Examining Privacy and Surveillance in Urban Areas: A Transportation Context

Caitlin D. Cottrill
Urban Transportation Center, UIC
412 S. Peoria St., Suite 340, CUPPA Hall
Chicago, IL 60607
Phone: +1-312-996-4820
Fax: 312-413-0006
ccottr2@uic.edu

Abstract:
In the post-9/11 world, trade-offs between safety, security and privacy have received an increasing amount of attention and discussion. Particularly within the realm of transportation, it is evident that no clear bright line exists as to the degree to which travelers are willing to exchange their "privacy in public" for an increased measure of safety and security. While certain invasions of privacy are generally accepted as being "critical" to ensuring safety and security (such as scanning of personal effects when flying or GPS-equipped cell phones) and are therefore submitted to with some degree of aacceptance, other forms of surveillance (such as red light cameras) are regarded as being invasive without providing concomitant benefits, and are thus argued against in public meetings and, eventually, the courts. It is interesting to ask, then, what forms of transportation surveillance currently being implemented or proposed are most likely to be accepted or rejected within the context of the urban environment, and to what extent will questions of equity and fairness impact these responses? It is critical, at this juncture in the development of advanced forms of intelligent transportation systems, to step back and evaluate the relevant impacts of surveillance, not only on the function and security of the transportation system, but also on the travelers within that system.

I. Introduction

Many definitions of privacy have been proposed, but most tend to have issues of control of information and its flow as their foundations. Alan Westin has defined privacy as, "the claim of an individual to determine what information about himself or herself should be known to others."[i] This very broad definition contains within itself a wealth of further claims related to different states of privacy, and to the context of the person and his or her information. By approaching the privacy claim from the viewpoint of context, the emerging literature on the social, political, and economic variations inherent in the experience of privacy reveal a range of expectations dependent upon the person's individual understanding. The concept of privacy as based upon a subjective or contextually-based understanding is also consistent with the legal understanding of the subject – for example, the Fourth Amendment, central to legal justifications for privacy protection, has been understood by the courts to be centered on "reasonable expectations of privacy".[ii] Security, on the other hand, often results in a loss of control due, in part, to an exterior determination of context. One of the most commonly used definitions of security is "A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences."[iii] While security may be established at the personal level, such as with home security measures, in the context of transportation it is more often used to refer to the travelers on the network, whether surface or other. Because the context of privacy is often set at the personal level, while the security context is most often determined at a community or societal level, the potential for conflict between the two is great.

This paper will focus primarily on the conflict between privacy and security from the framework of surface transportation, particularly in regard to Intelligent Transportation Systems (ITS). ITS technologies have begun to change the transportation landscape. Whereas traditional transportation initiatives focused primarily on constructing the physical landscape (such as roads, bridges and traffic signals) to enhance mobility and safety, ITS technologies are primarily concerned with managing the flow of information to travelers, transportation providers, and vehicles themselves to enable efficient transportation choices that in turn increase mobility and safety. ITS is a critical component in enhancing the flow of information, but its use comes at a cost. According to Joe Palen of Caltrans New Technology and Research Program,

> An Intelligent Transportation System (ITS), by definition, involves the use of intelligence to enhance the operation of the transportation system. Intelligence, by definition, requires information. Information, by definition, is data formulated in a formation. Data is generated by surveillance. Therefore, surveillance forms the basis

> for the formation of information for an ITS. You can't have a usable ITS without surveillance. (Palen, 1997)

Surveillance within the realm of surface transportation has many components, such as red light cameras used for the purposes of ticketing offenders and encouraging law-abiding behavior; GPS units used as vehicle probes to track the flow of traffic; and Electronic Toll Collection (ETC) systems used both to improve traffic flow through toll collection points and to estimate traffic flows along toll corridors. At first glance, the privacy and security ramifications of such technologies may not appear great, but both the information gathered and the possibility for linking this information with other sources opens up the potential for a wide range of security applications and privacy violations. This paper will first examine these potential uses and applications in the context of security, followed by some of the conflicts that may emerge with privacy preferences. Two examples of technological applications will then be presented to identify how they may have impacts within the urban environment. Finally, needs for further research will be identified.

