PRIVATE EYE:
INTELLIGENT TRANSPORTATION SYSTEMS AND PERSONAL PRIVACY

14 November 2014
Paper submitted for presentation at the
2015 Annual Meeting of the Transportation Research Board
7394 words

by

Jaimee Lederman, JD
(310) 562-7356
jaimee.lederman@ucla.edu

Mark Garrett, JD, PhD (corresponding author)
(310) 562-7356
mgarrett@ucla.edu

Brian D. Taylor, PhD
(310) 903-3228
btaylor@ucla.edu

UCLA Institute of Transportation Studies
3250 Public Affairs Building
Los Angeles, CA 90095-1656
www.its.ucla.edu
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 norms. 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 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 through 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 confidentiality of data storage, and other ways to build trust and foster consumer consent.
PRIVATE EYE: INTELLIGENT TRANSPORTATION SYSTEMS AND PERSONAL
PRIVACY

INTRODUCTION
Intelligent Transportation Systems (ITS) hold great promise to address economic, environmental, and social problems but also raise significant issues with respect to personal privacy. ITS depends on gathering, analyzing, and acting on large amounts of individualized data to, for instance, personalize navigation and to forecast travel behavior. Many modern technologies collect personal information, but ITS is unique in its public nature and its potential to collect information about travelers as well as their position and movement, often times without explicit consent on the part of the consumer, who may not be fully aware of how intrusive ITS data collection can be. Such information can now be combined with other personal information about travelers from ever expanding reservoirs of data to reveal a very great deal about individuals, their activities, and travel in a manner that may be viewed by many as a gross invasion of privacy for those who do wish to have their every movement tracked.

How much privacy do consumers demand? What can be done to protect information from disclosure or misuse? What should be done in cases 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? These important questions that sit at the juncture of transportation engineering, law, and public policy are the focus of this article.

However, the increasingly prodigious production and consumption of data on vehicle movement (and, by extension, the people and goods in them) has outpaced the evolution of laws governing the collection, ownership, availability, and use of such data, raising important privacy questions. Potentially, private information relating to specific individuals and their actions may be made widely available to others beside those collecting it, or personal information acquired for one reason acceptable to the user may be used for another entirely unrelated and unapproved purpose. To date, there is very little in the way of legal guidance regarding the ever-greater volumes of information being generated about the movement of people, goods, and vehicles. Moreover, 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. The lack of accepted universal privacy standards may ultimately make consumers more reluctant to accept those benefits and could even inhibit further development and deployment of ITS technology.

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 expectation 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 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.
ITS AND DATA COLLECTION

Intelligent transportation systems represent 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, real-time public transit arrival and departure information, delay-sensitive navigation systems, and GPS-enabled destination searches on personal mobile devices are just a few of the many dozen ITS technologies. Each may collect different types of personal information.

ITS technologies

ITS technology can be categorized in many ways, including by whether it is deployed 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 of violating vehicles to registration data. They also often provide a photograph of the driver of the vehicle, who may or may not be the registered owner. 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.
- **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 or individuals riding in them is present.
- **Automatic tolling devices:** These use transponders in vehicles to record vehicles passing a tolling gantry 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.
- **Parking information services:** Some cities have begun experimenting with sensors embedded in on street parking spaces connected to 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.
- **Smart transit passes:** As transit agencies shift 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 fund balance, 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. 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.

Even purely informational systems may have the capacity to collect personal information
from users. Transit arrival and departure information can now be posted to electronic billboards
located at transit stops, or via computers, tablets, or smart phones. While users may access this
information anonymously, it may be also possible to collect data on the device being used,
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.

Private industry is also collecting information related to ITS. 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 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 offer drivers discounts for limiting night-time driving, speeding, or
sudden stops – factors they have determined to be associated with higher claims rates. Some
insurers are marketing these services to parents, enabling them, and insurance companies, to
track teen 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 are likely unaware of the extent of the information now being collected
about their travel by newer vehicles.

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 accelerate and decelerate, the routes they take, and whether they adhere to other
corporate policies. As more and more vehicles are coming factory-equipped with computerized
components and services it is increasingly difficult for private automobile drivers to avoid
generating similar information that can then be collected by the manufacturer or other third
parties.

U.S. PRIVACY LAW

There are currently no comprehensive laws in the U.S. addressing privacy protections vis-à-vis
ITS technologies. 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. In fact, 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 (1; 2).

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 (3). There has recently been a flurry of proposed
consumer privacy legislation, but no comprehensive legislative scheme for privacy protection.
(See http://ftc.gov/os/2012/03/120326privacyreport.pdf, for a list of such proposed legislation.)
Privacy legislation is a stated goal of the Obama Administration (4), but it appears to have fallen
behind other legislative priorities. The Administration did release 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 (5).
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 (6).
The federal Connected Vehicle Research program published its own set of Fair Information
Practice Principles (FIPPs), but the DOT has yet to craft ITS-specific privacy and legal
guidelines. The FIPPs (sometimes FIPs) inform and guide the federal government’s rules
governing privacy (7). These principles attempt to provide guidance for the private sector to self-
regulate in the current fractured legal environment (1).

