8 People and place
Patterns of individual identification within intelligent transportation systems

Colin Bennett, Charles Raab, and Priscilla Regan

Introduction
One of the most interesting and perhaps ambitious applications of geographic information technologies is the development of Intelligent Transportation Systems (ITS). Implementation of ITS requires the application of technologies to both roadways and vehicles to perform surveillance, communications, data processing, traffic control and navigational tasks. The range of ITS is extensive, and includes services such as the wireless provision of traffic information to drivers, law enforcement, the management of commercial vehicle fleets, environmental regulation, the provision of route and location information to the traveler, and – the topic of this chapter – electronic toll collection.

In this chapter, we compare the implementation of three current systems of road toll collection: the 407 Highway system in Toronto, Ontario; the Smart Tag system in Virginia; and, more briefly, the Dartford River Crossing in England. Potentially, the systems allow an almost unparalleled level of tracking of vehicle users. A host of questions are relevant: To what extent is this actually occurring? What sorts of data are collected, and to what extent do vehicle users know about these collection and processing activities and have control over them? Are data matching and integration occurring, and what are the implications for individual privacy? Are these systems tracking vehicles as they cross geographically situated toll collection centers? What are the intended and unintended consequences for power relations between public and private agencies, on the one hand, and individuals, on the other?

These questions frame a partial agenda for investigating ITS, and geographic information systems (GIS) generally. Such investigation is important because the implementation of surveillance systems to track human movement is rapidly becoming a common practice. Its trajectory has outpaced the ability of theory, research and regulatory policy adequately to comprehend.
or control it, although ITS has attracted attention in academic as well as regulatory policy circles (Agre and Harbs 1994; Wright 1995). Empirical studies of how ITS works, and of its contexts, are not yet so prolific as to confirm or reject the forebodings of those who directly, and in our view incautiously, read off human consequences from the technological possibilities of ITS and GIS. Yet human processes related to mobility—movement through space—have become a focus of attention in a wide variety of organizations and jurisdictions for which mobility is either a problem or an opportunity.

Data-handling systems for locating, identifying and recording persons’ behavior and preferences, including the authentication of individuals’ claims, provide the infrastructure for many processes. These include electronic commerce and the electronic delivery of public services, but with more particular reference to ITS, they include the control of physical movement across borders and the control of access to premises and other spaces. Within or alongside these processes are further examples: the provision of services or goods to those on the move, the extraction of payment for the movement or the tracking of volume and speed of movement, and the tracking of criminal suspects in transit. "Surveillance" is the term that most usefully embraces these activities.

Although we cannot here explore the complex issues involved in human identity and identification, they are at the heart of our inquiries into ITS and other applications of GIS. They also reinforce a view of the broadly political nature of ITS and GIS as if these systems affect the distribution of values within and across societies, and affect the fate of persons and groups. More concretely, the "politics" of ITS and GIS—which we barely touch on here—involves decision-making concerning the application of technologies to the purposes of government and the economy, and the implementation of rules for their use. But the significance of these systems goes beyond the political into more intimate realms of identity, and into the relationship between persons and the larger structures of states, economies, and—in the present case—systems for allowing, constraining and keeping track of human physical mobility.

Among other observers, sociologists and anthropologists have long viewed human identity as multiple and fluid. Individuals routinely act differently in different contexts, adopting different roles in different social settings. The ability to negotiate social contexts is essential to sociability and individuality (Goffman 1959). At the same time, cultural and social geographers have shown that in many cases the contexts within which identities are established are places and, to a large degree, human identity is tied to the places within which people work, shop, play, and carry on many other activities central to their lives (Duncan and Agnew 1990; Tuan 1982).

Moreover, students of bureaucratic and industrial processes have shown that knowledge of social and geographical identities has come to be seen as essential to the management of these institutions (Beniger 1986).

As a consequence, government and industry have become increasingly interested in the development of technological systems that will be able to organize, and make accessible in a geographically coded form, information about individual activities. If these information systems constitute an institution’s way of knowing individuals, their relationships, and their contexts, these organizations themselves inevitably develop within institutional milieus that favor particular ways of knowing and particular purposes for knowing.

Individuals and locations are understood, classified, and acted upon according to the needs and abilities of the designers and operators of the information systems.

The concept of personal identity is a problematic and theoretical focus in several of the social sciences as well as in philosophy. Checking identity is also an issue for states, governments and public policy. Is it worrisome and regrettable that the way in which "identity" features in discourse and practice differs so widely between these two domains, the academic and the practical? Moreover, the values, views, and goals which information systems facilitate may be very different from those of the subject population itself. Where theorists problematize identity, and often take the individual's perspective from the bottom up, practitioners seek to stabilize it through an administrative perspective in which identities are attributed, recorded and categorized in ways that are often independent of place, time and context. Once assigned to a category, it is difficult to transfer to another, or to invoke the situational subtleties that belie categorization (Bowker and Star 1999). With regard to movement, identity is never straightforward. Persons who seek to travel across national borders are normally required to reveal their identity and thus establish their right to travel from one country to the other. What are they required to reveal about themselves? Or, to put it another way, what can be said about the categories within which the person's identity is established? Are these definitions incontestable, and can they ever be definitive?

Information systems instantiate the values, epistemologies, and ontologies of their creators and impose them on their subjects (Agre 1994). Indeed, if these systems are often invisible to their subjects, they very often operate in terms of schemes of categorization that would be quite foreign to those subjects. Social identities "do not derive from the self-reflexive acts of individual egos, but from traces of behavior pertinent to the apparatuses of consumer and state surveillance" (Frohmann 1994: 9). Individuals may not even be aware of their inclusion in particular groups. Similarly, in geographic information technologies,
places are seen as locations to which individuals are only contingently attached... [T]he traditional practices of place formation and sources of attachment to place disappear... to be a part of a place is simply to maintain the right set of socioeconomic characteristics.