II. Understanding security

For purposes of this paper, it is first necessary to clarify how security may be defined. Security may be approached from the two primary directions of deterrence and response. Under this approach, deterrence may be evaluated in terms of lessening the chance of a malicious attack, while response may be understood as the ability to use collected data for purposes of law enforcement, such as strengthening a case against a suspect with recorded footage of his or her involvement in an incident. Tinnefield describes the difference between the two by stating, "Preventive [or deterrence-oriented] surveillance is different from its traditional use for investigating a specific criminal offense, which requires proof that a crime has taken place or is likely to occur. Preventive surveillance lacks any such connection to a specific criminal act."[iv] While ITS applications may be used both for deterrence/preventive and response purposes, the timing and approach for each purpose is significantly different. For deterrence, the presence of ITS surveillance technology should be acknowledged for maximum impact at the point of potential conflict. For secondary, post-incident uses, however, covert methods of surveillance may be more useful, as avoidance of the surveillance device is likely if the location is known. Because many agencies intend that surveillance technologies will serve both purposes, it is possible that a combination of both overt and covert ITS surveillance applications may prove most effective.

III. Security in the transportation context

Following the events of September 11th, 2001, the U.S. Congress passed into law the Aviation and Transportation Security Act, which created the Transportation Security Administration (TSA). While much of the focus of the TSA has rested on aviation applications, the overall mission of the department is to, "protect…the Nation's transportation systems to ensure freedom of movement for people and commerce."[v] Under this guiding mission, part of the TSA's focus has been placed on security applications of ITS. According to *The National Intelligent Transportation Systems Program Plan: A Ten-Year Vision*, one of the overarching goals of ITS is, "…a transportation system that is well-protected against attacks and responds effectively to natural and manmade threats and disasters, enabling the continued movement of people and goods even in times of crisis."[vi] According to a 2002 report published by the NYU Wagner Rudin Center for Transportation Policy and Management, the Federal Highway Administration (FHWA) has recommended the following strategies to meet this goal:

1. Develop emergency plans, tools, and resources;
2. Perform vulnerability assessments;
3. Compile case studies on attacks;
4. Conduct freight technology security demonstrations;
5. Solicit ITS technology projects intended to improve security; and
6. Host workshops to discuss these and other related issues.[vii]

The fifth strategy mentioned above is perhaps most related to issues surrounding the conflicts between security and privacy. In accordance with this strategy, a number of technologies have been or are being implemented, including the following:

- Smart Cards
- Biometrics
- Automatic Vehicle Identification
- Map Databases
- Vehicle Classification Sensors
- Weigh-in-Motion Technology
- Spatial Geo-Location[viii]

In the realm of security, each of these technologies is dependent upon the ability to identify and track travelers and freight along the nation's transportation system. The guiding principle is that data collected and linked from the implementation of these technologies may be used, not only for managing the flow of travelers, but also to prevent or deter terrorist attacks. For example, Peyrebrune and Cerreño state that, "…technologies exist that enable security personnel to detect the contents of vehicles, including hazardous substances, explosives, and drugs, without opening the vehicles firsthand. Also available are technologies that match a specific vehicle with a specific operator and specific cargo, preventing travel in the absence of a match."[ix] Such ITS technologies, in addition to others listed above, may have very beneficial ramifications for the nation's security.

Particularly within the urban environment, the melding of the strategies outlined above become of great interest. Because of the diversity of modes available in areas of concentrated population (including mass transit, air transportation, personal vehicles, cycling and walking), along with static cameras used for other purposes, the potential to align and link different methods of ITS surveillance along a route increase. As in the example of the September 11th hijackers, where a network of images from ATMs, gasoline purchases, and airport security were combined to produce an activity path, it is possible to recreate detailed patterns of behavior from the network of surveillance methods becoming ever more pervasive in the urban environment.[x] In such a context, where law-breaking behavior has occurred, the response characteristics of ITS may be viewed as very beneficial by the general public. In question, however, is how the desire for these benefits compares to their potential privacy invasions.

