LEGISLATIVE SUMMARY: ETHICS OF GOVERNMENT USE OF DATA COLLECTED VIA INTELLIGENT TRANSPORTATION SYSTEMS

[Full Report at www.michigan.gov/documents/mdot/MDOT_EthicsDataCollectedITS_394489_7.pdf]

INTRODUCTION

Michigan is a recognized leader in both connected vehicle technology and the larger realm of intelligent transportation systems (ITS), and its expertise and leadership in this area is a competitive advantage for the state and its automotive industry. Current Michigan law permits deployment of most connected vehicle technologies, and connected vehicles already are being tested in the state. While taking full advantage of this technology and gaining the benefits of connected vehicles and their wide deployment in Michigan and nationwide, legislative action may need to be considered to ensure that the state protects the privacy and data security of its citizens.

The convergence of sensing, wireless communications, and multi-media platforms has provided new opportunities for the development of a fully connected transportation system. Connected vehicles can collect real-time data related to travel time, pavement condition, vehicle condition, and more. Together, ITS and connected vehicle technology enable dissemination of real-time traffic and other information to motorists, increased efficiency of transportation networks, and improved system management.

While deploying ITS and connected vehicle technology improves the safety and efficiency of the transportation system, these technologies also introduce potential ethical concerns and raise questions regarding personal privacy, tracking, data ownership, and security. Such concerns must be addressed to the satisfaction of the public, transportation system operators, and other stakeholders to encourage broad adoption of these technologies and realization of their many benefits.

FINDINGS AND RECOMMENDATIONS

Legal Environment: The U.S. lacks an overarching information privacy law governing government agencies and private businesses. While the U.S. has federal and state laws that regulate collection and management of personal information within government agencies, as well as laws that regulate use of consumer data in specific industries, such regulation is a patchwork of legal provisions that lacks national consistency.

The federal government has not adopted a set of privacy policies for ITS applications. Both the Federal Highway Administration (FHWA) and the National Highway Traffic Safety Administration (NHTSA), however, have authored reports on connected vehicles that outline design goals related to privacy. Neither agency references formal laws or regulations in these reports. Federal sources provide only limited guidance on transportation-related privacy issues, especially with respect to ITS applications.

Identifiable Information: Agencies should collect only needed data and use anonymous information whenever possible to reduce legal liabilities and requirements. For applications that require personally identifiable information (e.g., electronic toll collection, Global Positioning System (GPS)-enabled insurance, and vehicle mileage fees), disclosure and consent will be a prerequisite to data collection. Informed consent mechanisms can be used to limit liability.

Anonymity: Anonymity can be addressed through two approaches: “anonymity by design” and “anonymity by policy.” Anonymity by design uses multiple technical controls that reduce the ability to determine the identities of vehicles and individuals from data exchanges or information from a system log file. Anonymity by policy uses commercial wireless networks, but focuses on securing access to the network itself, rather than on stripping away identifiable information. Anonymity by design provides the maximum anonymity and is preferable when it is feasible and can support desired applications.

Privacy-Quality Tradeoff: Advanced data suppression techniques and system design architecture, such as separating communication and traffic servers, using encryption, and sepa-

rating identity and location related processing, can be used to balance the tradeoff between privacy and quality of ITS information.

Outreach: Educational initiatives, focus groups, demonstrations, and media events can facilitate public acceptance by helping constituents realize why data is being collected, understand that only necessary data is being collected, and perceive benefits to data collection and use.

Freedom of Information Act: While ITS data held by public entities could be publicly accessible under state and federal Freedom of Information Acts (FOIA); public agencies can take actions to protect the data by seeking special exemptions from legislatures.

Private Sector: Public-private partnerships can be used to increase both societal and individual benefits of data collection and use. Outsourcing data management and information technology operations to a third party can also reduce liability for public agencies. Commercial management and use of data can be governed by contracts.

SPECIFIC APPLICATIONS

Intelligent transportation systems must be designed to provide maximum constituent privacy while ensuring that the particular application in question is able to function. MDOT is particularly concerned with protecting constituent privacy with respect to data collected and used in connected vehicle applications, including traffic safety, traffic control, asset management, and usage-based mileage fees. These and other examples of ITS data collection and locational privacy are presented in Table 1. Michigan law currently allows deployment of most connected vehicle technology, but does not allow use of connected vehicle data for user-based mileage fees.

Traffic safety, traffic control, and asset management applications are all possible using anonymous data that contain no personally identifiable information. These applications should employ an "anonymity by design" approach that uses anonymous data and limits information that could be used to track and identify vehicles and participants. To limit tracking, vehicles can transmit messages without a unique identifier (or regularly change their identifier) and report location in terms of a zone or road segment instead of a precise point. For example, a pothole detection application does not require information that identifies the exact cars driving over potholes, just the location and severity of the detected potholes.

Protecting constituent privacy for usage-based mileage fee applications could be more difficult, but could also make use of anonymous data (e.g., drivers could use prepaid cards so payments would not need to be attached to a particular driver or car). In addition, rather than transmitting GPS tracking information, a vehicle could simply send out a summary of miles traveled; for a system by which tolls are variable based on time of day and type of road, an aggregate summary compiled over a longer period of time could be used (e.g., a monthly calculation of miles traveled by category of road and time of day could be created for tax assessment purposes).

Table 1: Examples of ITS Data Collection Techniques and Locational Privacy

Data Collection Techniques	Use(s) of Data Collected	Vehicle Information & Identification	Driver & Occupant Information & Identification	Privacy Expectation & Legal Protection
Loop Detectors	Volume, Vehicle Class, Speed, Estimated Travel Time, and Incident Detection	No Individual Vehicle Information Obtained	None	None
Video Image Detectors	Vehicle Class, Estimated Speed, Volume, and Incident Detection	Individual Vehicle Information Likely Obtained	None	Medium
Infrared & Thermal IR Cameras	Occupant Observation	Vehicle Identification Likely Obtained	None	Medium
Toll Transponder	Origins and Destinations, Volume, and Average Speed	Vehicle Identification Obtained	Possible through Vehicle Registration System	Medium
License Plate Reader	Origins and Destinations, Average Speed and Travel Time	Vehicle Identification Obtained	Possible through Vehicle Registration System	Medium
GPS-enabled Mobile Phones or Probe Vehicles	Real-time Vehicle Location, Travel Paths, Speed, Origins and Destinations	Vehicle Identification Likely Obtained	Possible through Vehicle Registration System and Telecommunication Records	High