(Curry 1997: 682)

Thus the processes of ascribed identification, and the geographic information technologies that sustain them, implicitly challenge the possibility of consent, an important requisite of liberal societies and political systems. Yet users of GIS must come to terms with the requirements of data protection, including consent, if individuals can be identified in locational data. This is especially true where such data are matched in order to profile groups and individuals according to categories that are commercially or governmentally relevant. This reconciliation may be particularly problematic as data-protection laws, rulings and interpretations of the principles of fair information practice change in the direction of more stringent requirements or of broader coverage. Among the most salient conflicts that relate to GIS and other systems of data is that between the acknowledged usefulness of these databases and technologies in commerce, planning, policy-making and daily life, and the right or claim of individuals and groups to the protection of their privacy. These conflicts may turn upon questions of identity: users of categorization schemes “know” a person by these devices, yet the person “knows” who she is, and perhaps disputes the users’ “knowledge.” How can conflicts be resolved between “we tell you who you are” and “I tell you who I am”?

These scenarios and questions usually imply a context of stable social phenomena and more or less settled identities by which persons are known, but other contexts are of increasing importance. David Lyon argues that “[m]obility creates a world of nomads and unsettled social arrangements... it is not surprising that in transit areas, such as airports, surveillance practices are intense” (Lyon 2001: 19). He draws particular attention to one consequence of movement: because we are in very frequent contact with strangers, both parties require “tokens of trust,” such as identity documents and other stable proofs of who we are (Lyon 2001: 81–2). Of particular relevance to this chapter is that information about mobile persons is also collected and transmitted in situations where the need for fast, efficient implementation of certain functional requirements, such as road-toll payment, has stimulated the development of systems to replace cash with other transactional methods.

These are less dramatic circumstances than the scenarios of nomads, migrants, and unsettled social arrangements. For them, the rationale for surveillance and tracking is related to the maintenance of public order and perhaps also to sovereignty questions of policing national borders. Yet with toll payments, it is important for road operators to verify the vehicle’s payment by collecting and matching its classification and registration (license) number plate, in order to detect violations and fraud. These technological mechanisms thus record and allow the use of data capable of identifying individuals and tracking their movements. ITS technologies, however, can be applied not only to payment functions, but also to communications, traffic management, and navigation. Global positioning systems (GPS) provide the driver with the vehicle’s location, but may also allow a surveillant to track the vehicle’s movement. Sophisticated technological devices provide route guidance to drivers, as well as information about traffic and weather conditions, accidents and hazards, and the vehicle’s proximity to services and goods.

All these technologies, in principle, could allow anonymity by concealing the identity of the traveler. In practice, however, information can be processed in ways that violate the traveler’s reasonable expectation of privacy. As an attorney with the USA’s Federal Highway Administration observes: “While driving is a public behavior, the ability to compile information about an individual’s driving behavior, travel patterns, toll payments and other travel activity creates the potential for a database which has not previously existed in an easily accessible format” (Dingle 1995: 18–19). ITS systems therefore pose sharp challenges to regulatory regimes that are concerned to protect privacy, but they also provide possibilities for designing privacy protection into the technologies themselves (Agre 1995: 129–33; Alpert 1995: 115–16; Halpern 1995: 70–2).

With these theoretical issues in mind, we now turn to the comparative analysis of three contemporary road toll collection systems in Toronto, Ontario, Virginia and Southeast England.

The 407 Express Toll Route in Toronto

The 407 Express Toll Route (ETR) runs east–west just north of the city of Toronto, Ontario. It was begun in 1993 and since 2001, the extensions now stretch 108 km through one of Canada’s most densely populated urban environments and busiest transportation corridors. It has the most frequent interchanges (every 2.3 km) of any similar highway in existence. Around 97 percent of current users are from within the province of Ontario.

The original purpose was solely to relieve traffic congestion. The Ontario government developed the highway from the outset as an electronic toll route, however, to reduce the burden on taxpayers and to expedite construction. The government created a separate Crown Agency, the Ontario Transportation Capital Corporation (OTCC), to complete the highway by working in partnership with a variety of private sector corporations (407 ETR
2001). In 1999 all responsibility for the management of the highway and the collection of tolls was passed over to a private corporation, 407 International Inc., which is now the sole shareholder, operator, and manager of the highway (407 ETR 2001). The government still owns the land, leased to 407 ETR, and is involved in case of any wider land usage issues. The Ontario Ministry of Transportation also maintains an auditing role under the controlling legislation (the 1998 “407 Highway Traffic Act”), and the concession lease agreement.

The technology is innovative, and to date unprecedented. The ETR’s toll collection technology has five main components: the vehicle transponders (leased by the vehicle owner and portable between vehicles of the same class); the vehicle recognition and identification system; the roadside toll collection system; the toll transaction processor; and the revenue management system. The 407 ETR is currently the only multiple entry and exit automatic toll road in existence. Instead of tollbooths or plazas, 28 separate interchanges on the highway, each defined by an overhead tolling gantry, automatically record the beginning and end of the trip. The equipment logs the entrance and exit of the vehicle from the highway by reading the transponder attached to the inside of the front windshield. On exit, a green light on the transponder and four short beeps indicate the toll transaction has been successfully completed. Highway 407 users are billed once a month.