IV. Understanding privacy

With the security benefits inherent in the applications noted above also comes the potential for violations of privacy. Peyrebrune and Cerreño, for example, note that, "…the issue of collecting information about people to prevent terrorist activities versus public privacy will be a public policy issue over the long term."[xi] Simson Garfinkel states the issue more clearly when he notes that, "If ITS systems are developed and deployed which do not respect the privacy of the American driver, there is a good chance that Americans will demand that the system be shut off. Without strong privacy provisions, ITS will not succeed."[xii] Some privacy concerns being voiced by opponents include the following:

- Because pervasive computing systems generally used in ITS may be embedded or invisible, users may not be aware that they are present and collecting data.[xiii]
- The ability to collect and connect data on users in their day-to-day activities may provide a more robust data set on actual travel patterns, origins and destinations – information that has not previously been readily available.
- Defining the secondary uses of collected data will greatly impact the user's level of comfort with pervasive ITS technology. Privacy considerations must guide the degree to which collected information may be shared and used.
- Users of ITS applications may not be aware of their potential privacy implications, making it difficult for them to accurately assess their desire for the potential benefits against potential privacy loss.

Though the issues named above do not cover the universe of concerns that have been raised by privacy advocates, they do indicate the diversity of issues that must be addressed by ITS technologies in the transportation context, and highlight some of the conflicts that are present in terms of security.

Given the difficulties identified above, it is necessary at this juncture to define more clearly the elements involved in expectations of privacy. The Federal Trade Commission (FTC) identifies five "core principles" relevant to privacy policy, namely: "(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/ Redress."[xiv] In short, these principles form the government's definition of privacy as it may be reasonably expected by the consumer. The first principle, notice/awareness, may be considered as the most fundamental in regards to the privacy/security debate, as it sets the context for the remaining four. According to the FTC, "Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[xv] The second principle, choice/consent, rests upon the belief that consumers should have options regarding if information will be collected and how that information will be used. This principle is particularly relevant in relation to secondary usage of data, in which information collected for one purpose may be used for a different and potentially unrelated purpose. The access/participation principle "refers to an individual's ability both to access data about him or herself…and to contest that data's accuracy and completeness."[xvi] Integrity/security is concerned with the responsibility of collectors to ensure the integrity of collected data via such means as cross-referencing against reputable data sets, as well as with ensuring that collected data is protected from loss and unauthorized access via both managerial and technical means. Finally, enforcement/redress is intended to ensure the efficacy of the preceding principles by providing a mechanism for enforcement. From a definitional standpoint, these principles expand the notion of "control" outlined above by introducing the associated concepts of notice, choice, access and security.

V. Privacy in the transportation context

In terms of the privacy/security debate, it is critical to note that in order to protect privacy in the context of personal expectations as required by the FTC, travelers must be aware of the potential that their personal information may be collected, and have some degree of control over what information they wish to share. For purposes of security from a deterrence standpoint, notice and awareness are also critical. For the same reasons that retail establishments often display a sign warning, "These premises are under CCTV surveillance", transportation departments and agencies may erect signs notifying travelers that their moves are being recorded. In this type of situation, the agency believes that by notifying the public that their actions are being monitored, they will be less inclined to participate in law-breaking behavior.

As noted above, however, notice and awareness may also have the effect of simply moving deviant behavior to a different location, as persons may avoid areas with overt surveillance. It is here that covert surveillance enters the picture, but this may be at odds with the principles of notice/ awareness and choice/consent.

If, as outlined in the introduction, the claim for privacy may be traced back in some part to issues of control, it is necessary that persons under ITS surveillance be aware of both the surveillance itself and of its potential ramifications in order that they may exercise control over what information is shared, to whom it is accessible, and for what purposes it is used. One issue of overarching concern with this requirement is that of equity and justice, as understanding the potential ramifications of ITS surveillance may highlight a knowledge gap between persons familiar with ITS technologies and those who are not. Without a concentrated effort to educate all travelers as to the actual benefits and costs evident in ITS surveillance, it is difficult to argue that travelers are able to make an accurate assessment of need. Two additional difficulties that emerge in the context of covert surveillance are, first, if covert surveillance is to be an effective means of security response, it must be allowed to gather any pertinent information outside of the control of the subject; and, second, information gathered under covert surveillance must be subject only to the control of the collectors for the purposes they deem necessary within the legal context. While these needs are at odds with the privacy principles outlined above, they are allowable within the legal framework that defines security measures. As was seen in the public outcry related to the National Security Agency's (NSA) warrantless wiretapping surveillance program, however, covert surveillance that applies to a broad spectrum of the population (such as would be necessary in a public travel environment) may be unpalatable to the general public without a full understanding of the benefits and costs of such a program and if viewed as taking place beyond the scope of applicable laws.

