research Group, Reference 115.

118. Massachusetts Public Interest Research Group, Reference 115.

119. Heavy Vehicle Licenses Plate, Inc., company website, available at http://www.helpprepass.com/ (last accessed June 1, 2012).

120. Heavy Vehicle Licenses Plate, Inc., Reference 119.

121. Reference 115.

122. Rani Gupta, "Privatization v. The Public's Right to Know," Reporters Committee for the Freedom of the Press (2007), available at http://www.rcfp.org/rcfp/orders/docs/PRIVATIZATION.pdf (last accessed June 1, 2012), describing how many state freedom of information statutes do not address the public disclosure requirements of quasi-public entities.

123. Briggs and Walton, Reference 24.

124. See e.g., *Illinois Tollway Act*, 605 ILCS 10/19.1, detailing the privacy obligations of the Illinois Tollway Authority.

125. Rachel Greenstadt and Michael D. Smith, "Protecting Personal Information: Obstacles and Directions," *Proceedings of the Fourth Annual Workshop on Economics and Information Security*, Cambridge, Massachusetts, May 2005, available at http://infosecon.net/workshop/pdf/48.pdf (last accessed June 1, 2012).

126. Briggs and Walton, Reference 24.

127. Aaron Strout, "Location: The Last Third of the Holy Trinity of Data," *WCG Company, Common Sense Blog* (2011), available at http://blog.wcgworld.com/2011/09/location-last-third-of-the-holy-trinity-of-data (last accessed October 13, 2011).

128. Strout, Reference 127.

129. Strout, Reference 127.

130. David M. Raab, "Marking in a Data Rich World," *Information Management Magazine,* August 2005, available at http://www.information-management.com/issues/20050801/1033585-1.html?zkPrintable=true (last accessed June 1, 2012).

131. *CAN-SPAM Act of 2003*, 15 U.S.C. 7701, et seq; *Telephone Consumer Protection Act of 1991*, 47 USC 227.

132. Greg Cragg, "OnStar Begins Selling Recorded User Information" *Newsletter: Law firm of Khorrami Pollard & Abir, LLP*, September 23, 2011, available at http://www.consumeradvocatelegalupdate.com/2011/09/articles/consumer-fraud/onstar-begins-selling-recorded-user-information/ (last accessed June 1, 2012).

133. See e.g., *Villanova v. Innovative Investigations, Inc*., 420 N.J. Super. 353 (App.Div. 2011).

134. See e.g., *In re Fannie Mae Securities Litigation*, 555 F.3d 814 (D.C. Cir. 2009) (non-party incurred $6 million in fees and costs in complying with subpoena for data). The Federal Rule of Civil Procedure do provide some protection to non-parties in terms of the cost and burden of producing data. *See* Federal Rule of Civil Procedure 45(c) and (d). Requests for information from non-parties are not to impose "an undue expense or burden on non-parties, and non-parties are to be protected from "significant expense" in producing the data.

135. See e.g., Federal Rule of Civil Procedure 26, 34 and 45.

136. See e.g., Federal Rule of Civil Procedure 26(b)(1). "Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."

137. See e.g., *Pearson v. Mille*r, 211 F.3d 57, 65 (3d Cir. Pa. 2000). "The court, in its discretion, is authorized [by Federal Rule of Civil Procedure 26(c)] to fashion a set of limitations that allows as much relevant material to be discovered as possible, while preventing unnecessary intrusions into the legitimate interests--including privacy and

other confidentiality interests--that might be harmed by the release of the material sought."

138. In 2006, the Federal Rules of Civil Procedure were revised to facilitate electronic discovery. There is evidence that this has increased the number of discovery requests, to both public and private organizations, to produce stored electronic data for litigation. For an overview, see John H. Beisner, "*Discovering A Better Way: The Need for Effective Civil Litigation Reform*," 60 *Duke L.J*. 547, 564-70 (2010) (discussing how electronic discovery has increased the costs and volume of material associated with discovery).

139. Paul Spinrad, "Big Network is Watching You" *Innovations: Research & News From Berkeley Engineering*, 3(2), 2009, available at http://innovations.coe.berkeley.edu/vol3-issue2-feb09/johncanny (last accessed June 1, 2012). Under the Federal Rules of Civil Procedure, it not clear when a non-party's duty to preserve potential evidence for litigation begins. Gary M. Pappas, "Guidelines for Nonparty E-Discovery under Rule 45," *American Bar Association* (2012), available at http://apps.americanbar.org/litigation/committees/businesstorts/articles/041510_pappas.html.

