Title
A private matter: the implications of privacy regulations for intelligent transportation systems

Journal
Transportation Planning and Technology, 39(2)

ISSN
0308-1060

Authors
Lederman, Jaimee
Taylor, Brian D
Garrett, Mark

Publication Date
2016-02-17

DOI
10.1080/03081060.2015.1127537

Peer reviewed

Transportation Planning and Technology

Routledge
Taylor & Francis Group

ISSN: 0308-1060 (Print) 1029-0354 (Online) Journal homepage: http://www.tandfonline.com/loi/gtpt20

A private matter: the implications of privacy regulations for intelligent transportation systems

Jaimee Lederman, Brian D. Taylor & Mark Garrett

To cite this article: Jaimee Lederman, Brian D. Taylor & Mark Garrett (2016): A private matter: the implications of privacy regulations for intelligent transportation systems, Transportation Planning and Technology, DOI: 10.1080/03081060.2015.1127537

To link to this article: http://dx.doi.org/10.1080/03081060.2015.1127537

TRANSPORTATION PLANNING AND TECHNOLOGY, 2016
http://dx.doi.org/10.1080/03081060.2015.1127537

Routledge
Taylor & Francis Group

A private matter: the implications of privacy regulations for intelligent transportation systems

Jaimee Lederman, Brian D. Taylor and Mark Garrett

UCLA Institute of Transportation Studies, 3250 Public Affairs Building, Los Angeles, CA, USA

ABSTRACT

The rapid development and deployment of Intelligent Transportation Systems (ITS) that utilize data on the movement of vehicles can greatly benefit transportation network operations and safety, but may test the limits of personal privacy. In this paper we survey the current state of legal and industry-led privacy protections related to ITS and find that the lack of existing standards, rules, and laws governing the collection, storage, and use of such information could both raise troubling privacy questions and potentially hinder implementation of useful ITS technologies. We then offer practical recommendations for addressing ITS-related privacy concerns though both *privacy-by-design* solutions (that build privacy protections into data collection systems), and *privacy-by-policy* solutions (that provide guidelines for data collection and treatment) including limiting the scope of data collection and use, assuring confidentially of data storage, and other ways to build trust and foster consumer consent.

ARTICLE HISTORY
Received 26 June 2014
Accepted 30 July 2015

KEYWORDS
Privacy; Intelligent Transportation Systems; connected vehicles; privacy-by-design; privacy-by-policy

1. Introduction

The rapid development and deployment of Intelligent Transportation Systems (ITS) promises great opportunities to address economic, environmental, and social problems but also raises significant issues with respect to personal privacy. Its potential power, the 'intelligent' part of ITS, depends on gathering, analyzing, and acting on large amounts of data. Some ITS technologies pose a threat to privacy when collecting individualized data to, for instance, forecast travel behavior. The potential danger is that private information relating to specific individuals and their actions may be made widely available, or that others beside those collecting it may gain access to the data, or that personal information acquired for one reason acceptable to the user may be used for another entirely unrelated and unapproved purpose. To date, however, little attention has been paid to the tradeoffs between the transportation benefits from collecting such personal information and the dangers from its possible disclosure and/or subsequent misuse.

Many new ITS devices and technologies are being placed into service but those behind these efforts have little in the way of legal guidance on this issue or the potential consequences of failing to protect privacy in ITS. Despite the obvious collective value of the

CONTACT Brian D. Taylor btaylor@ucla.edu

information being generated from ITS for optimizing transportation systems, the lack of accepted or universal privacy standards may ultimately make consumers more reluctant to accept those benefits and could even inhibit further development and deployment of the technology.

Clearly, the explosion of information gathering associated with mobile devices is increasing concern about the capacity of both government and private industry to gather and share personal information for a variety of purposes. ITS technology amplifies this debate because it adds a tracking component to other information about the user and places visited, making it possible to learn far more than even before about individual activity, often times without a choice on the part of the consumer. Even if consumers are initially willing to accept data collection about them in other areas, they may not be fully aware of how intrusive ITS data collection can be, particularly given the potential to combine such location data with other personal information from multiple sources.

How much privacy does the consumer demand? What can be done to protect information from disclosure or misuse and what should be done in the case where that trust is violated? What level of privacy protection is needed for consumers to accept and even contribute to the collection of these data? What rights should they have regarding what information is collected, who has access to it, how long it is stored and what use is made of it?

In the absence of universal regulations, there is uncertainty over appropriate standards to follow, and privately developed codes of conduct that may be developed and voluntarily adopted by transportation industry groups may or may not meaningfully serve the public interest in the long run. Too strict standards may forestall useful ITS technologies, while overly lax standards may damage public confidence in collection of data about them. Further, widely publicized harms to individuals whose privacy rights may have been unambiguously violated might conceivably generate a public backlash leading to even stricter regulation of ITS technologies.

In this paper, we survey the current state of privacy protection related to ITS technology and address various strategies that have been put forth for addressing issues that may inhibit its further evolution or violate consumer standards of privacy. We begin by describing some of the emerging ITS technologies and the types of personal information they are capable of generating. We next survey the admittedly thin body of federal and state laws and private industry standards for data gathering as background to examining the current state of practice in data collection privacy protection. Drawing on this analysis, we propose a framework for understanding privacy concerns and use it to consider the benefits and drawbacks of various schemas for protecting ITS-gathered personal information. Finally, we offer recommendations for factors to be considered should ITS privacy legislation or policies be pursued. Specifically, we discuss procedures for limiting the scope of data collection, who may have access to data and the purposes for which it can be used, options for protecting the confidentially of data gathering, and how to foster consumer consent to the collection and use of personal data.

1.1. ITS and data collection

ITS refer to a diverse family of technological applications to increase the efficiency and effectiveness of both personal and commercial travel. Freeway performance monitoring,

real-time traffic signal optimization, automated toll roads, delay-sensitive navigation systems, and real-time public transit arrival and departure information are just a few of the many dozens of ITS technologies. After many years of gradual implementation, the explosion in ownership and use of personal, commercial, and vehicular mobile data technologies has rapidly accelerated ITS implementation.

However, the increasingly prodigious production and consumption of data on the movement of vehicles (and, by extension, the people and goods in them) has outpaced the evolution of standards, practices, rules, and laws governing the ownership and use of many forms of transportation data raising important privacy questions regarding the collection, availability, and use of such information. With the widespread deployment of mobile location-tracking technologies present in cell phones, and the recent revelations concerning clandestine data collection by the National Security Administration (NSA),[1] the US is at a cultural, political, and legal juncture where it will be increasingly difficult to longer ignore the issue.[2] To date, however, there is very little in the way of legal guidance on how ever-greater volumes of information about the movement of people, goods, and vehicles is being collected, how it is being stored, who has access to it, how it can be used, and a host of other questions that implicate personal privacy.[3]

Many modern technologies collect personal information, but ITS is unique in its potential to collect locational and movement data without consumer consent and choice; specifically the position and movement of vehicles and mobile devices, and by implication their owners. When this information can be combined with other personal information about a vehicle's occupants now available in an ever expanding reservoir of data bases, a great deal can potentially be learned about the travel behavior of individuals but in a manner that may be viewed as an invasion of privacy for those who do not care to have their every movement tracked.

It appears likely that some form of privacy regulation is on the way, but how soon and what form it takes is still to be determined. A 2015 report by Senator Markey on data collection and protection practices of automobile manufactures found that while large amounts of personal and locational data are collected by automakers, security measures are inconsistent and unreliable, and data retention practices varied greatly. The report concluded that privacy protection was insufficient and confusing for consumers, who had little choice about whether their data are collected (Markey 2015). Following this evaluation, legislation was introduced directing the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to establish automobile privacy standards that stress transparency and flexibility for consumers to opt-out of data collection (Security and Privacy in Your Car Act of 2015, S. 1806, 114th Congress). While a promising step toward ITS privacy protections, the bill is not yet law and the outcome of any resulting regulations remains an open question. Too little privacy protection and the public may not be willing to embrace useful new ITS technologies, but too much protection may limit the usefulness of any data collected.