Within the context of ITS the uses of security and mobility management are mixed. Given this, the question arises as to which needs take precedence. If the overarching desire is for mobility improvements, then adoption of associated technologies such as GPS probes and ETC tags will depend in large part upon the acceptance of the traveling public, which in turn will depend upon identifying and addressing their privacy concerns. If, on the other hand, the desire for security is prevalent, it may be necessary to limit the amount of information provided to travelers in order to enhance the amount of information gathered. The following section will attempt to outline the potential ramifications of each approach in the examples of ETC and GPS.

VI. Privacy and security implications of Electronic Toll Collection (ETC)

Electronic Toll Collection (ETC) systems are gaining widespread adoption in the United States. Advocates of the systems tout their benefits in terms of convenience, improvement of traffic flow, decreases in fuel consumption and improvement in air quality.[xvii] According to Briggs and Walton, the systems generally work as follows: "ETC allows participating vehicles equipped with electronic transponders, or tags, to avoid stopping to pay tolls. Instead, the electronic transponder communicates via radio frequency or microwave to a roadside computer. The tagged vehicle is identified as an electronic toll collection system user, and the toll amount is debited from the user's account."[xviii] ETC systems require a fair amount of data from the user. According to the Briggs and Walton report, different ETC providers require a varying amount of information from travelers, including contact information (name, address, telephone number(s)), vehicle information (license plate number and state and make, model and year of the enrolled vehicle), and financial information (generally a credit card or bank account number).[xix] Additional information requested by some providers includes driver's license number, social security number, or mother's maiden name.[xx] While some systems debit transactions directly from the user's bank account, others use a pre-paid account that must be kept loaded with a minimum amount of funds. In the latter configuration, users are either notified directly when their balance falls or is about to fall below the minimum requirement, or have funds directly debited from a linked bank account.

A number of privacy concerns have been raised about ETC systems, particularly insofar as electronic records provide for the linkage of personal, vehicle, travel and financial records. In order to provide a record of transactions in case of charge dispute or other concern, ETC agencies typically keep logs of transactions, including locational information, on each customer. Patrick Riley notes one common concern in his case study of the FasTrak ETC system in the California Bay Area, stating that, "personal information can be used when required by law or ordered so by a court of 'competent jurisdiction.' This apparently includes civil court, as many divorce attorneys seek access to and admit as evidence FasTrak logs."[xxi] The potential for transaction logs and customer files to be accessed either for legal purposes or by malicious agents may create a disincentive for use, despite potential cost and time savings for the user. Riley notes that in a survey of Bay Area residents, the third and fourth most commonly noted reasons (out of 13 possible responses) cited by respondents for not taking part in the FasTrak program are "I have privacy concerns" and "I'm worried about how my private information may be used."[xxii] Such concerns have the potential to impact the deployment and benefits of ETC systems.