Transponders are mandatory for any heavy vehicle (over 5 tons) traveling the 407 under the Ontario Highway Traffic Act. There are both practical and economic reasons for this. The rear license plate of any training vehicle is not necessarily registered to the driver or owner of the truck itself, so the license plate would not necessarily match with the registered owner. Moreover, rear license plates are often obscured from video cameras on heavy vehicles. The OTCC also wanted to ensure a level playing field for all commercial vehicles, and did not want to put domestic industry at a competitive disadvantage with out-of-province or international vehicles. Owners of lighter vehicles who are frequent users of the highway are strongly encouraged, but not required, to register and lease a transponder from the 407 ETR Corporation. On registration, the vehicle owner is asked for basic contact details as well as the plate number, make, model and year of the vehicles registered to that owner. The applicant is then asked to select a payment option: pre-payment, post-payment, pre-authorized bank withdrawal, or charging to a credit card.

Owners of lighter vehicles may choose not to lease a transponder, in which case trips are logged by using a license plate recognition system. The system is located on each overhead gantry and sends up to five video images of the rear plate to a central processing computer, housed in the 407 Corporation, whenever such a vehicle enters and exits the highway. A $2 non-transponder charge per trip is added for this process. The central computer checks to determine if an account exists for that license plate. If not, an electronic search is made of the Ontario Ministry of Transportation’s License and Control Branch database for the name and address of that license plate holder. The number of account holders has increased since its inception, and the processing of non-transponder usage has declined.

The question of personal privacy was a priority from the time Project Request for Proposals for the 407 ETR was issued in September 1993. Since 1994, the Office of the Information and Privacy Commissioner (OIPC) has been actively involved in discussions with the Ontario Transportation Capital Commission (OTCC) about how individuals could travel along the 407 ETR and still maintain their privacy. If residents of Toronto were to use this new system, it was necessary to gain their trust by building in strong safeguards against the inappropriate collection, use and disclosure of personal information. The OTCC worked closely, therefore, with the OIPC to ensure that the toll and billing system did not compromise personal privacy.

They claim that the result is the first Intelligent Transportation System in the world to allow users to travel the road anonymously. This is accomplished through three features. First, the plate recognition system (for vehicles without transponders) only records the rear license plate of the vehicle; the OTCC agreed that it was not necessary to collect any more information for toll collection purposes. Thus, like “photo radar” programs developed in other parts of Canada to catch speeding drivers, the cameras have a fixed geometry and do not take images of the interior or the front of the vehicle.

Second, the governing legislation only permits the ETR corporation to use any personal information it collects for toll collection, traffic management and for its own marketing purposes. The 1998 407 Highway Act stipulates that personal information may only be collected

1. To assist the owner in the collection and enforcement of tolls, fees and other charges owing with respect to Highway 407.
2. To assist the owner in traffic planning and revenue management with respect to Highway 407.
3. To assist the owner in communicating with users of Highway 407 for the purpose of promoting the use of Highway 407.
4. To assist an entity with whom the owner or the Ministry of Transportation has an agreement relating to the collection and enforcement of tolls (407 Highway Act 1998: c.28 s.54(5)).

In addition, tight contractual clauses between the Ministry of Transportation and 407 International Inc. ensure that the confidentiality of personal information is protected and that it is not used for any purpose not referred to in the legislation.
Finally, potential travelers have the option of obtaining a transponder and travelling the 407 without providing any personal information. The user can effectively open a pre-paid cash account at which point he or she receives a transponder and a booklet of payment slips pre-printed with the anonymous account number. The user is reminded to replenish the account when the transponder flashes yellow, rather than green, as the car travels under one of the 407 gantries. The user simply visits any chartered bank to deposit funds into the account number that appears on the payment slip. These funds are then electronically transferred into the user’s 407 account. Of course, if users wish to remain anonymous, they cannot allow their balances to fall below zero. If they do so, the rear license plate identification and the recognition system will be activated (Information and Privacy Commissioner, Ontario 1998). To date, very few individuals have taken advantage of this anonymous option. Nor is this option encouraged, as it significantly increases the processing costs for the corporation.

These relatively tight controls mean that, with few exceptions, the information gathered on the 407 ETR is only used for toll collection purposes. Aggregate data on patterns of overall traffic flows are reported to the government, as are accidents. Law enforcement agencies, however, cannot obtain personal information from the 407 corporation on, for instance, stolen vehicles, unless under warrant. No information is transferred to the police on more minor traffic infractions such as speeding. At first glance, the 407 seems to have been designed, developed and implemented with extensive safeguards against the inappropriate use of information about vehicle movement. The system does constitute a tracking technology, but it is one that has been clearly designed to prevent widespread secondary uses of personal data.

The 407 ETR system, while touted as “state-of-the-art” is, however, expensive to operate and use and not suitable for wider traffic management purposes. The Ontario government has installed a new system (COMPASS) on other Toronto freeways to respond to traffic congestion problems caused by accident, breakdown or peak rush hour use. This system collects no personally identifiable information but can warn motorists of incidents and delays. The system is fully integrated with emergency response procedures.

It is apparent, however, that these contemporary intelligent transportation systems may eventually be overtaken by cellular and GIS technologies. Currently, 28 percent of vehicles traveling on Canadian roads contain cellular devices. Private sector providers may soon have the ability and incentive to collect that tracking information which might then be purchased by government for traffic management purposes. The amount and specificity of the traveler information that might be available is then enhanced. Drivers may get real-time information on congestion, emergency services and routing (i.e., the best way to get from A to B on this particular evening when there is a ball game and bus strike). The collection and processing of this kind of information may also obviate the need for automatic toll collection systems such as the 407 ETR, and instead will reduce the need for jurisdictions like Ontario to build traffic loops, on-ramps and install video cameras. The smart vehicle of the future will record location information, and cellular operators will collect it for governmental use. The efficiencies of on-board cellular and GIS tracking technologies for a range of public and private purposes will likely present far greater challenges to individual privacy than the relatively discrete and manageable highway system on Toronto’s route 407.