1.2. ITS technologies

ITS technology can be categorized in many ways, including by whether it is collected for public or private aims. Among the current government-operated ITS technologies are:

- *Red-light cameras*: These devices collect information on where a vehicle is located and who owns the vehicle by matching license plate numbers to vehicle registration data. They also typically provide a photograph of the driver of the vehicle, who may or may not be the registered owner. While the same was true of traffic stops by police officers, these systems are being deployed more ubiquitously and thus the opportunities for this information to be collected and retained on a large scale (even if there is no ticket issued) are far greater than in the past. Future systems may even be able to identify vehicles through electronic devices embedded in the vehicle.
- *Speed-detectors*: Similar to red-light cameras, these devices can not only identify the location of a vehicle but also its movement and speed. Obviously the data collection is necessary for law enforcement purposes to identify and punish scofflaws but there are fears over how long the information is retained, who may have access to it, and to what other uses it could potentially be put.
- *Traffic monitors*: Many transportation agencies rely on systems of cameras and/or embedded road sensors to monitor traffic conditions. Much of these data are anonymous, identifying only overall numbers of vehicles, average speeds, accident locations, bottlenecks, etc. but the capacity to identify particular vehicles is waxing, raising concerns similar to those mentioned above in that sensitive cameras and other devices may be able to identify actual vehicles or individuals riding in them.
- *Automatic tolling devices*: These use transponders in vehicles to record vehicles passing a tolling station in order to deduct the appropriate charge from the user's account or send out a bill. Such devices are very useful in eliminating long lines at the toll collection booth, and enable the deployment of road pricing systems. But they also guarantee that information concerning the vehicle and its location at various times is collected at numerous locations. The tolling authority also collects data on travelers when they apply for the service linked to a payment account.
- *Parking meters*: The increasing use of debit cards, credit cards, and other forms of electronic payment media to 'feed the meter' generates location and duration information for the cardholder's vehicle. This information may be tied directly to the holder's identity, address, and possibly his or her financial institution and account information. While this may be necessary for billing purposes, there are again concerns over how long the government (as opposed to the bank) may keep the information and who else might have access to it.
- *Parking information services*: Some cities have begun experimenting with sensors embedded in on street parking spaces connected to global positioning system (GPS) enabled devices that provide drivers with information on the location of available parking spaces in order to minimize the problem of drivers 'cruising' for an open space. Information may be collected from those accessing the system and some systems may also accept reservations and/or payment information that add to the amount of data collected. Similar to red-light cameras, if these parking systems are also used identify violators this can increase the likelihood that individual location data will be gathered.
- *Transit passes*: As transit agencies shift away from currency and paper passes to smart cards and other new forms of payment media, more information about the people using transit is now available. While some cards can be purchased anonymously and contain only a balance of funds available, others are tied directly to a particular

purchaser through a linked credit card or other information provided when they are obtained. When the card is swiped, data on the location of the user (who might not necessarily be the purchaser) and time of use is generated. Some of this information is needed for billing, and aggregated location data can be valuable to analyze flows for transit planning purposes, but individual location and travel data are generated in the process.

In the future, highways equipped for partially or fully autonomous vehicles may not only detect a vehicle at a particular location but track that vehicle throughout its journey while it is connected to the system either via roadway sensors or through a GPS network. Transit arrival and departure information can now be provided to electronic billboards located at transit stops, or via computers, tablets, or phones. While users may access this information anonymously, it may be also possible to collect data on the device being used to do so, particularly if one has to subscribe to a service or when one enters query information concerning certain locations or routes. The same can be said of services providing information on traffic conditions, alternative routing, and other information particularly if it is connected to some type of in-vehicle GPS system that can identify the location of the requesting vehicle.

Private industry is also collecting information related to ITS. In vehicle GPS devices can be helpful in locating and directing users to restaurants, shops, theaters and a host of other consumer destinations. They also collect information on the location of the vehicle or mobile device, its owner, and the places that he or she is interested in visiting, possibly even tracking the vehicle/mobile device movement to and from those destinations. For years now the trucking industry has used GPS to track the movement of its vehicles, their shipments, and the driving behavior of its operators; when they start and stop, how fast they travel, the routes they take, whether they adhere to other company policies. As more and more vehicles are coming factory-equipped with computerized services it may be harder for private automobile drivers to avoid generating similar information that can then be collected by the manufacturer or other third parties.

Today, most cars come equipped with sensors that are or can be linked to computers that record information on the performance of the vehicle and its operation, including speed, braking, and driving patterns. Some of this may be very valuable to consumers in locating the source of mechanical problems, or notifying rescuers in the event of a crash, or reducing automobile insurance costs. For example, many insurance companies have implemented programs offering drivers discounts for limiting night-time driving, speeding, or sudden stops – factors they have determined to be associated with higher claims rates.[4] Some insurers are marketing these services to parents, enabling them to track their teen's driving behavior. Potential discounts notwithstanding, many drivers chafe at the idea of their insurance carriers (or government agencies) monitoring their, or their family members', driving. Many people may not even be aware of the extent of the information now being collected by newer vehicles. Some have even proposed that vehicle computers be connected directly to the web and even serve as roving mobile 'hot spots' to extend the reach of the internet. If that comes to pass even more information may potentially be available to those with the wherewithal to access it.

2. US privacy law

There are currently no comprehensive laws in the US addressing privacy protections vis-à-vis ITS technologies.[5] Instead we have a piecemeal system of legal guidance for the public and ITS stakeholders; a complicated patchwork of some binding law from different jurisdictions, and a series of non-binding 'best practices' guidelines gathered from disparate sources.

2.1. Federal privacy laws

To date, the most substantial piece of federal privacy legislation is the Privacy Act of 1974, which only applies to information maintained by the Federal Government, though it has been mimicked by many states to varying degrees (Douma and Deckenbach 2009). There has recently been a flurry of proposed consumer privacy legislation, but lacking is a truly comprehensive legislative scheme for privacy protection (see FTC [2012] for a list of such proposed legislation).

The current federal ITS research program, the IntelliDrive Program,[6] has published its own set of Fair Information Practice Principles (FIPPs),[7] but has yet to craft ITS-specific privacy and legal guidelines.[8] Aside from these there are a series of 'model laws' and administrative guidance put forth mainly by the FTC, but also by the Department of Commerce, that are intended to serve as guidelines in lieu of legislation, though these model laws may also inform Federal legislation, should it eventually be enacted. In addition, they provide a model for state privacy laws (Fries et al. 2012).

2.2. State laws

Inconsistent regulations among states and localities, which are left to develop their own ITS policies in the absence of federal leadership, exacerbate the situation. Many states have enacted their own, and highly varied, privacy laws (Briggs and Walton 2000; Cottrill 2009). One example concerns Electronic Data Recorders (EDRs) in newly manufactured vehicles. There are no federal laws or regulations governing this technology, favoring the industry self-regulation approach (McDonald and Cranor 2006). In 2004, California passed what at that time was the only ITS-specific privacy law in the US, requiring manufacturers to give notice about the presence of EDRs, and granting buyers complete control over how black-box data, automatically collected about the driving behavior of the car, is used (Glancy 2009). Following California's lead, other states adopted similar EDR laws, although they differ in the levels of disclosure restrictions and privacy protection afforded the consumer (Phillips and Kohm 2011).