ETC systems are installed on designated toll roads only, which limits the applicability of their data collection at lower spatial resolutions. Additionally, transactions are only recorded at designated toll plazas, which may limit the degree of temporal resolution that may be attained from these records. One obvious benefit for purposes of data manipulation, however, is that transaction records are associated with a specifically identified transponder ID, and thus may be automatically linked to and stored with the user's profile. Such a system makes performing analysis on the database relatively easy. Additionally, the limited number of transaction records may make the computing overhead relatively low. Mills and Huber, in their 2002 article “How Technology Will Defeat Terrorism”, relate the security potential for ETC systems when they state, “Even systems as simple as these can be linked up to security networks, too, and can do much to enhance safety, because so much of security comes down to establishing identity and tracking patterns of conduct – just the sorts of things that the automatic toll collectors already do.”[xxiii] Given the evident concern with privacy implications of ETC, however, it is unclear as to whether the security uses of ETC will be efficient in an opt-in system as currently used. Mills and Huber state that, “The first step is to divide the civilian world into two, separating the trustworthy cooperators from the non-cooperators, so we don’t have to search *every* car, package, and pocket.”[xxiv] This approach, however, requires the clustering of all persons with high privacy concerns – thus conflating persons with legitimate privacy concerns and those who are law-breakers. While the potential for security uses of ETC-type systems is evident, balancing these against privacy concerns will require further examination of overt uses, such as in cases where the user must choose to participate, and covert uses, where ETC sensing equipment could be programmed to record identification information from Radio Frequency Identification (RFID) tags implanted in vehicles for tracking and other purposes.

VII. Privacy and security implications of Global Positioning Systems (GPS)

Global Positioning Systems (GPS), unlike ETC systems, tend to have the ability to be more universal in scope. The use of GPS in vehicle navigation and tracking systems has been growing in recent years, particularly as the selective availability feature, which introduced signal errors into non-military applications, has been disabled. Active vehicle-based GPS tracking architectures typically consist of an on-board unit, a base station and a communication link.[xxv] The on-board unit collects and periodically provides a message containing identification and travel environment data over the communications link to the base station, where the data are recorded and stored. Within the realm of tracking, GPS are increasingly being used for vehicle probe applications. According to Hoh and Gruteser, “Probe vehicles carry GPS receivers and communication infrastructure such as cellular links to periodically report records with the following parameters to traffic information systems: latitude, longitude, time, speed. From this information the system can estimate current mean vehicle speed, which can be fed into navigation systems or can be used to build a real-time congestion map.”[xxvi] Such probe applications are likely to grow in scale and deployment, and will be used here to examine potential benefits, drawbacks, and privacy concerns for GPS tracking applications. It should be noted that GPS-based location trackers do not have to be vehicle-based; in fact, one great benefit of GPS systems is that they may be included in devices that may be carried by a pedestrian or cyclist. This analysis, however, will focus on vehicle-based systems.

One of the primary benefits of GPS probe applications is that they are not bound to specific segments of the roadway. Unlike ETC systems, which tend to be concentrated on fairly large or heavily traveled roads (due in part to the overhead costs of implementing the systems, as well as to legal designations of toll roads), GPS probe systems are able to collect data at any given location as long as a connection may be established to the GPS satellite network. This aspect of GPS probe applications is particularly useful to transportation network administrators, as there has long been a paucity of data available on those roads with low functional classifications (particularly local roads) due to infrastructure costs and maintenance. Additionally, unlike ETC systems, which may only collect data at when the user's transponder interacts with the roadside computer, GPS tracking devices have a nearly unlimited ability to transmit information continually once the system has been installed. Additional benefits of a GPS-based probe system identified by FHWA are: relatively low operating cost after initial installation, automated data collection, and the increasing availability of GPS as a consumer product.[xxvii] Potential disadvantages noted are privacy issues, potential signal loss in urban areas, consistency between drivers, and a relatively high installation cost.[xxviii]

User benefits of GPS-based probe systems may be considered in two ways. Improved data and analysis abilities on the part of transportation planners and others may lead to improvements in the transportation network, saving the traveler time, fuel, and other resources. Additionally, real-time knowledge of events may improve the efficiency with which transportation network administrators are able to deploy information and personnel. A second way that these applications may be useful to the user is if they are linked with a vehicle navigation system, which could provide the user with efficient travel routes and updated information related to traffic incidents. For security purposes, GPS are particularly useful, as they may be small, difficult to detect, and transmit data that may be mined to look for patterns indicating the potential for deviant behavior.

