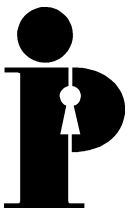
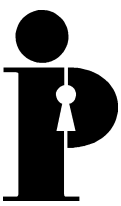
Information
and Privacy
Commissioner/
Ontario

Eyes on the Road: Intelligent Transportation Systems and Your Privacy



Tom Wright
Commissioner
March 1995



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Table of Contents

Introduction

Imagine your car being able to tell you, based on your present location, what the fastest, most congestion-free route to your destination is, or where the nearest parking space is. How about sitting back while your car drives itself?

Now imagine that at the same time, your every move on the highway is being monitored, or that personal information is being collected from you at various points along the highway (e.g., where your car was on Tuesday at 2:43 p.m., when you paid that road toll). Imagine this information being disclosed and used in ways unknown to you.

This vignette provides a glimpse into just a few of the possible benefits and privacy implications of a group of traffic technology applications known collectively as "Intelligent Transportation Systems" (ITS).[1]

The goals of the Information and Privacy Commissioner/Ontario (IPC) in producing this paper are to create greater public awareness of ITS and its privacy implications, and to stimulate public discussion. The IPC is looking to both public and private sector organizations involved in the development and implementation of ITS to educate and discuss the issues with the public to ensure that individual rights to privacy are maintained.

This paper briefly describes ITS and discusses the key privacy issues associated with it. The paper also reviews ITS applications and their status in Canada and internationally.

What is ITS?

ITS refers to a wide variety of advanced and emerging technology applications designed mainly to reduce traffic congestion and emissions, and to improve highway efficiency, safety, and convenience. It should be noted, however, that these benefits are disputed and have not been clearly supported by research.[2]

ITS may be applied to or involve:

- all types of vehicles, including private cars, taxis, trucks, buses, and trains;
- all aspects of the surface transportation system, including urban and rural roads, freeways, transit stations, and ports;
- a variety of information devices, such as computers, signs, dash-board monitors, hand-held equipment, and kiosks.[3]

Although most ITS applications are still in the developmental and testing stages, there are a few which some of us have already encountered. These include anti-lock brakes, electronic road tolls, and variable message signs (electronic message boards located over the highway that alert drivers to road or weather conditions ahead).

ITS and your privacy

Many ITS applications/technologies have little if any impact on privacy — primarily because they do not identify you or your vehicle. Technologies that generate data about drivers or their vehicles can have a direct impact on your privacy.

This paper focuses on some of the privacy-related concerns that have been identified in relation to ITS. Generally, these concerns fall into two broad categories: personal privacy and informational privacy. We will begin by exploring the areas where personal privacy may be compromised as a result of ITS technologies.

Personal privacy

In the context of this paper the term "personal privacy" implies that individuals are entitled to freedom of movement and expression, freedom from harassment and indignities, and freedom from invasions of their personal space. This section examines issues concerning the surveillance of travellers and the impact on privacy as it relates to individual autonomy under ITS.

Surveillance

Perhaps the greatest threat to privacy posed by ITS lies in its ability to conduct unwarranted and unwelcome surveillance on specific individuals. ITS can track and monitor a person's movements, transactions, and communications — and do so without his or her knowledge.

This may be achieved through the video camera monitoring of vehicles, satellite-based global positioning systems, Automated Vehicle Identification (AVI)[4], or other means. Combined with mapping and other technologies that can be used for surveillance, AVI could make it possible to display the exact position of a particular vehicle at a particular time.[5]

In the area of Commercial Vehicle Operations (CVO), certain technologies enable constant monitoring of the weight, speed, and emissions of commercial transporters. But these same technologies also make it possible for employers to find and track drivers and their vehicles, at all times. Some labour unions in the North American transport-trucking industry are already grappling with this form of employee surveillance.