140. Deleting data does not necessarily free data holders from the burdens of producing data. See e.g., *In Tener v. Cremer*, 2011 N.Y. Slip op. 6543 (1st Dep't 2011), even though the non-party had "overwritten" the relevant data a number of times did not necessarily mean, it still had an obligation to see if it could retrieve the ostensibly deleted data could be retrieved using forensic software.

141 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, Reference 22.

142. Jeffery Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, Brookings Institution (May 2, 2011), available at http://www.brookings.edu/papers/2011/0502_free_speech_rosen.aspx (last accessed June 1, 2012).

143. Madsen and Baxandall, Reference 92.

144. *Illinois Tollway Act*, 605 ILCS 10/19.1; *California Streets and Highways Code Sections* 31490

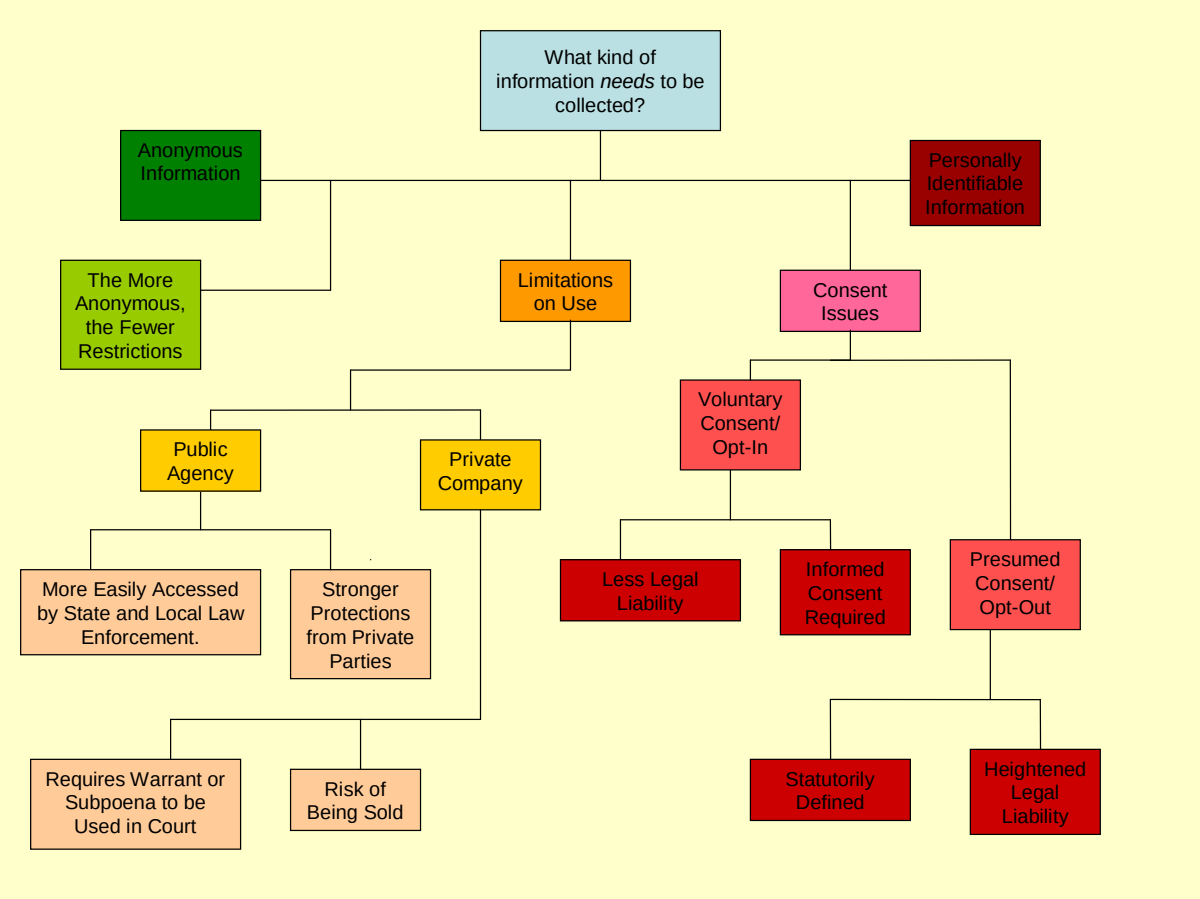
145. Blumberg and Eckersley, Reference 27.

146. For a summary, see Cottrill, Reference 27.

Appendix A

Toolbox for Identifying Privacy Issues

Figure A-1: Toolbox for Identifying Privacy Issues



Appendix B

Taxonomy of Privacy Expectations and Legal Protections

Table B-1: Taxonomy Of Privacy Expectations And Legal Protections

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