The 2012 update of 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.”

Aside from these there are a series of “model laws” and administrative guidance put forth
mainly by the Federal Trade Commission (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 (8). The FTC has become a defacto—if unofficial—government privacy
enforcer (9). Though FTC authority is currently limited to consumer protection (4), there is
momentum towards granting them statutory power to enforce privacy violations (6).

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 (10; 11). For example, in 2004 California passed what
at that time was the only ITS-specific privacy law in the U.S., requiring vehicle manufacturers to
give notice about the presence of Electronic Data Recorders (EDRs) in their vehicles, and
granting buyers complete control over how black-box data, automatically collected about the
driving behavior of the car, is used (12). 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 (1).
Differing state legal regimes pose a challenge to ITS deployment as manufacturers and
service providers may be forced to comply with multiple, and sometime contradictory, standards
(7). 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 (12). 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?

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 (13). 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 (14). 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. ITSA has developed its own version of the FIPPs (see http://www.itsa.org/images/mediacenter/itsaprivacyprinciples.pdf). These principles include respect for individuals’ right to privacy, public transparency on what information is collected and how, data security guidelines, relevance of data collected to the task at hand, anonymity when practicable, limiting secondary use to non-personally identifiable information only, and oversight mechanisms to ensure compliance with these principles. Though non-binding, states may minimize risk by following these guidelines if future national laws are eventually developed in collaboration with ITSA (15).

The impact of ITSA model laws and regulations on actual privacy practices is unclear. Since they are voluntary guidelines, Cottrill (10) argues that manufacturers and governments have little incentive to invest money to protect privacy to a standard that is neither universal nor required, and 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 (16). But if manufacturers increasingly conform to ITSA guidelines in the months and years ahead, they may ultimately prove too ingrained for future legislation to ignore. Still, some consumer advocates worry that the public sector will ultimately allow private industry to largely dictate ITS privacy regulations (17).

DATA MANAGEMENT AND PRIVACY LAW

The spatial nature of travel demands data sharing among ITS devices and networks across multiple jurisdictions in order to fully realize promised efficiencies and other gains (18). Multi-jurisdictional and metropolitan planning organizations have been able to broker information sharing policies to regulate and standardize access and protection issues (18), 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 (10). It appears likely that some form of federal privacy regulation is on the way, but how soon and what form it takes is still to be determined given the current profound partisan impasse in Congress. 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. Further, high-profile negative publicity over harms to individuals whose privacy rights may have been violated...
Evaluating privacy concerns

People’s desires for privacy protections are evolving along with technology. For instance, location-tracking applications via mobile telephones are increasingly commonplace, while the proportion of people who say they are concerned about their privacy has also increased (19). A November 2010 study found that 55 percent of those already using location based services are concerned about their loss of privacy (20). Eighty-seven percent of survey respondents wanted control over what personal information is shared and how it is being used (21).

Privacy concerns vary from person to person and are largely dependent on 1) the personal nature of the data collected, 2) the specific party collecting the information, 3) user perceptions of the technology used to collect data, 4) trust in whoever is collecting the information, 5) the stated reasons for collecting data, and 6) who else may have access to the data (8). These are discussed below.

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.

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 a way that subsequently enables individual identification (22). Cottrill and Thakuriah (23) estimate that 87 percent of the population can be identified by searching only zip code, sex, and date of birth. The U.S. 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 (24).

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 (25). 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.

Who is collecting the information?

Another 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 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 \( (25) \). As the government already possesses so much personal information from other sources, many users may fear giving it locational data as well, especially if it may lead to criminal prosecution.

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.

**User perceptions and preferences**

Research suggests that an individual’s desire for privacy protection in the context of a particular technology is largely determined by his or her context-specific perception of the technology, rather than a consistently principled consideration of privacy concerns.

One of the primary concerns is that ITS will create a “big brother” who will track everyone’s 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 \( (26) \). In a 2000 survey of municipal governments’ experiences with ITS deployment, Briggs & Walton \( (11) \) found that public perceptions were highly correlated with 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 \( (11; 26) \).

**Trustworthiness**

Closely linked to ITS privacy perceptions is trust in the organization collecting the data \( (23; 27) \). Several private sector privacy policing systems are now available in response to both pressure from ITS industries and economic incentives \( (28) \). These “privacy professionals” 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 \( (27) \) and grant companies use of their seals of approval to gain consumer confidence \( (9; 28) \). 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 \( (27) \). 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 \( (27) \).