Differing state legal regimes pose a challenge to the legal certainty of ITS deployment as manufacturers and service providers may be forced to comply with multiple, and sometime contradictory, standards (Douma and Deckenbach 2009). California, for example, is alone in requiring businesses to provide requesting consumers with a list of personal information disclosed to third parties and the identities of those third parties (Cal. Civ. Code § 1798.83, 2006), which forces companies to either build this capacity into their systems for everyone, or separate the data of California customers.

In addition to privacy laws, state tort protections and systems also vary, further undermining the effectiveness of state privacy enforcement (Glancy 2009). For example, if a

person chooses to use a given routing technology based on real-time location identification in a state like California that protects secondary sale of such data, what happens when she drives across state lines where privacy laws differ? Who, if anyone, is responsible for notifying the driver that her information can now be resold? Who may be liable if that information is misused? This is further complicated by the state-by-state system of tort law and complex choice-of-law[9] rules governing which laws are applied.

2.3. Self-regulation in the private sector

The speed of technological development has made crafting a national ITS policy difficult and this has opened the door for private industry developments on these issues.[10] The Intelligent Transportation Society of America (ITSA) is a private industry group that seeks to coordinate research, technology, and deployment efforts of ITS nationally and among its members, which include public agencies, private corporations, and academic institutions. ITS America acts as a political advocacy group that broadly represents the disparate interests in the ITS world (ITSA 2015), and is a leading player in the development and deployment of ITS technologies. ITSA has produced model laws and guidelines that, *in lieu* of formal federal (or state) legislation, have become de facto industry standards and have already influenced legislation in some states. Though non-binding, states may minimize risk by following the guidelines if future national laws are developed in collaboration with ITSA.[11]

The impact of ITSA model laws and regulations on actual privacy practices is unclear. Since they are voluntary guidelines, Cottrill (2009) argues that manufacturers and governments have little incentive to invest money to protect privacy to a standard that is neither universal nor required, which may hinder the development of procedures for protecting consumers. On the other hand, legal uncertainty regarding privacy requirements may make some hesitant to deploy ITS technologies due to liability concerns (Pethtel et al. 2011).[12] But if manufacturers increasingly conform to ITSA guidelines, they may ultimately prove too ingrained for future legislation to ignore. Promulgating industry regulations is a tried and true tactic across industries to either head off government regulations over which industry actors may have little influence, or at a minimum influence the regulations ultimately enacted. Still, since government is ultimately responsible for the safety of sidewalks, streets, highways, and public transit systems it builds, operates, and maintains, some observers worry that the public sector will ultimately allow private industry to largely dictate ITS privacy regulations (Bagby and Gittings 1999).

3. Data management and privacy law

3.1. General data practices

The spatial nature of travel may also necessitate both technical and policy agreements for data sharing among devices and networks across multiple jurisdictions in order to fully realize efficiencies and other gains promised by ITS technologies (Maccubbin et al. 2008). Multi-jurisdictional and metropolitan planning organizations have been able to broker information sharing policies to regulate and standardize access and protection issues (Maccubbin et al. 2008), but while sharing more complete ITS data sets in real-

time is especially useful for ITS operations, it raises additional privacy concerns. Unfortunately for ITS decision-makers in both the public and private sectors, the exact relationship between usefulness and privacy protection remains murky, and likely to entail considerable experimentation in the months and years ahead (Cottrill 2009).

3.2. Evaluating privacy concerns

People's desires for privacy and privacy protections are evolving along with the technology. For instance, location-tracking applications via mobile telephones are increasingly commonplace, and the proportion of people who say they are concerned about their privacy has also increased (Ban and Gruteser 2010). A November 2010 study found that 55% of those already using location based services are concerned about their loss of privacy (Ozer et al. 2010). Eighty-seven percent of survey respondents wanted control over what personal information is shared and how it is being used (Sapienza 2012).[13]

Privacy concerns vary from person to person and are largely dependent on (1) the personal nature of the data collected, (2) user perceptions of the technology used to collect data, (3) trust in whoever is collecting the information, (4) the specific party collecting the information, (5) the stated reasons for collecting data, and (6) who else may have access to the data (Fries et al. 2012). Given this, we draw on the literature to identify below factors that help explain the likely level of consumer privacy concerns with ITS-particular technologies.

3.2.1. Personally Identifiable Information

Personally Identifiable Information (PII) refers to information that can be used to identify a particular individual, either directly by name or indirectly, for example, by location of a home or a credit card number attached to an electronic tolling device. When data are 'anonymous', they typically contain no PII. Unfortunately, any discussion of data privacy in the context of PII is problematic on several counts.

First, there is no agreed upon definition of PII, and therefore no easy corresponding 'bright line' rule for legal guidance. Scholars furthermore worry that even information that is not PII may be aggregated by third parties in ways that enable individual identification (Wang and Loui 2009). Cottrill and Thakuriah (2011) estimate that 87% of the population can be identified by searching only zip code, sex, and date of birth. The US Office of Management and Budget acknowledges these difficulties in its description of PII as:

> … information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual. (Orszag 2010, 8)

Even if PII can be clearly identified, it is more readily a starting point for developing privacy guidelines than a clear indicator that its collection represents a privacy violation.

From the ITS perspective, privacy concerns are foremost when the technology gathers data on the movement of specific people or vehicles, rather than flows on the system as a

whole (Douma and Aue 2011). Furthermore, the Center for Democracy & Technology, commenting to the FTC for its 2012 Privacy Report, expressed concerns that even tracking locations and activities without PII could lead to questionable behavior, such as discriminatory pricing.

3.2.2. User perceptions and preferences

There is growing body of research suggesting that an individual's desire for privacy protection in the context of a particular technology is largely determined by his or her perception of the technology, rather than a consistently principled consideration of privacy concerns. Fluid user perceptions thus add an additional layer of complexity for agencies implementing ITS technologies. Indeed, strong privacy protections may prove necessary to permit widespread adoption of some ITS technologies in order to ensure a functional and cost-effective network, even at the expense of some utility.

One of the primary concerns that people have expressed is that ITS will create a 'big brother' who will track all their movements. For example, the Arizona DOT found that simply changing references to their traffic camera policy from 'video surveillance' to 'video monitoring' helped to allay some of the public's fears surrounding the technology (DeBlasio et al. 1999). In a 2000 survey of municipal governments' experiences with ITS deployment, Briggs and Walton (2000) found that public perceptions were highly correlated with both public acceptance of ITS, and could be influenced by media attention. Government implementers of ITS have generally found that people will not accept new technologies without fully understanding both the benefits and the privacy implications. Thus ITS-implementing agencies have little choice but to engage in informative marketing and communication with users in order to successfully deploy new ITS technologies (Briggs and Walton 2000; DeBlasio et al. 1999).

3.2.3. Trustworthiness

Closely linked to ITS privacy perceptions is trust in the organization collecting the data (Cottrill and Thakuriah 2011; Xu, Teo, and Tan 2005). Several private sector privacy policing systems are now available in response to both pressure from ITS industries and economic incentives (Cottrill 2011). There is a budding industry of 'privacy professionals' who help organizations navigate regulations and best practices, and some large companies have created their own privacy officers. Third-party assurance organizations such as BBBOnline and TRUSTe provide privacy-auditing services for Internet businesses that collect data on their users (Xu, Teo, and Tan 2005). These organizations grant companies use of their seals of approval to gain consumer confidence (Bamberger and Mulligan 2011; Cottrill 2011).