The Smart Tag System in Virginia

Smart Tag is an electronic toll collection (ETC) system used at five locations in the State of Virginia: the Dulles Toll Road in northern Virginia; the Dulles Greenway in northern Virginia; the George P. Coleman Bridge on the eastern shore of the middle peninsula; the Powhite Parkway Extension in the Richmond area; and the Expressway System in Richmond. The Smart Tag system has been phased in at these locations beginning with the Dulles Toll Road in April 1996; the Dulles Greenway in May 1996; the Coleman Bridge in August 1996; the Powhite Parkway Extension in July 1999; and the Richmond Expressway System in July and August 1999.

As of the summer of 2000, there were more than 257,000 Smart Tags in use: 175,000 in northern Virginia, 32,000 on the Coleman Bridge, and 50,000 in Richmond (Smart Tag Statistics 2001). In each location, usage of the Smart Tag system exceeds original expectations. On the Dulles Toll Road, over 60 percent of cars use Smart Tag during rush hour with about 40 percent usage overall. On the Dulles Greenway, about 80 percent of the cars use Smart Tag during rush hour with over 50 percent usage overall. The Coleman Bridge reports the highest usage with 90 percent of cars using Smart Tag during rush hour and about 80 percent usage overall. The newer Smart Tag systems in the Richmond area were heavily subscribed from their inception and have about a 50 percent rush hour usage.

The Dulles Toll Road system was initiated in March 1994 when a contract was awarded to Castle Rock for installation of an ETC system called FASTOLL. The genesis for the system was the Virginia Department of Transportation’s (VDOT) March 1993 strategic plan (Smith 1993) for Virginia called PROGRESS, VDOT’s Intelligent Vehicle-Highway Systems (IVHS) Program for an Efficient and Safe System. Beginning in 1991, the federal government also encouraged the implementation of ETC systems such as Smart Tag through the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA) program. ISTEA provided federal funding and
incentives for automatic toll facilities in order to reduce congestion at toll plazas. As in Toronto, VDOT recognized the potential of IVHS to increase the efficiency and lower the expense of surface transportation. But it was equally impressed with the potential of IVHS to enhance economic growth through development of an IVHS industry, which might benefit high technology firms in Virginia. The plan spoke enthusiastically of new potential for innovative public–private partnerships. Although the FASTOLL system was originally to be completed during 1995, it did not become fully operational until April 1996. In January 1998, VDOT changed the name to Smart Tag as part of its overall Smart Travel system.

The Smart Tag system, like most ETC systems, uses several key components (Electronic Toll Collection 1998). Automatic Vehicle Identification (AVI) uses a radio frequency device located in a transponder, which is designed to link the account on the transponder to the toll equipment. As in the Toronto system, the Smart Tag transponder is read electronically, and the toll is deducted from a pre-paid Smart Tag account. The Smart Tag transponder can be used at any Smart Tag collection plaza in the state. A Video Enforcement System (VES) can capture the license plates of vehicles that do not have a valid transponder or sufficient funds. On the Coleman Bridge, motorists who get a “blue light” when driving through the Smart Tag Only lanes have their license plates recorded and retained, and toll violations can be issued to those motorists. Video enforcement for toll collection for the Dulles Toll Road is not yet in operation but is an enhancement project that was proposed in the 1999–2000 Six Year Plan.

Any ETC usually requires a communications and database system. A lane controller receives input from the AVI, VES and AVC (Automatic Vehicle Classification) equipment and records the customer’s toll. All Smart Tag systems in Virginia use a compatible ETC system (Mark IV reader). There may also be a toll plaza computer, which consolidates data and checks the validity of toll tags. A Customer Service Center receives toll transactions and posts these transactions against the customer account, as well as storing data on valid accounts. VDOT owns and operates a Customer Service Center with two satellite locations; this one center manages all Smart Tag accounts throughout Virginia.

The current marketing literature and the 1993 strategic plan promote six fairly typical advantages of Smart Tag. First mentioned are efficiencies in terms of traffic flow. VDOT currently reports that on the Dulles Toll Road, lanes with attendants collecting tolls process 525 vehicles per hour; exact change lanes process 650 vehicles per hour; and Smart Tag Only lanes process 1,400 vehicles per hour. A second benefit is that there is less need for capital construction to widen or reconfigure toll plazas to accommodate increased traffic volume. Indeed, some ETC systems eliminate toll plazas altogether or streamline them to require little capital construction. A third advantage is that ETC systems are seen as being environmentally friendly because cars release fewer pollutants as they idle for less time at toll plazas. A fourth benefit involves freeing personnel from the monotonous and hazardous job of collecting tolls. Fifth, ETC systems provide a more accurate and comprehensive accounting system. Finally, ETC systems can encourage travel at off-peak times by reducing tolls. New federal legislation, the Transportation Equity Act for the 21st Century (TEA-21), promotes more sophisticated uses of ETC systems, promoting, for example, variable pricing in order to reduce peak hour traffic volumes.

In addition to marketing these advantages, the state has endorsed the use of several incentives to encourage drivers to adopt Smart Tag. Smart Tag users receive a 10 percent discount at toll collection sites on the Richmond Metropolitan Authority Expressway System. In August 1999, the Dulles Greenway announced a toll increase of 25 cents, to $1.75, for those who are not using Smart Tag. The rationale for the increase was to help ease traffic backups at toll plazas (Blum and Hedgpeth 1999). When the Dulles Toll Road opened HOV-2 lanes, it designed them so they fed directly into the Smart Tag Only lanes at the toll plaza.