Besides having the ability to identify individual travellers, ITS can also collect and store a lot of sensitive information about you. It can, for example, be used over time to create individual travel profiles indicating, among other things:

- your driving habits and any traffic violations committed;
- where and how you like to travel;
- where you live and when you are home;
- where and when you go to work;
- where and when you shop;
- where you go for recreation (bars? casinos?);
- what place of worship you attend and how often;
- what community groups you associate with;
- where your children go to school;
- where your friends live;
- what political protests or rallies you may have attended;
- whether you have been to a doctor (or abortion clinic, or AIDS clinic…).[6]

These profiles can, in turn, be matched with other personal information, such as insurance, credit, buying habits, income, bankruptcies and liens, age, marital status, health data, and so forth. On a large scale, all of this could be arrayed geographically, resulting in amazingly detailed personal profiles on potentially millions of people.

Such a personal profile could be used to make decisions about you, as well as to predict and manipulate your future choices. It could be used as a substitute for dealing with you personally. It has even been suggested that this ability

> to assemble information selectively, or to correlate existing information [is a] capacity, obviously facilitated by information technology, [which] enables (government) agencies (and other organizations) to identify, target, and perhaps manipulate a certain segment of the population that has common … characteristics.[7]

Privacy and personal autonomy

ITS can have serious consequences for individual autonomy and personal choice. At the most basic level, there is concern that you will not be given a genuine choice about your participation in ITS. Or, if given a choice, you might not be allowed much control over your individual use of the system. You might have no control over what data are collected about you, or how they are used.

"Road pricing," Advanced Vehicle Control Systems (AVCS), and surveillance technologies are just some of the technologies that can limit autonomy and choice. Each of these is briefly discussed below.

Road pricing[8] is an example of a technology that reduces choice and, therefore, autonomy. Although road pricing may make the whole transportation system more efficient overall, it might not be adaptable to individual needs. For example, you might require a specific travel option (e.g., parking or road use) at a particular time, only to discover that, when you need to use it, it has been priced beyond your financial reach. This could also inadvertently lead to the creation of two classes of drivers — those who can afford the best travel options and those who cannot.

To address this problem, it has been suggested that a public program might be created to qualify certain travellers (e.g., people who are poor, disabled, or elderly) for transportation subsidies. However, this produces its own privacy concerns, such as extensive information collection and data matching to verify eligibility.

Another matter related to cost is the concern that ITS may require commuters to pay just to maintain their current levels of privacy. Having to pay for something that once was free has the effect of constraining your choices.

Autonomy is further affected by applications in the area of Advanced Vehicle Control Systems (AVCS). AVCS can actually take over the operation of your vehicle if its in-vehicle sensor technologies "determine" that you or your vehicle are not "fit" to drive (i.e., your tires are worn, you are sleepy or impaired, etc.).

Surveillance technologies such as AVI (mentioned above) can also severely limit autonomy. The capacity of AVI and other ITS technologies to monitor your movements and to collect, use, and disclose detailed information about you, without your knowledge or consent, can have a chilling effect on your behaviour. Knowing that we are being watched changes the way we feel and act. Privacy and autonomy are affected when, due to ITS surveillance, you no longer feel comfortable about going wherever you want, whenever you want, and associating with whomever you want. But it doesn't have to be that way.

ITS applications may be designed in such a way that they provide total anonymity and privacy, while still achieving the desired goals. Take for example an electronic toll payment system which offers "absolute privacy" and "cannot be used to trace the identity of the card or its owner to a given transaction".[9]

Another example involving a card for automatic transit fare collection indicates that while "it is possible for a card reader to keep detailed records of card usage without the card user's knowledge … the reader can be designed so that it protects the card user's privacy by not keeping long-term records, which include tracking information".[10] The development of privacy-protective options such as these must be encouraged.