The perceived strength of privacy protection is also related to the likelihood of enforcement for violations. A company may tell consumers that strict privacy protections are in place through their privacy policies, but without a mechanism to independently audit and enforce violations, such assurances may do little to increase trust among consumers (Xu, Teo, and Tan 2005). Therefore privacy policies backed by independent protection, including third-party or legal protections, are trusted more than those governed merely by industry standards and company assurances, which rely solely on the trust of the party collecting the data (Xu, Teo, and Tan 2005).

3.2.4. Who is collecting the information?

An important concern for consumers is whether the government or a private organization is collecting the information. Stricter privacy protections are generally desired for the public sector, owing to greater demand for accountability. For example, the Federal Government is subject to the Privacy Act of 1974, which limits interagency data sharing and is subject to Freedom of Information Act (FOIA) requests, while private corporations are not. But legal constraints on public sector data access are not universal; law enforcement does not always need a warrant or subpoena to access information, such as locational data acquired through electronic tolling, but some legal process is requires for a private company wishing to access such data (Douma and Aue 2011). This fact can cause apprehension among users because the government already possesses so much personal information from other sources, so many users fear giving it locational data as well. Contrast this with the private sector, where data consolidators – such as credit reporting agencies – have access to increasing arrays of data, mirroring the capacity of government to collate information but with fewer protections on use, the gradual recognition of which may begin to alter the public's more generous privacy perceptions regarding the private sector.

3.2.5. Aims of the technology

Research has shown that people have greatly differing privacy preferences depending on the aim of the technology. The clearest legal distinction involves restrictions against the use of information gained through ITS or other technology by law enforcement, since criminal prosecutions are subject to the strict evidentiary standards of the Due Process clause of the Constitution. But the existence of such copious data is also an undeniably attractive tool for law enforcement. Smart phones have surged in popularity with consumers in the recent years, and have thus grown as a law enforcement tool as well. In the past 5 years, there were over 1.3 million demands by law enforcement agencies to wireless carriers for information such as location data, calling records, and text messages, which rarely requires a warrant under increasingly outdated electronic surveillance legislation and rules ('The End of Privacy?' 2012). The combination of the inherent severity of criminal sanctions and the appeal of the technology to law enforcement results in one of the most significantly unresolved pressing issues.

At the other end of the spectrum is commercial data use, typically by a private company, such as for GPS navigation. Commercial products more often provide a personal benefit to the user, for which many people are willing to pay and/or trade on their privacy. Other uses, such as research, safety, and environmental purposes, fall along this spectrum, as they are widely perceived as promoting the public welfare, though with less real-time benefit for the user. Nevertheless consumers may be more willing to have their personal data collected and stored for these purposes, however privacy concerns may begin to grow when these data are made available to others, or used for purposes beyond which they were originally collected.

3.2.6. Secondary use

One of the most important data management policy issues concerns information sharing, which ranges from interagency data sharing policies to more general 'secondary use' concerns, and center on the reuse of data after they are collected and used for their initial purpose. While private corporations have economic interests in protecting customers'

privacy, they face competing economic incentives to share their proprietary data which are often highly valued by third parties (like marketers) – creating a dilemma for ITS firms in possession of valuable and private user data (Douma and Deckenbach 2009). Transportation agencies must similarly carefully monitor who has access to data in order to balance privacy and information sharing demands (Maccubbin et al. 2008). Secondary usage also increases the chances that data may be aggregated, heightening concern over personal identification (Cottrill 2009).

Concern over secondary usage of data is prevalent in privacy scholarship (Briggs and Walton 2000; Douma and Aue 2011), as users are typically reluctant to relinquish personal information if they are ultimately not in control of who has access to it and what it is used for (Cottrill 2009). For example, the GPS manufacturer TomTom engendered considerable consumer and political antipathy when it sold driver data, without users' permission, to authorities in the Netherlands, who then set up speed traps where the data revealed high incidences of speeding (Arthur 2011).

Secondary usage as it is applied to government surveillance is a particular concern in ITS. Traffic cameras, GPS devices, and electronic toll records held by the government can be combined to gain a picture not only of an individual's movement, but of activity and social patterns as well. That government might cross-reference data to determine where and with whom an individual is interacting is particularly disconcerting for those who fear the 'big-brother' aspect of government data collection (McDonald and Cranor 2006). Due to these concerns, many scholars (Briggs and Walton 2000; Cottrill 2009; Douma and Aue 2011) have proposed substantial restrictions on secondary use of data, particularly by the public sector, although of course such restrictions must be balanced against both the initial and ultimate utility of the collected data.

3.3. A proposed framework for understanding privacy concerns

Given the disparate landscape of privacy protections and data usage, it simply is not possible for a single privacy protection policy – no matter how carefully conceived – to effectively address all ITS technologies. As such, we propose that the place to start is by developing a hybrid privacy regime for ITS that draws from privacy protections adopted and proposed for other, non-ITS technologies. Our review of such technology-focused privacy protections suggest that ITS-specific privacy protections should address privacy across four dimensions: (1) who is collecting the information, (2) the potential criminal implications resulting from the data collected, (3) whether PII is being collected, and (4) whether there is a possibility of secondary usage of collected data. Figures 1 and 2 illustrate varying levels of privacy concern for these four dimensions along a continuum from less need for protection to greater need for two ITS applications, traffic cameras and travel behavior research. That government directly collects data from traffic cameras and uses it for law enforcement and possibly other purposes suggests the need for greater attention to privacy protection in terms of collection and dissemination compared to merely using data for travel research purposes, though such activity may raise separate concerns due to its potential for collecting more PII.

While each of the four ITS privacy dimensions outlined in Figures 1 and 2 are conceptually distinct, there are of course interrelations among them, which highlights the importance of addressing all four dimensions in any comprehensive ITS privacy program.

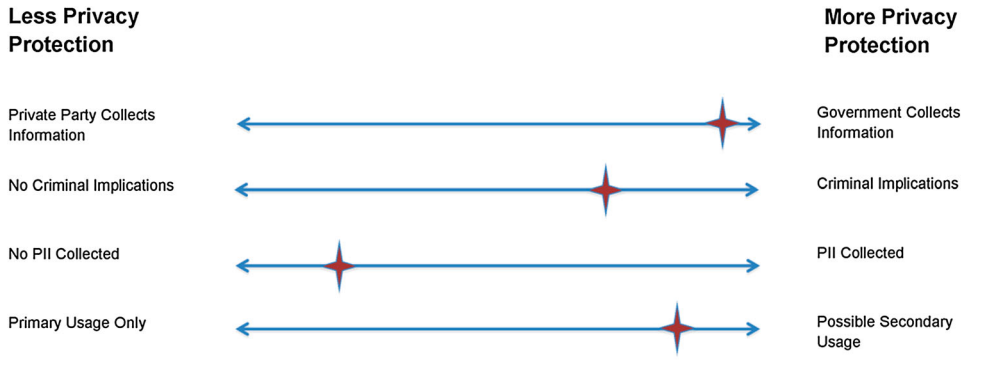

Figure 1. Considering the four ITS privacy dimensions with respect to traffic cameras.

Accordingly, the next section reviews ways to improve privacy protection with respect to ITS technologies, and the following section evaluates frequently suggested ways to improve ITS privacy protections in light of the findings from our review of the literature.

4. Types of privacy protections

Until recently, privacy concerns have been given little weight in the design of ITS technologies (Ban and Gruteser 2010). The tide is shifting, however, as the federal government now requires all federal agencies and programs to conduct a Privacy Impact Assessment, or PIA, to analyze how PII is collected, used, shared, and maintained (FTC 2015). For example, managers of the former federal IntelliDrive initiative acknowledged that privacy considerations needed to be addressed in ITS development (Cottrill 2009). Currently, there are two main mechanisms for technology-related privacy protections: that of *privacy-by-design* and *privacy-by-policy*. We consider each in turn below.