Privacy concerns are not visibly addressed or acknowledged in the Smart Tag literature. The twenty-item customer agreement for Smart Tag does not mention information collection, disclosure or use practices. In the Smart Tag brochures, two items have privacy implications but are not presented as privacy issues. The brochure mentions that if people want to pay cash instead of using their Smart Tag, they should remove the Smart Tag from the vehicle or wrap it in aluminum foil. Smart Tag developers recognize that drivers may want to be anonymous on some trips, but they do so by implication only, and not by addressing the privacy concern directly. Second, the brochure states that receipts are not provided when someone uses a Smart Tag, but a customer can obtain a detailed statement from the service center “starting at $2.00 a month.” By implication, the brochure acknowledges that records containing date, time and location for Smart Tag uses are compiled and retained, but implies that Smart Tag owns this information and customers must pay for access. The question of who other than the customer might have access either by court order or request is left undefined.

The Smart Tag Application Form states: “All information is personal and confidential,” but there is no indication of how a customer can verify that statement. The personal information supplied on the application form is technically information supplied to the state for an administrative purpose. Because of concerns about requests for access to that information, personal information related to toll facilities, particularly ETC information, is exempt from the state’s Freedom of Information Act. Custodial control for the
information is assigned to VDOT and could be released in response to a subpoena. According to Smart Tag personnel, information is not released for marketing or other purposes. This is not spelled out on the application form or customer agreement in part because of the difficulty of drafting language that takes into account all contingencies; the statement quoted above, that "all information is personal and confidential" is regarded as the overarching policy.\textsuperscript{10}

This statement is very similar to that made by the Massachusetts Turnpike Authority's Fast Lane which says the Turnpike "shall hold all customer account information confidential." When asked about the possibility that law enforcement authorities would subpoena this information, a Turnpike Authority responded that they would resist releasing information but that they thought such demands unlikely (Kerber 2001). The E-ZPass toll system in New York, however, has complied with such demands. In one case, E-ZPass locating records allowed authorities to find the body of a kidnapping victim by using E-ZPass records to track where and when his car had traveled (Sipress 2000). New case law in Massachusetts, New Jersey, and New York requires law enforcement officials to demonstrate that they are investigating a serious crime to obtain toll records. Bills have also been introduced in state legislatures to protect the privacy of toll records and to specify the conditions under which they could be released for law enforcement purposes (Most 1998).

The Smart Tag brochure indicates that Smart Tag transponders can be used by other vehicles with the same number of axles. From a privacy standpoint, this means that the transponder may not be recording the movements of the individual account holder. The account holder could authorize its use for a child or friend. In such a case, the account holder may want to know when and where the transponder was used. This feature of the transponder also makes it a target for stealing. If it is stolen, the account holder, Smart Tag officials and the police may all have an interest in accessing the records.

Another privacy implication of the Smart Tag system is that it is designed to encourage customers to use a credit card. If travelers do not use a credit card and automatic replenishment on the Smart Tag account, they must pay a $15 refundable security deposit. The automatic replenishment system is the easiest and least expensive method, but it does entail an authorization to allow Smart Tag to charge a credit card account. It also means that some information about road travel may become incorporated into one's credit history and could be used for profiling purposes. Smart Tag offers alternatives to automatic credit card replenishment. Customers can add money to the account by mailing a check, visiting customer service, or calling in a credit card authorization.

The institutional and management arrangements for Smart Tag are particularly interesting in three respects: within the Smart Tag system itself; between Smart Tag and the I-95 Corridor system in which use of E-ZPass is dominant; and between Smart Tag and the larger Smart Travel system in Virginia.

Although all the Smart Tag road systems are located in Virginia, the organization and management of each road system involve different configurations of government and private involvement. For example, the Dulles Greenway is privately owned. The Dulles Toll Road is owned and operated by VDOT. The Richmond Metropolitan Authority (RMA) owns and operates the Expressway System, including the Powhite Parkway, Downtown Expressway, and Boulevard Bridge. Each of these road management authorities contracted with a private sector partner to build the Smart Tag system. MFS Transportation Systems, a subsidiary of MFS Network Technologies, built the RMA Smart Tag system. The project covers fifty-five lanes of the system and includes toll plaza infrastructure modifications, upgrades to computer and communication systems, replacement of audit systems, integration with current customer service centers, and a five-year maintenance contract (ITS America 1998).\textsuperscript{11} Castle Rock Consultants advised on the design and implementation of the FASTOLL/Smart Tag system on the Dulles Toll Road.

Despite the fact that the road systems are managed differently and that the Smart Tag systems have been built by different contractors, the technical configuration of each of the Smart Tag systems is compatible. Most importantly, the actual operation and management of Smart Tag is organizationally separate from road management. The real operation of Smart Tag occurs in the Smart Tag Customer Service Center, which is owned by VDOT. VDOT then contracts for its services. This Center serves as the financial and administrative clearinghouse. All five Smart Tag systems in Virginia feed their ETC transaction and customer accounts through this one central office.

The pivotal position played by the financial management center explains, in part, the relationship that the Virginia Smart Tag has with other ETC systems on the East Coast. The Regional Consortium, comprised of five transportation agencies representing Delaware, New Jersey and New York, manages the E-ZPass system. These Consortium Member agencies are part of a larger E-ZPass Interagency Group (IAG), an association of sixteen northern toll agencies spanning seven states (E-ZPass Network 1999). The IAG allows travelers with E-ZPass transponders to use them on member toll roads in New York, New Jersey, Delaware, Pennsylvania, Maryland, Massachusetts, and shortly West Virginia (ITS America 1999). One of the components of the Northern Virginia District's Smart Travel vision is that
“VDOT will implement a toll tag that will be usable throughout Virginia and the member states of the I-95 Corridor Coalition. Similarly, electronic toll tags used by the I-95 Corridor Coalition states will be usable throughout Virginia” (Tang 1999a: 13).