**Aims of the technology**

Research has also shown that people have greatly differing privacy preferences depending on the aim of the technology. The clearest concerns involve the use of information gained through ITS or other technology by law enforcement. But the existence of such copious data is also an
undeniably attractive tool for crime prevention. With the recent surge in smartphone use, over
the past five 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
require a warrant under increasingly outdated electronic surveillance legislation and rules (29).
The Supreme Court has unanimously restricted the police’s ability to attach a GPS device to a
suspect’s car but left unanswered whether obtaining that same information from a service
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 private commercial data use. Commercial products
more often provide a personal benefit to the user, such as GPS navigation and the location of the
nearest well-reviewed independent coffeehouse, for which many people are willing to 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.

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,
including 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 (3). Transportation agencies
must similarly carefully monitor who has access to data in order to balance privacy and
information sharing demands (18). Secondary usage also increases the chances that data may be
aggregated, heightening concern over personal identification (10).

Concern over secondary usage of data is prevalent in privacy scholarship (11; 25); users
are regularly reluctant to relinquish personal information if they are ultimately not in control of
who has access to it and what it is used for (10). For example, the GPS manufacturer TomTom
generated 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 (30).

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 (31). Due to these concerns, many scholars (10; 11; 25)
have proposed substantial restrictions on secondary use of data, particularly by the public sector.

IMPROVING ITS PRIVACY PROTECTIONS
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. Based on a review of the technology and privacy literature – both in transportation and other sectors – it appears likely that if a comprehensive, flexible ITS privacy policy is to emerge, it will do so as a hybrid privacy regime for ITS that draws from privacy protections adopted and proposed for other, non-ITS technologies. Currently, there are two main mechanisms for technology-related privacy protections: privacy-by-design and privacy-by-policy, which are discussed in turn below.

**Privacy-by-design**

Protections that are embedded into the technological system are referred to as privacy-by-design. This framework stresses maintaining the anonymity of data either by never collecting PII or by stripping it of unique identifiers before storage. Ohm (7) postulates that privacy 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 (19; 32; 33). Though such system design-focused approaches can prove a challenge when multiple systems and multiple data users are involved. The second-best approach is often to adopt the most secure way to manage needed PII (32).

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 to improve public perceptions of privacy protection (11). Beyond perceptions, institutional separation between collection and analysis is also a significant privacy protection itself (34). Another option is the use of third parties to manage personal data, typically by encrypting or anonymizing the data (32; 33).

While privacy-by-design systems have obvious technical advantages, there are various downsides. First, restricting collection of possibly private data from the outset can limit the usefulness of data collection for many non-personally invasive purposes. For example, eschewing collecting trip origin and destination zones greatly limits travel behavior research possibilities. Second, privacy-by-design protections are relatively expensive since they must be built into the system at every stage of development and deployment (19; 32) – a clear disincentive to ITS developers who tend to favor lowest cost options for privacy protection (10). Third, Kung et al. (32) also note that incorporating privacy-by-design creates challenges for distributing technology across multiple users in the absence of universal standards.

**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. 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 (35). As such, consumer groups
tend to favor the first approach, which provides choice and notice to consumers, while 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 (25). 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. Douma & Aue (25)
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, Gahrooei, Chowdhury, and Conway (8) 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
dUI 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 (36). The opt-in/opt-out dichotomy is an important
element 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 (10).

EVALUATION AND FUTURE DIRECTIONS

Though research on data-intensive ITS technologies is relatively new, 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 (11; 25).

Second, 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 they will be protected, and for what
they 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, particularly law enforcement agencies (11; 25; 28; 34).

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 actors in so many parts of transportation
systems, that individual opt-in privacy protections are 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 \((11; 25; 28; 34)\).

In sum, we 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. While each of these four ITS privacy dimensions is conceptually distinct, there are of course interrelations among them, which highlight the importance of addressing all four dimensions in any comprehensive ITS privacy program.

CONCLUSIONS AND RECOMMENDATIONS

While the pace of both development and deployment is waxing, intelligent transportation systems are at a crossroads. Absent clear regulatory guidance, increasingly invasive ITS must consider privacy protection at the earliest possible stages of 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. 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 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 still 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 such as the routine deletion of personally-identifiable information from archived data after it has been used for its stated purpose \((11; 25; 28; 34)\). 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 \((26)\).

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.
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.

Acknowledgements

This research was funded by Grant # 1111971 from the 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 article. We thank Jane Berner (Caltrans), Jim Misener
(consultant), and Joan Walker (UC Berkeley) for their valuable comments and suggestions on
erlier 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.
REFERENCES


Douma, F., and S. Aue. ITS and Locational Privacy: Suggestions for Peaceful Coexistence. In, University of Minnesota, Center for Transportation Studies, Intelligent Transportation Systems Institute, Minneapolis, 2011.