4.1. Privacy-by-design

Protections that are embedded into the technological system are referred to as privacy-by-design. This framework stresses the anonymity of data either by never collecting PII or by

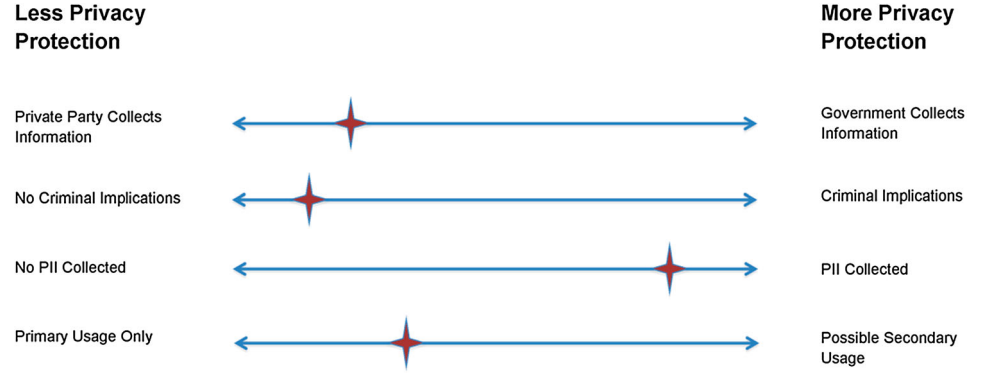

Figure 2. Considering the four ITS privacy dimensions with respect to travel behavior research.

stripping it of unique identifiers before storage. Ohm (2010) postulates that legislation often focuses on protecting anonymity because it is an easy solution, avoiding complex consideration of countervailing benefits from increased innovation, like for instance, instant reviews of nearby restaurants when in an unfamiliar area. While far from perfect, data anonymization remains the primary privacy-protecting approach in ITS technologies.

Privacy-by-design stresses 'data minimization', the concept that technologies should be designed to collect as little PII as possible in order to achieve its desired function (Ban and Gruteser 2010; Kung, Freytag, and Kargl 2011; Steinfeld 2010),[14] though such system design-focused approaches can prove a challenge when multiple systems and multiple data users are involved.[15] The second-best approach is often to adopt the most secure way to manage needed PII (Kung, Freytag, and Kargl 2011).

Institutional separation among the organizations that collect personal information (like through electronic tolling) from other government agencies (such as those responsible for traffic enforcement) is a common strategy. Such institutional separation is often more visible to consumers than internal privacy protections and has been found to improve public perceptions of privacy protection (Briggs and Walton 2000). Beyond perceptions, institutional separation between collection and analysis is also, in itself, a significant privacy protection (Center for Automotive Research 2012). Another option is the use of third parties to manage personal data, typically by encrypting or anonymizing the data (Kung, Freytag, and Kargl 2011; Steinfeld 2010). This is an attractive protection option, particularly for a government entity, when the ultimate user of the data could combine ITS and other data in order to re-identify the user.

While privacy-by-design systems have obvious technical advantages, there are various downsides. First, restricting collection of *possibly* private data from the outset provides less information and thus limits the usefulness of data for many non-personally invasive purposes. For example, eliminating the collection of a person's home address greatly limits the travel behavior research possibilities of a data set. Second, privacy-by-design protections are relatively expensive since they must be built into the system at every stage of development and deployment, and as a result are not very adaptable to inevitable system evolution, multi-jurisdiction systems, or activity-based ITS applications (Ban and Gruteser 2010; Kung, Freytag, and Kargl 2011) – a clear disincentive to ITS developers who tend to favor lowest cost options for privacy protection, such as less stringent data encryption and data storage security (Cottrill 2009). Third, Kung, Freytag, and Kargl (2011) also note that incorporating privacy-by-design creates challenges for distributing technology across multiple users in the absence of universal standards.

The diminished utility of anonymous data for transportation system planners and operators and the possibility of *ex post* re-identification combine to undermine the appeal of privacy-by-design ITS systems (Ohm 2010).

4.2. Privacy-by-policy

Privacy-by-policy refers to systems where PII is collected, but privacy is protected through the legal and functional treatment of the data. This describes most current privacy protections promulgated through public policy, voluntary industry standards, and consumer selected privacy preferences on sites like Facebook.

Privacy-by-policy approaches include both 'opt-in' data collection and 'opt-out' privacy protection. Under an opt-in framework, personal information is not collected unless the user explicitly agrees to collection, whereas in an opt-out scheme user data are collected by default unless the user takes the explicit step of 'opting out' of the collection. Research shows, however, that the effort required to opt-in or -out discourages many from either choice, so that the majority of users stay with the default regardless of actual preferences (Thaler and Sunstein 2008). As such, consumer groups tend to favor the first approach, which provides choice and notice to consumers, and industry groups typically favor the latter.

One benefit for organizations is that an opt-in scenario is typically legally sufficient to waive privacy liability, since the user explicitly agrees to data collection (Douma and Aue 2011). An opt-out scenario, on the other hand, may be deemed to constitute only 'implied consent' by the user that data may be collected, which is not as legally strong as explicit consent; in order for it to be legally sufficient to waive liability courts would have to determine whether notice was properly given and balance the interests of the organization in not providing an opt-in option. Douma and Aue (2011) suggest that implied consent may ultimately prove an effective schema for ITS, since implied consent is often sufficient when the states' interests are preventing injury, property loss, or loss of life. Fries et al. (2012) further suggest that implied consent for ITS technologies that advance safety aims should be tied to driver licensing requirements (much as drivers currently are deemed to give their implied consent to obey traffic officer requests for driving under the influence tests). But such an approach may not prove sufficient for ITS applications with other aims, such as transportation system efficiency, congestion mitigation, and emissions reductions, despite their substantial collective benefits. Still, any implied consent schema that required a person to accept a perceived invasion of privacy in order to drive might not stand up to judicial scrutiny (Internet Policy Task Force 2010).

The opt-in/opt-out dichotomy is an important example of the struggle to balance the usefulness and adoption of ITS applications with privacy protections for travelers. If presented with a flexible schema in which users explicitly set their own personal privacy preferences, those pushing for ITS applications worry that many people would set their preferences to strictly limit access, which would undermine the usefulness of the data for transportation system management – a principal motivation to pursue ITS in the first place (Cottrill 2009).

5. Evaluation and future directions

Though research on data-intensive ITS technologies is relatively new,[16] the literature on other data-intensive technology industries tells us a lot of about preferences and behavior of firms and consumers, as well as possible solutions to privacy challenges. First, meaningful privacy protections require that ITS applications should collect as little PII as possible and stringently protect what is collected. PII should furthermore be stripped from aggregated data or any data used for secondary purposes (Briggs and Walton 2000; Douma and Aue 2011).

Second, perception and trust greatly influence consumers' willingness to relinquish personal data. To encourage widespread adoption of ITS technologies, collecting entities must earn trust from consumers. This can be accomplished through greater transparency in

both the uses of the technology and policies governing the data collected. This may entail marketing campaigns to promote awareness of the presence of data-collecting ITS technologies, the reasons for them, and the privacy protections available to consumers. Agencies collecting data should be able to clearly articulate what data will be collected, how it will be protected, and for what it will be used. Absent explicit consumer opt-in, ITS-collected data should never be used for anything other than the stated purposes, and public agencies should be especially vigilant about secondary uses of data by third parties. For example, public agencies could require court-ordered warrants before turning over PII to law enforcement agencies for use in criminal proceedings (Briggs and Walton 2000; Center for Automotive Research 2012; Cottrill 2011; Douma and Aue 2011).