At this time, the Smart Tag system is technically compatible with the E-ZPass system. Smart Tag readers can read information from E-ZPass transponders and vice versa. But the Smart Tag and E-ZPass financial clearinghouse systems are not compatible, and transactions cannot be made between the two systems. Although the readers can get information from the transponders, they cannot interact with the transponder. This is not a technological problem, but an institutional one. The VDOT, as well as Smart Tag and E-ZPass users who travel in both systems, want compatibility between the systems. An additional factor that may hasten compatibility is that TEA-21 includes a requirement that agencies demonstrate “consistency” with the National ITS Architecture to be eligible for federal ITS funds.

The third institutional and management arrangement is between Smart Tag and Smart Travel. As noted above, the name Smart Tag replaced FASTOLL in 1998 to symbolize the unity of all ITS applications under one umbrella concept (Tang 1999b: 1–4). The plan is to develop interrelated systems so that, for example, surface street management, freeway management, incident management, traveler information, customer service, and payment systems can work together. The vision entails a statewide network of Smart Travel centers that will provide the intelligence for the system.

The Dartford River Crossing in England

As a brief comparative illustration of an existing electronic toll-payment system in Europe, we look at the Dartford River Crossing of the Thames in southeast England, near London. The new privately financed Queen Elizabeth II Bridge opened in 1991 as part of the densely traveled M25 motorway around London, which already included the Dartford Tunnel. Tolls are meant to recover construction costs, and the physical infrastructure for collecting them from the estimated forty million vehicles using the crossing each year includes a new £2.5 million system, DART-Tag, described as “Europe’s most advanced toll system” (HHS Online 1999; Flowchart 2001). The tag—a microwave transponder, is free. Drivers pay in advance by setting up a direct debit facility in the bank. Some lanes are reserved for the use of DART-Tag users.

When a vehicle approaches, the tag is interrogated by an antenna to obtain a customer number and retrieve a customer record. If the driver’s account is in credit, the barrier automatically opens. Traffic lights at the barrier tell the driver roughly how many credits are left, and a red light means the account is empty in which case the barrier will not open. Passing through the open barrier updates the driver’s account record. Drivers receive a monthly statement itemizing the entries. As in the Smart Tag and 407 ETR cases, there is a price incentive to obtain the tag, in this case a 7.5 percent discount. An estimated 20 percent of vehicles using the crossing are subscribers. Travelers have the option of throwing coins into a basket or going through a staffed booth if they require change. A central computer keeps a count of every vehicle using these services, presumably to compile simple tallies for financial management purposes.

Whereas Smart Tag’s Customer Agreement is vague about information practices, the Dartford River Crossing company’s terms of conditions and use contains a privacy policy statement. It describes the information required when an account is set up, why it is necessary, how it will be used (including use in an aggregated form for flow-monitoring purposes), and how the user can opt out of third-party use. It explains that the web site used for transactions contains security software (certification system provided by BT Trustwise in connection with Verisign) including encryption for all communications with customers and banks, firewalls, and secure premises. Information is kept confidential, with internal company procedures to guard against unauthorized disclosure. If the privacy policy changes, customers will be informed on the web page and consent will be sought for any substantive changes of use of information. Subscribers automatically consent to the passage of their information outside the European Economic Area during use (Dartford River Crossing Limited 1999).

Concluding observations

It is apparent that each of these three systems is both a reflection and a precursor of future ITS. At a policy level, these cases offer some insights into the evolving nature of the privacy issue and how it might best be addressed in the context of current and future ITS applications. Four conclusions are relevant about the protection of privacy.

The first lesson concerns the business case for these systems. Often the logic of these systems is framed in terms of speeding the flow of traffic. Efficiency, therefore, is the goal, and the architecture is crafted in terms of relating intelligence directly to traffic management. Moreover, the economics of these systems, based on complex public–private partnerships, favors more extensive and intensive uses and sharing of personal data. The logic then favors surveillance. In order for privacy to be taken into account, it has to be addressed in the development of that architecture, but those involved in the process are transportation specialists and contractors. There are few natural
entry points for the privacy interest even in the presence of an overriding legal privacy framework.

The second lesson relates to the importance of technical standards and how the standard-setting process can institute protocols that embody privacy protective or invasive measures. European developments are instructive. As a result of the need to promote the free flow of goods and services throughout the EU, there has been considerable standards activity in Europe concerning transport telematics applications, including ETC (sometimes known as electronic fee collection – EFC). The European Commission has played a large part in coordinating and supporting research and development, and in addressing major issues, of which the interoperability of these systems has been perhaps the largest. The Fourth Framework Programme is an example of this effort. Interoperability exists within, but not across, countries with EFC systems. The international and European standards organizations (ISO and CEN) have also been closely involved in these developments. While current standards do not ensure interoperability of payments, work was proceeding in that direction, for instance within CEN TC278, and through an agreed Applications Interface Definition for an EFC based on Dedicated Short-Range Communication (DSRC). Technical standards decisions about the various elements of toll collection systems can have profound policy consequences for the collection of personal information.

It is too soon to say whether systems in European countries or any future common system will make extensive use of advanced GIS, including geopositioning through satellite communication. Countries that have invested in particular toll collection infrastructures and technologies may be more reluctant to move towards a new system. These fixtures include toll plazas, payment lanes, roadside or overhead equipment, etc., as well as personnel. The calculation of tolls by means of distance traveled, involving “virtual” toll collection points rather than a system of lanes, overhead gantries, and the like, would involve the collection of such data through these technologies. That, in turn, depends on the standardization work that might be undertaken by a working group in CEN TC278.

By contrast, there has been less need for standards-setting activity in Canada and the United States. Indeed the incremental, state-by-state use of E-ZPass on the I-95 corridor would indicate that interoperability in US systems is not an initial goal but became a later addition to the policy agenda when significant incompatibilities arose. Toll systems in North America tend to develop locally to meet local traffic management needs by state and provincial departments of transportation and local/regional transportation authorities.