Many of the benefits in terms of data collection, retention and analysis seen in ETC systems are also true of GPS probe applications. Assuming that sent messages include a unique vehicle identifier, the automated nature of the data collection system will make it easy for records to be linked to an individual vehicle and its travel path. Such information will be particularly useful for determining real-time traffic patterns, analyzing traffic patterns over time, and tracking individual travelers. Depending on the level of temporal resolution at which data are collected, great benefits are also possible for establishing a library of data and patterns on roadways of lower functional classification, which may allow better tracking of actual origin-destination routes. The level of temporal resolution, however, may have great impacts on the amount of computing overhead required for the use of these systems. If great amounts of data are collected from a great number of vehicles, the computing costs of storage and analysis may overwhelm the agency's system. Additionally, even if traveler data is collected anonymously, thus meeting in practice privacy requirements of the privacy concerned, it may still be able to use GPS to identify individuals. Hoh, et al. conducted a study of vehicle probes in which anonymous GPS traces of 239 vehicles in the Detroit, Michigan region were subjected to a clustering analysis to see if it would be possible to determine the likely home location.[xxix] Based on a sampling frequency rate of one record per driver per minute, the authors found that it was possible to identify a likely home location for approximately 85% of the vehicles.[xxx] Such a finding indicates that for purposes of privacy preservation, it will be necessary to lower the temporal resolution at which data are collected, while security advocates may desire the temporal resolution to remain high. For users to accept the full degree of GPS applications within security and transportation realms, it will be necessary to fully disclose both the potential for misuse and the protective methods by which such misuses may be halted.

Table 1 presents a general overview of the data characteristics and potential security and privacy impacts of the two ITS systems outlined above. As the above review has shown, each system has a variety of benefits and considerations for both users and agencies in terms of overhead and infrastructure costs, the level of data able to be collected, and the potential privacy and security impacts of their use. Additional considerations regarding use of archived data (including secondary use for marketers and law enforcement, among others) should also be considered, though not covered here in detail. The ability of both ETC and GPS systems to create electronic records of travel make them especially useful for security purposes, as this increases the efficiency with which collected data may be utilized for identification of potential security threats. However, this is also the characteristic that is perhaps of greatest concern from a privacy perspective, as it may allow a fairly detailed travel history to be constructed and used for purposes that may be resisted by system users. Generally, decisions regarding the resolution and speed of data collection must represent a balance between the data desired by transportation security advocates and the degree of privacy desired by the traveler. While there is great potential for transportation networks with the advent of ITS technologies such as ETC and GPS, their costs and potential risks, particularly from the point of view of the potential user should be taken into consideration when planning for system implementation.

System Type	Data Characteristics					Potential Security Applications	Potential Privacy Concerns
	Spatial Resolution	Temporal Resolution	Speed				
			Collection	Cataloging	Analysis		
Electronic Toll Collection Systems	Relatively limited; based on location of static collection points.	Relatively low due to limited number of collection points.	High	High to medium depending on number of records collected and computing capabilities.	High to medium depending on number of records collected and computing capabilities.	Analysis of travel patterns linked to individual financial records, allowing for potential identification of security threats; Potential to expand uses of ETC infrastructure to collect additional data on vehicles and travelers.	Linking of identifiable individual information, travel patterns, and financial records may subject records to malicious uses; Records may be subpoenad for use in legal proceedings.
Global Positioning Systems	High within the space covered by collection infrastructure.	Potential for a very high temporal resolution within the network; may need to be lowered due to privacy and computing overheads.	High	High to low depending on computing capabilities and number of records collected.	High to low depending on level of resolution.	Potential to collect and analyze data on individual travel patterns at high resolution with little knowledge by the person being surveilled.	High degree of information gathered may open concerns for malicious uses; Travelers may be unaware of amount of data being collected and secondary uses.

Table 1: Overview of ITS Data Collection Characteristics

VIII. Conclusion

The overview above has only begun to touch upon the issues prevalent in the security/privacy debate in relation to ITS. Because of the concentration of travelers and security threats in urban areas, the discussion is particularly relevant to urban dwellers and travelers. Armstrong and Ruggles, for example, note that, “Cameras are not (yet) everywhere, but camera proliferation has been accepted by many urban residents as a fact of everyday life.”[xxxi] While the presence of these static cameras may be accepted by some, further uses such as those outlined above may create more of an incentive to resist the installation and adoption of cameras that may be used to identify and track along a route in urban areas. Additional studies have also indicated that the socio-demographic characteristics of those who are willing to adopt such ITS technologies and those who resist them may differ, thus bringing additional questions of equity and fairness to light. As the transportation realm struggles to balance the need to ensure the security and protect the privacy of travelers along its network, it will be necessary to further address these issues, and examine in more detail the relevant benefits and concerns.