Third, research has shown that consumers will be more accepting of ITS privacy protection schema that offer travelers as many options as possible to meet their personal privacy preferences. Unfortunately, there is little research on how practical such options would be for ITS technologies, which are increasingly integrated into transportation infrastructure networks. Data are collected, integrated, and analyzed by so many parts of transportation systems, making individual opt-in privacy protections an increasingly complex challenge for ITS operators. Opt-in policies may also limit necessary data collection for systems that rely on complete aggregated information in order to function. Where it would be impractical to allow for substantial numbers of ITS consumers to opt-out, opting-in may be encouraged by providing users tangible benefits (such as suggested real-time shortest paths routes in congested conditions, or real-time on-street parking availability information) in exchange for personally identifiable private information (Briggs and Walton 2000; Center for Automotive Research 2012; Cottrill 2011; Douma and Aue 2011).

6. Conclusions

While the pace of both development and deployment is waxing, ITS are at a crossroads. ITS designers and managers face increasingly vexing challenges integrating the many components of transportation systems in order to increase their efficiency amidst a stubbornly muddled and uncertain regulatory environment. Absent clear regulatory guidance, they must consider privacy protection at the earliest possible stages of ITS development to insure flexibility in responding to both consumer privacy preferences and possible subsequent regulatory mandates. Such an environment calls for adaptability, in which products can easily incorporate new privacy design features.

Growing concerns over the massive data collection programs of the NSA and private firms like Google may eventually engender a voter privacy backlash resulting in strict new privacy laws and regulations, or they may numb consumers to the comparatively innocuous personally identifiable data collection efforts of ITS system operators. Absent regulatory mandates, principles directing ITS system operators to share data collection and distribution practices with consumers and to collect the minimum amount of personal data necessary to achieve the ends of the program or project are important to protect traveler privacy. For example, collecting data that delete the first and last kilometer of each trip can protect the home address and destinations of travelers, while providing transportation analysts with needed system use data. ITS system designers must also consider how

privacy-by-design features might be built into systems from the outset, such as through data encryption, password protection, and/or third-party storage.

Beyond designing in privacy protections, ITS system managers can choose to adopt commonly recommended policies (Briggs and Walton 2000; Center for Automotive Research 2012; Cottrill 2011; Douma and Aue 2011) such as the routine deletion of PII from archived data after it has been used for its stated purpose. While this may not fall directly on ITS designers, it is an important feature of privacy protection, and designers can make it easier for collecting agencies to permanently delete personal data. Such policies are particularly effective when collaborating government agencies all choose to adopt similar practices (DeBlasio et al. 1999).

An important gray area is consumers' willingness to relinquish private information in exchange for personal benefits. Private firms are quickly learning that consumers' privacy concerns recede when desirable information is provided. To date, the literature has dealt mostly with financial remuneration from private companies for such data. But this becomes more difficult in the context of ITS, where government may be discouraged from 'selling' information to those who will 'pay' with relinquished privacy.

Finally, ITS systems designers and managers need to consider the important privacy challenges of system integration, where data are moved freely among mobile devices, vehicles, and roads. Technologies embedded in infrastructure are localized, involving commitments from municipalities, and generally (though not absolutely) give the user little or no choice whether to participate. Vehicular technologies place more of the burden on manufacturers and allow for greater consumer choice, but face issues of whether a critical mass is necessary for adoption in order that the full benefits of these new technologies can be realized.

Such general recommendations aside, additional research on ITS and privacy is clearly needed. Most of the existing research deals with data collection by private companies, or by government, particularly in the context of law enforcement and criminal rights. One of the most revealing things from our survey of the literature is that *personal data* is not a clearly defined term, and its meaning varies greatly depending on the situation. Therefore, protective treatment of the personally identifiable data in one context may not translate meaningfully to another.

A particularly understudied topic is how personal data are protected from access by law enforcement. Much research has shown the heightened concern of criminal penalties resulting when the government is the collecting party. It may be necessary to craft ITS-specific laws that prohibit the use of personal data by law enforcement in order to overcome these concerns, but there is little research exploring the necessary parameters of such legislation.

Given the great variety of ITS technologies making their way into the market, it is unlikely that any single universal approach will be sufficient to ease concerns over data collection and dissemination in all circumstances. Each technological situation will likely need to be addressed based on its own particular circumstances and appropriate policies will need to be developed that permit weighing the benefits of greater information gathering against the potential costs.

One key issue is whether, given the potential for disclosure of their private information, consumers will buy in to using new technologies and how if at all to overcome any such resistance. Those employing ITS will have to establish a high trust level by at least making

consumers better aware of what ITS data are being used for, why collecting certain types of personal and travel information is necessary, and perhaps offering various options for control over what information is collected, how it is used, who has access to it and for how long, as well as possibly giving consumers tangible direct benefits to compensate them for their participation.

Those wishing to advance the development of ITS will need to be cognizant of the potential pitfalls from the collection and use of personal information and give serious consideration to policies that build consumer confidence in the process. This can be accomplished by limiting the collection of personal information to only that necessary to meet project objectives, or by protecting such information from being disseminated beyond those entities collecting it, or by limiting its use for purposes beyond those for which it is originally collected. Whatever path is followed, acceptance of PII collection by ITS technologies is likely to hinge on consumers being fully aware of ITS data collection practices and having given their informed consent in some legally defensible fashion.

Notes

1. On 2 June 2015, the Senate passed and President Obama signed the USA Freedom Act that ended the National Security Administration's bulk collection of individual's phone records but which requires phone service providers to retain the metadata and permits the NSA to conduct searches of the material with judicial approval (Kelly 2015).
2. Generalizing from privacy issues present in cellular phone technology both provides insight into the issues presented by location tracking, and also in some cases cell phones may be used for ITS applications, such as monitoring traffic conditions (McDonald and Cranor 2006).
3. The United States is the only developed western nation that has not passed comprehensive privacy legislation, generally favoring a sectoral approach related to specific concerns, such as medical and financial records (Bennett 2011; Phillips and Kohm 2011). Comprehensive privacy legislation is a stated goal of the Obama Administration (Angwin, Thurm, and Hickins 2011) but it appears to have fallen behind other legislative priorities.
4. Currently some states, like California, limit the use of such data for setting insurance rates.
5. The Obama Administration released a "Consumer Bill of Privacy Rights" in February of 2012 outlining the basic principles it hoped to ultimately include in privacy legislation, and urged Internet companies to adopt the guidelines in the interim (Ngak 2012). These principles address the procedural dangers of legal uncertainty and stress that national guidelines would ameliorate the uncertainty caused by divergent state laws and standards (The White House 2012).
6. This program was begun in response to the 1991 Intelligent Vehicle Highways Systems Act, which annually allocated $250 million to ITS research and testing and required the Secretary of Transportation to report to Congress regularly on policy concerns related to the ITS program (Dingle 1995).
7. These principles include respect of individuals' right to privacy, public transparency on what information is collected and how, data security guidelines, relevancy of data collected to the task at hand, anonymity when practicable, limiting secondary use to non-PII (personally identifiable information) data only, and oversight mechanisms to ensure compliance with these principles. The FIPPs (sometimes FIPs) inform and guide the federal government's rules governing privacy (Ohm 2010). These principles attempt to provide guidance for the private sector to self-regulate in the current fractured legal environment (Phillips and Kohm 2011). They were updated in 2012 by the FTC, which has become a de-facto – if unofficial – government privacy enforcer (Bamberger and Mulligan 2011). Though FTC authority is currently limited to consumer protection (Angwin, Thurm, and Hickins 2011), there is momentum towards granting them statutory power to enforce privacy violations (The White House 2012).