Thirdly, we would stress the importance of an overriding legal framework for the collection and use of tracking information. Such frameworks exist in Canada, the United Kingdom and in the rest of Europe. In Canada, specific data protection provisions were introduced into the enabling highway legislation for the 407 ETR. In the UK, the collection of personal information for toll collection purposes is regulated under the aegis of the Data Protection Act 1998 and the Information Commissioner, though to date there have been few if any policy pronouncements or regulatory actions by the Commissioner on this issue. In the Netherlands, the Registratiekamer (the Dutch Data Protection Authority) has been involved in considering the privacy implications of road-tolling proposals for managing intra-urban traffic congestion. A related point, then, is the active involvement of a privacy watchdog office at the outset of system development. The significance of privacy in the context of the development of the 407 ETR is explained to a large extent by the early involvement of the Office of the Ontario Information and Privacy Commissioner, and to the very public way in which that office raised privacy concerns.

In the US, there is no overriding legal framework, perhaps accounting for the less stringent controls over possible secondary uses of electronic toll information, and for the less prominent mention of privacy in the materials provided by the Smart Tag system. Most states have laws addressing the privacy and confidentiality of state records but these, of course, are not tied explicitly to information related to ETC. ITS America, an advisory committee of the US Department of Transportation, has, after a lengthy period of consultation with stakeholders, finalized a set of Fair Information Principles for personal information related to ITS. But these are voluntary guidelines and have no binding force (Voccola 2001: 4).

The fourth lesson is that complex technologies do not necessarily require complex privacy-enhancing solutions. No doubt, a range of encryption solutions can be advanced to protect the integrity of the tracking information generated within toll collection systems. It is instructive, however, that the solution adopted in Toronto’s 407 involved no major changes to the existing infrastructure of collection. It merely allowed a payment and accounting process that did not require the submission of personal identifiers. The fact that very few individuals have so far taken advantage of this system suggests, however, that the administrative burden is not something that most users of the highway would tolerate in order to protect the privacy of their movements. Similarly, in the Smart Tag system, the cash payment option is inconvenient compared to the credit card payment process.

In the Dartford River Crossing and the Smart Tag System in Virginia, where there are controlled points of entry and exit, privacy can still be maintained through the anonymity of cash payment at a traditional toll plaza. Thus far, therefore, any privacy pressures have been translated into privacy solutions by the retention of traditional payment devices, although the more
convenient way to use both systems is to supply valid credit card information and thus surrender a measure of privacy. There are legal and political pressures to retain this sort of facility, but with the application of advanced ITS technologies, perhaps especially on multi-lane roads where the channeling and slowing of traffic for toll payment is to be avoided, traditional processes may be highly vulnerable.

We now return to the more general questions and issues raised at the outset of this chapter. The implications of ITS for these matters of identity, surveillance, and the categorical sorting of persons and groups are not yet particularly evident in the toll-road applications we have studied so far. From the analysis of these systems, it is apparent that the range of personal data collection is still quite limited to essential payment-related information. Systems vary in terms of their transparency and general concern for privacy-related questions. But the overall picture is one in which the payment collection technologies are usually confined to the simple purpose of making sure that the right people are charged the right amount for the journeys they have completed. The most obvious sorting in toll collection systems is among those using electronic tolls, those using exact change and/or tokens, and those needing change. The electronic toll systems represent the most expeditious way of negotiating the toll plaza but in most instances involve some divinement of personal information and use of a credit card to open and upicate an account.

The matching and sharing of personal data obviously vary according to the number of organizations within the contractual arrangements surrounding these systems, and also according to the number of jurisdictions from which travelers might originate. Thus far, the opportunities for policy intervention to protect values such as privacy are present, though variable, because of the relatively discrete and bounded character of the data processes involved. The latter's significance for politics and policy has been relatively modest to date; ITS has not been an important site for the kinds of overt or covert conflict between institutions and individuals, the watchers and the watched, that are projected in many scenarios concerning technology and human movement.

However, it is also apparent that each of these systems is under pressure for the secondary uses of the data collected. So far, these pressures have tended to originate from public sector agencies and been motivated by various traffic management and law enforcement interests. Aggregate data collected through these systems might be useful in managing traffic flows, physical and environmental maintenance, and in reducing congestion. Individual-level data might also be valuable in tracing stolen vehicles, enforcing customs rules, catching speeding and dangerous drivers, and apprehending criminals. But wider commercial pressures for the use of these data to profile, for example, the kinds of people who drive particular vehicles along specific routes at specific times, have not yet been significant or have been resisted by policy intervention.

This preliminary research, however, has also revealed that these systems are rapidly being overtaken by more advanced technologies that will enable a more intensive and extensive surveillance of vehicle movement, and thus may broach the larger social, political and privacy questions. For example, the European Commission listed thirty-five telematics applications projects for transport in 1997–98 (European Commission 1999). These covered a variety of land, water and air transport applications, of which only a small number concerned tolling and related road applications of ITS. Some applications are of particular interest. VERA (Video Enforcement for Road Authorities, using video records as evidence to prosecute road traffic offenders throughout Europe) has a law-enforcement purpose, including harmonized approaches to enforcing traffic laws by employing video and digital imaging technologies. The objective of SANSICOM (High-Technology GNSS Satellite Navigation System with Integrated Communication Link for Road Applications) is to integrate a communication link for various road applications into a satellite navigation system with a communication capability. This will be used to monitor road situations, including in-vehicle systems for safety. Applications will relate to fleet management for road haulers, container and car tracking, stolen vehicle recovery, search and rescue operations, and road traffic control. In the US, the 1991 ISTEA encouraged the development of what was first termed Intelligent Vehicle-Highway Systems (IVHS) and then extended to Intelligent Transportation Systems (ITS). In 1995, the Department of Transportation spoke of bundling these systems into six groups: travel and transportation management; travel demand management; public transportation operations; electronic payment; commercial vehicle operations; emergency management; and advanced vehicle control and safety systems.