[i] Westin, A. “Social and Political Dimensions of Privacy.” *Journal of Social Issues,* Vol. 59, No. 2, 2003. Pp. 431-453.

[ii] Slobogin, C. “Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity.” Mississippi Law Journal, 72: 213-299, 2002.

[iii] http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html.

[iv] Tinnefeld, M.T. “The Security Principle – A Challenge to the Right of Privacy and of Freedom of Information. Presented at the First Annual European Freedom Summit. Berlin, July 2, 2007.

[v] TSA Mission statement. http://www.tsa.gov/who_we_are/mission.shtm.

[vi] ITSA. “Delivering the Future of Transportation – The National Intelligent Transportation Systems Program Plan: A Ten-Year Visions.” Executive summary. January 2002.

[vii] Peyrebrune, P.E. and A.L.C. de Cerreño. “Security Applications of Intelligent Transportation Systems: Reflections on September 11 and Implications for New York State.” July 2002.

[viii] Ibid.

[ix] Ibid.

[x] Armstrong, M.P. and A.J. Ruggles. “Geographic Information Technologies and Personal Privacy.” Cartographica, Vol. 40, Iss. 4. Winter 2005. Pp. 63-73.

[xi] Peyrebrune and Cerreño.

[xii] Garfinkel, S. “Why driver privacy must be a part of ITS.” Converging Infrastructures: Intelligent Transportation and the National Information Infrastructure. MIT Press. 1996.

[xiii] Bhaskar, P. and S.I. Ahamed. “Privacy in Pervasive Computing and Open Issues.” Second International Conference on Availability, Reliability and Security. 2007.

[xiv] Federal Trade Commission. “Fair Information Practice Principles.” 25 June 2007. http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[xv] Ibid.

[xvi] Ibid.

[xvii] Holdener, D.J. “Electronic Toll Collection Information: Is Personal Privacy Protected?” Compendium: Graduate Student Papers on Advanced Surface Transportation Systems, Southwest Region, University Transportation Center Research Report # SWUTC/96/72840-00003-1, Texas Transportation Institute, Texas A&M University System. August 1996. Pp. D-3 – D-4.

[xviii] Briggs, V. and M. Walton. The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data. Southwest Regional University Transportation Center. May 2000.

[xix] Ibid.

[xx] Ibid.

[xxi] Riley, P.F. “The Tolls of Privacy: An Underestimated Roadblock for Electronic Toll Collection Usage.” Computer Law and Security Report, 24. 2008. Pp. 521-528.

[xxii] Ibid.

[xxiii] Mills, M.P. and P.W. Huber. “How Technology Will Defeat Terrorism: At home and abroad, digital wizardry will keep us safe.” City Journal, Winter 2002.

[xxiv] Ibid.

[xxv] Padmanabhan, J. “GPS Based Vehicle Tracking System.” http://www.gisdevelopment.net/technology/gps/techgp0044.htm.

[xxvi] Hoh, B. and M. Gruteser. “Enhancing Security and Privacy in GPS-Based Traffic Monitoring Systems.” WINLAB Project Summary. Fall 2006.

[xxvii] Turner, S.M., W.L. Eisele, R.J. Benz and D.J. Holdener. Travel Time Data Collection Handbook. Report No. FHWA-PL-98-035. March 1998.

[xxviii] Ibid.

[xxix] Hoh, B., M. Gruteser, H. Xiong, and A. Alrabady. “Enhancing Security and Privacy in Traffic-Monitoring Systems.” Pervasive Computing. IEEE, October – December 2006. Pp. 38-46.

[xxx] Ibid.

[xxxi] Armstrong, M.P. and A.J. Ruggles. “Geographic Information Technologies and Personal Privacy.” Cartographica, Vol. 40, Iss. 4. Winter 2005. Pp. 63-73.