8. The 2012 update to the program's Strategic Research Plan summarizes concerns over privacy and liability guidance for stakeholders. These include the

> development of policies and practices to appropriately protect privacy and comply with applicable privacy laws; research and analysis of the Department's authority as it relates to the connected vehicle environment; analysis of stakeholders' potential legal risks and liability for purposes of providing recommendations about whether the Federal government should consider a risk-sharing regime; assessment of intellectual property/data ownership issues that might hinder adoption of connected vehicle technologies; and, identification of legal parameters and considerations relative to governance, funding and other aspects of implementation.

9. There are many factors that determine whether the lawsuit is brought under the state where the accident occurred, the state where the product is manufactured, the home state of the driver, etc., all of which may have different legal standards in such cases.
10. Zimmer (2005) noted the particular dangers of rapid advances in ITS for privacy, calling the problem of privacy in public the 'key casualty' of the laws' inability to maintain pace with technology.
11. The private sector is by nature more nimble and has the economic incentive to bear the liability risks if a product is profitable, and industries will develop self-regulation to encourage adoption of their products if there are no federal guidelines (West and Lu 2009). While this sort of regulatory capture may seem irresponsible to many, it is often a necessary byproduct of the slow-moving legislative-regulatory system and its heavy administrative costs. Furthermore, industries have the incentive to self-regulate as they experiment in an open legal environment, ultimately aiming to present their legal framework as a positive starting point for legislation.
12. Privacy concerns have been cited by municipalities as a factor against installing traffic and red-light camera technologies (McDonald and Cranor 2006) and vehicle-mile tolling (Eno Center for Transportation 2012). A 2010 survey of state and municipal transportation agencies illustrates the differing state-by-state treatment of privacy in the deployment of ITS applications. Many municipalities have chosen not to employ red-light camera enforcement due to privacy concerns and lack of legal guidance. A survey of agencies by Fries et al. (2012) found similarly varying responses to the use of GPS by law enforcement, as well as guidelines for the treatment and storage of surveillance data. Thirty-nine percent of survey respondents expressed the view that privacy concerns, either real or perceived, were the primary impediment to successful implementation of vehicle mile tolling systems.
13. The growth in the concern over privacy protection is evidenced by the recent Congressional discussion of a 'Do Not Track' initiative, which spurred popular Internet browsers to publicize the addition of 'Do Not Track' features. Mozilla reported that 11% of users have turned the feature on, and 18% have enabled a similar feature that blocks locational data collection on the mobile browser. The Mozilla Global Privacy and Policy Leader said, 'If you're receiving millions of these signals every day, it reaches critical mass and they can't ignore it' (Singer 2012).
14. Ban and Gruteser (2010) note that transportation modelers have traditionally sought to obtain as much information as possible and view privacy concerns as a limiting factor. They argue that transportation modeling research should explore ways to achieve the same results using less personal data. For example, they point out that measuring travel speed and delay can be accomplished by measuring between two fixed locations as opposed to collecting real time trajectory data. By using two fixed points, the privacy concerns of knowing the path a vehicle is travelling are alleviated.
15. For example, transportation analysts monitoring congestion desire aggregated data, collected in real time, which quickly loses value. In contrast, academic researchers value individualized data for detailed analyses of cause and effect, but do not value immediacy (Liu et al. 2002).
16. Some guidance in the ITS arena can be gleaned from the Intelligent Transportation Society of America's Fair Information and Privacy Principles and from the government's IntelliDrive

Privacy Policies Framework (Intelligent Transportation Society of America 2014; Intelligent Transportation Systems Joint Program Office 2009), which acknowledges that the program's previous focus on privacy-by-design raised many questions about complexity, deployability, and cost. Accordingly, the focus was shifted to incorporate privacy-by-policy protections. Still, Cottrill (2009) criticizes the Department for not incorporating enough privacy-by-policy protections to bolster what she characterizes as failed ITS privacy-by-design principles.

Acknowledgements

We thank Jane Berner (Caltrans), Jim Misener (consultant), and Joan Walker (UC Berkeley) for their valuable comments and suggestions are earlier versions of this manuscript. We also thank Juan Matute, Allison Yoh, and Joseph Issa in the UCLA Institution for Transportation Studies for their guidance on this project and assistance with the preparation of this manuscript. Finally, any errors or omissions are the responsibility of the authors alone, and not the NSF or those thanked herein.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This research was funded by Grant # 1111971 from the US National Science Foundation, and the authors are grateful for this support. The authors do not have any commercial ties to any of the private organizations discussed in this paper.

References

Angwin, Julia, Scott Thurm, and Michael Hickins. 2011. "Lawmaker Introduces New Privacy Bill." *Wall Street Journal Digits: Tech News & Analysis from the WSJ*, February 11. http://blogs.wsj.com/digits/2011/02/11/lawmaker-introduces-new-privacy-bill/.

Arthur, Charles. 2011. "TomTom Satnav Data used to set Police Speed Traps." *The Guardian*, April 28. http://www.theguardian.com/technology/2011/apr/28/tomtom-satnav-data-police-speed-traps.

Bagby, John W., and Gary L. Gittings. 1999. "Litigation Risk Management for Intelligent Transportation Systems." *ITS Quarterly* 7 (3): 53–67.

Bamberger, Kenneth A., and Deirdre K. Mulligan. 2011. "Privacy on the Books and on the Ground." *Stanford Law Review* 63: 247–316.

Ban, Xuegang, and Marco Gruteser. 2010. "Mobile Sensors as Traffic Probes: Addressing Transportation Modeling and Privacy Protection in an Integrated Framework." In *Traffic and Transportation Studies 2010*, edited by Baohua Mao, Zongzhong Tian, Haijun Huang, and Ziyou Gao, 750–767. Reston, VA: American Society of Civil Engineers.

Bennett, Steven C. 2011. "The Politics of Privacy." *The National Law Journal*, January 31.

Briggs, Valerie, and C. Michael Walton. 2000. *The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data*. Austin, TX: University of Texas at Austin, Center for Transportation Research. http://swutc.tamu.edu/pub … hnicalreports/721925-1.pdf.

Center for Automotive Research. 2012. *Ethics of Government Use of Data Collected Via Intelligent Transportation Systems*. Ann Arbor, MI: Michigan Department of Transportation. http://www.mi.gov/documents/mdot/MDOT_EthicsDataCollectedITS_394489_7.pdf.

Cottrill, Caitlin D. 2009. "Approaches to Privacy Preservation in Intelligent Transportation Systems and Vehicle-Infrastructure Integration Initiative." *Transportation Research Record: Journal of the Transportation Research Board* 2129: 9–15. doi:10.3141/2129-02.

Cottrill, Caitlin D. 2011. "Location Privacy: Who Protects?" *URISA Journal* 23 (2): 49–59. http://ares.lids.mit.edu/fm/papers/Cottrill.URISA.pdf.

Cottrill, Caitlin D., and Piyushimita Thakuriah. 2011. "Protecting Location Privacy: Policy Evaluation." *Transportation Research Record: Journal of the Transportation Research Board* 2215: 67–74. doi:10.3141/2215-07.

DeBlasio, Allan J., David Jackson, Anne C. Tallon, Gerald M. Powers, and John P. O'Donnell. 1999. *Successful Approaches to Deploying a Metropolitan Intelligent Transportation System*. Cambridge, MA: U.S. Department of Transportation, Volpe National Transportation Systems Center. http://ntl.bts.gov/lib/jpodocs/repts_te/8483.pdf.

Dingle, Julie. 1995. "FHWA, IVHS, and Privacy." *Santa Clara High Technology Law Journal* 11 (1): 15–20. http://digitalcommons.law.scu.edu/chtlj/vol11/iss1/3.