New projects continue to be developed in these areas and many reflect new technological advancements in GPS and wireless systems. Development of these systems is accelerated by federal funding and policy, most recently by TEA-21, as well as by states and private communications and transportation vendors (US Department of Transportation 1995).

The incentive to suppliers as well as to road users, of the added functionality that advanced GIS tracking technologies may make possible - targeted information about weather, goods, services, etc. - will obviously raise additional privacy issues. These may well bring into play a more intensive development of sorting and classification systems in order to tailor messages and services to the known, or presumed, characteristics and preferences of drivers. With existing systems, toll payments may be based on the
measurement of the physical dimensions of the vehicle as it traverses the payment point, with the dimensions related to classification systems of vehicle types with associated levels of charges. But they may also be based upon license plate number capture, or through information transmitted from the vehicle’s on-board unit. So far, the main interest of the ITS community in classification has been in terms of vehicle types.

However, quite a lot can be known, or at least inferred, about vehicle owners and drivers. Data reveals who drives what vehicle, where and when, and allows analysis of the previous travel behavior of individual road users; those data can also be linked to other sources of information for profiling purposes. Commercial pressures to use tracking information have so far been limited, but we can foresee them intensifying as the convergence of on-board telematics and GIS technologies increasingly become adopted for toll collection and traffic management functions. That convergence will also continue the erosion of the distinction between the public and the private realms, and between the individual and the vehicle, as commerce extends the assumption that “we are what we drive.”

Notes

1 These technologies and user services and their implications for various privacy interests, based upon the US Department of Transportation’s Program Plan, are discussed in Alpert (1995) and Glancy (1995).

2 This chapter is part of a larger project, funded by the National Science Foundation in the USA (Grant No. SES-0083277), which attempts to gain an analytical understanding of the implementation of personal identification in geographically coded information systems, and an appreciation of the effect that identification practices have on individual privacy, sociability, trust, and risk. This will involve, in part, locating and clarifying contradictions and ambiguities in common notions of identification and privacy, conceptually systematizing practices of identification, and theorizing the effects of these practices on social equity amongst individuals and on the individual’s relation to political and economic communities. The research project analyses particular types of geographic information systems, and performs a series of comparative case studies – in the USA, Canada, and Europe – of the processes by which identification practice is incorporated into these systems. A companion paper in this volume by our project colleagues, David Phillips and Michael Curry, reports initial findings concerning another field of application, geodemographic systems.

3 Discussion of a wider range of technological applications for location and tracking, including systems that are not necessarily related to movement, can be found in Clarke (2000).

4 For seminal explorations of surveillance, see Lyon (1994, 2001).

5 The authors are grateful to Peter Walker for his research assistance on this section of the chapter.

6 Interviews with staff at the Ontario Ministry of Transportation, 2 March 2001.

7 Interviews with staff at the 407 Corporation, 2 May 2001.

8 Interviews with staff at the Ontario Ministry of Transportation, 2 March 2001.

9 We acknowledge the research assistance of Brendan Crowley for this section of the paper.

10 Interviews with staff at the Virginia Department of Transportation, 12 April 2001.

11 MFS Transportation Systems has implemented a number of other ETC projects including the Denver E-470, the California 91 Express Lanes, and the Regional Consortium for Toll Collection (NJ, NY, and DE) as well as projects in South America, Canada, Europe and the Pacific Rim.

12 Interviews with staff at the Virginia Department of Transportation, 12 April 2001.

13 In mid-1999, there were at least 17,000 km of tolled motorway in Europe, operating in nine European Union (EU) and other countries, and including Electronic Fee Collection (EFC) in France, Italy, Spain, and Norway. Some two million EFC subscribers were involved; this accounted for about 10 percent of toll transactions in places where EFC was available. The French system is TIS, the Italian is TELEPASS, the Norwegian is the 5.8 GHz system, and the Portuguese is Via Verde. New EFC systems were being planned for introduction in several other countries: the Netherlands, the Nordic countries, Germany, Switzerland, and the UK. Different national requirements meant that these were designed in a non-interoperable manner, and influential opinion did not consider it feasible or desirable to harmonize the existing systems. Yet it was thought possible to work towards a migration of the different EFC systems, in stages, to a common system through the enlargement of the diverse national ones. See EC – DG XIII, Telematics Application Programme, Transport Sector, CARDME-3 (Project TR 4102), Deliverable 5.1: Review of Current Possibilities for Migration of EFC Systems (Doc. D5.1, Version V2.01, Draft), 1 June 1999.

14 See also www.itas.org. Regulations are noticeably absent in the United States, perhaps accounting for the less stringent controls over secondary uses on the Dulles toll road, and for the less prominent mention of privacy in the materials concerning the Smart Tag system.

15 Among these projects are ADVANCE (Advanced Vehicle Classification and Enforcement Systems, involving electronic fee collection on toll motorways), CARDME-3 (Concerted Action for Research on Demand Management in Europe, on convergence of motorway tolling systems throughout Europe), and INITIATIVE (Industry Initiative To Introduce Automatic Tolling In Vehicles in Europe, concerning a search for the optimal electronic fee collection system on toll motorways). These are important overlaps and collaboration among several of these, including a network of technical personnel from public and private organizations. A further grouping is the Nordic countries’ MÄNS (Objective-oriented Nordic Co-operation on Interoperable Payment for Transport Services).

Bibliography


407 Highway Act 1998, c. 28, s. 54 (5). Province of Ontario, Canada.


Tang, A. (1999a) *Strategic Plan: Northern Virginia District (NOVA) Smart Travel Program.*

— (1999b) *Executive Summary: Northern Virginia District (NOVA) Smart Travel Program.*