Douma, Frank, and Sarah Aue. 2011. *ITS and Locational Privacy: Suggestions for Peaceful Coexistence*. Minneapolis, MN: University of Minnesota, Center for Transportation Studies, Intelligent Transportation Systems Institute. http://www.hhh.umn.edu/centers/slp/transportation/pdf/ITSandLocationalPrivacy-SuggestionsforPeacefulCoexistence-FinalReport.pdf.

Douma, Frank, and Jordan Deckenbach. 2009. "The Challenge of ITS for the Law of Privacy." *University of Illinois Journal of Law, Technology and Policy* 2009 (2): 295–332. http://illinoisjltp.com/journal/wp-content/uploads/2013/10/Douma-Deckenbach.pdf.

Eno Center for Transportation. 2012. *Transportation Investment as Part of a Deficit-Reduction Package*. Washington, DC: Eno Center for Transportation. https://www.enotrans.org/wp-content/uploads/wpsc/downloadables/Deficit-Redux-paper1.pdf.

Fries, Ryan N., Mostafa Reisi Gahrooei, Mashrur Chowdhury, and Alison J. Conway. 2012. "Meeting Privacy Challenges While Advancing Intelligent Transportation Systems." *Transportation Research Part C: Emerging Technologies* 25 (Dec. 2012): 34–45. doi:10.1016/j.trc.2012.04.002.

FTC (Federal Trade Commission). 2012. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*. Washington, D.C.: Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

FTC (Federal Trade Commission). 2015. "Privacy Impact Assessments." Federal Trade Commission. http://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

Glancy, Dorothy J. 2009. "Retrieving Black Box Evidence from Vehicles: Uses and Abuses of Vehicle Data Recorder Evidence in Criminal Trials." *The Champion*, May 12.

Intelligent Transportation Systems Joint Program Office. 2009. *Anonymity and IntelliDrive, Pre-Decisional Discussion Document*. Washington, DC: U.S. Department of Transportation, Research and Innovation Technology Administration.

Internet Policy Task Force. 2010. *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*. Washington, DC: U.S. Department of Commerce. http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

ITSA (Intelligent Transportation Society of America). 2014. "ITS America's Fair Information and Privacy Principles." Intelligent Transportation Society of America. Accessed April 28, 2014. http://www.itsa.org/images/mediacenter/itsaprivacyprinciples.pdf.

ITSA (Intelligent Transportation Society of America). 2015. "ITSA." Intelligent Transportation Society of America. http://itsa.org/.

Kelly, Erin. 2015. "Senate Approves USA Freedom Act." *USA Today*, June 2. http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/.

Kung, A., J.C. Freytag, and F. Kargl. 2011. "Privacy-by-Design in ITS Applications: The Way Forward." Paper presented at the Second International Workshop on Data Security and Privacy in Wireless Networks (D-SPAN), Lucca, Italy, June 20–24.

Liu, Henry X., Rachel He, Yang Tao, and Bin Ran. 2002. *A Literature and Best Practices Scan: ITS Data Management and Archiving*. Madison, WI: University of Wisconsin at Madison. http://wisdotresearch.wi.gov/wp-content/uploads/02–11itsdata-f.pdf.

Maccubbin, Robert P., Barbara L. Staples, Firoz Kabir, Cheryl F. Lowrance, Michael R. Mercer, Brian H. Philips, and Stephen R. Gordon. 2008. *Intelligent Transportation Systems: Benefits, Costs, Deployment,*

and Lessons Learned. Washington, DC: U.S. Department of Transportation, Research and Innovation Technology Administration. http://ntl.bts.gov/lib/30000/30400/30466/14412.pdf.

Markey, Ed. 2015. "Tracking & Hacking: Security & Privacy Gaps Put American Drivers At Risk." *U.S. Senate*. http://www.markey.senate.gov/imo/media/doc/2015–02–06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

McDonald, Aleecia M., and Lorrie Faith Cranor. 2006. "How Technology Drives Vehicular Privacy." *I/S: A Journal of Law and Policy for the Information Society* 2 (3): 981–1015. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/u-mcdonald-cranor.pdf.

Ngak, Chenda. 2012. "Obama's 'Consumer Privacy Bill of Rights' Tackles Online Privacy Concerns." *CBS News*, February 23. http://www.cbsnews.com/news/obamas-consumer-privacy-bill-of-rights-tackles-online-privacy-concerns/.

Ohm, Paul. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57 (6): 1701–1777. http://www.uclalawreview.org/pdf/57–6–3.pdf.

Orszag, Peter. 2010. *Guidance for Agency Use of Third-Party Websites and Applications*. Washington, DC: Executive Office of the President, Office of Management and Budget. https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10–23.pdf.

Ozer, Nicole A., Chris Conley, Hari O'Connell, Ellen Ginsburg, and Tamar Gubins. 2010. *Location-Based Services: Time for a Privacy Check [White Paper]*. San Francisco, CA: ACLU of Northern California. http://aclunc-tech.org/files/lbs-privacy-checkin.pdf.

Pethtel, Ray D., James D. Phillips, and Gene Hetherington. 2011. *A Policy Review of the Impact Existing Privacy Principles have on Current and Emerging Transportation Safety Technology*. Blacksburg, VA: Virginia Tech, The National Surface Transportation Safety Center for Excellence. http://scholar.lib.vt.edu/VTTI/reports/PrivacyFinalReport_05122011.pdf.

Phillips, James D., and Katharine E. Kohm. 2011. "Current and Emerging Transportation Technology: Final Nails in the Coffin of the Dying Right of Privacy?" *Richmond Journal of Law and Technology* 18 (1): 1–31. http://jolt.richmond.edu/v18i1/article1.pdf.

Sapienza, Russell J. 2012. "Ready, Willing and Able? Consumer Attitudes on Data Privacy." *Huffington Post*, October 1. http://www.huffingtonpost.com/russell-j-sapienza-jr/consumer-attitudes-privacy_b_1927893.html?view=screen.

Singer, Natasha. 2012. "When the Privacy Button is Already Pressed." *New York Times*, September 15. http://www.nytimes.com/2012/09/16/technology/in-microsofts-new-browser-the-privacy-light-is-already-on.html.

Steinfeld, Aaron. 2010. "Ethics and Policy Implications for Inclusive Intelligent Transportation Systems." Paper presented at the Second International Symposium on Quality of Life Technology, Las Vegas, NV, June 28–29.

Thaler, Richard H., and Cass R. Sunstein. 2008. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New Haven, CT: Yale University Press.

"The End of Privacy?" 2012. *New York Times*, July 14. http://www.nytimes.com/2012/07/15/opinion/sunday/the-end-of-privacy.html.

The White House. 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Washington, DC: The White House. https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Wang, J. L., and M. C. Loui. 2009. "Privacy and Ethical Issues in Location-Based Tracking Systems." Paper presented at the IEEE International Symposium on Technology and Society, Tempe, AZ, May 18–20.

West, Darrell M., and Jenny Lu. 2009. *Comparing Technology Innovation in the Private and Public Sectors*. Washington, DC: Brookings Institution. http://www.brookings.edu/~/media/research/files/papers/2009/6/technology-west/06_technology_west.pdf.

Xu, Heng, Hock-Hai Teo, and Bernard C. Y. Tan. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk." In *International Conference on Information Systems 2005 Proceedings*. AIS Electronic Library.

Zimmer, Michael. 2005. "Surveillance, privacy and the Ethics of Vehicle Safety Communication Technologies." *Ethics and Information Technology* 7 (4): 201–10. doi:10.1007/s10676-006-0016-0.