Personal privacy — Questions to ask

There are some key questions you may wish to ask ITS developers and operators to ensure that your personal privacy is not jeopardized by ITS:

1. To what extent may I participate in any decisions to implement technologies that could diminish my personal privacy?

2. Will I be informed (by street signs or other means) that I and/or my vehicle may be under surveillance?

3. Will monitoring or surveillance be continuous or sporadic?

4. What kinds of surveillance technologies will be involved (e.g., tracking by satellite, video camera, or transponder)?[11]

5. Will I have to pay to maintain my current level of personal privacy?

Informational privacy

"Informational privacy" implies that all information about you belongs to you. Therefore, you should have the right to control how this information is collected, used, stored, disseminated, disposed of, or otherwise treated. This section will discuss concerns related to the collection and treatment (i.e., retention, use, disclosure, security, and disposal) of personal information under ITS.

Collection of personal information

ITS can jeopardize informational privacy because you may not know what types of data are being collected from you, or about you, or how they are being used. There are several ITS applications/technologies that generate personal information, including many in the Travel and Traffic Management Systems (TTMS) and Electronic Payment categories. Both Advanced Traveller Information Systems (ATIS) and Advanced Vehicle Control Systems (AVCS) require the identification of specific vehicles and/or drivers. Other technologies, such as "route guidance,"[12] require continuous, real-time collection of information regarding your location and destination.

Data generating technologies rely on one or two-way interactions between you or your vehicle and the ITS infrastructure. Each interaction generates identifiable transactional data that can be stored in a computerized database. This information may then be used by the ITS operators. For example, it would be possible to analyze it to determine your travel patterns and driving habits. It can also be used to track your car and its occupants.

This is especially so in the case of Automated Vehicle Identification (AVI). Electronic toll collection involving AVI can create a huge database holding vast amounts of information about credit and transportation habits. Debit-based AVI requires your address and vehicle registration. Credit-based AVI may require collection and storage of your credit card account number so that a bill may be sent to you. Your bill would also list the exact time and location of your car when the charge was incurred.[13]

Automatic toll and road pricing systems have caused concern in some countries because of their reliance on computers, which provide for the centralized storage of personal data. Such data have included road use records on specific motorists so that they could be appropriately billed.

ITS technologies are also capable of collecting and retaining more information than is absolutely necessary to fulfil the purposes of the program. For instance, it is technically possible to capture and store positively identifiable photographic images of your entire vehicle, or your face. The practice of photographing license plates for the purpose of collecting tolls or issuing speeding tickets is a case in point. While photographic tracking for billing purposes does not require anyone to be personally identified, the capability exists.

The photo could capture the faces of drivers and passengers, not only in the targeted vehicle, but surrounding vehicles as well. Pedestrians, cyclists, or others who happen to be within the vicinity of the targeted vehicle could also be caught on film. Access to the database of original photos remains yet another issue (i.e., it becomes a treatment of personal information issue).

Treatment of personal information

In addition to the collection of personal information, there are assorted issues regarding its treatment, i.e., retention, use, disclosure, security, and disposal. For example, signals from satellite applications and cellular radio signals between vehicles and ITS computers (for traffic updates or emergencies) can be intercepted and used by third parties.

Concern has also been expressed that governments are simply retaining too much personal information about citizens and that ITS records represent a whole new cache of information about individuals that governments can possess. The heavy reliance of ITS on computers raises still more issues. This is because data in electronic form tend to be easier to access, share, compare, match, merge, compile, and transfer.

There is particular concern about the tendency for information which has been collected for one specific purpose to be used for other, unauthorized purposes. It has even been said that, "(ITS) technology is just the kind of technology that tantalizes technologists and government planners to add new and perhaps overreaching uses".[14] For example, government-held ITS

data could become accessible to the public in the same way that licensed driver and vehicle ownership records are currently accessible. Or worse, ITS databases in different jurisdictions could be connected to form national or international tracking systems.

Both private industry and different levels of government may be interested in buying, selling, renting, or trading personal data generated by ITS. Business could use it for direct marketing. Indeed, the marketing and selling of personal information is a growing industry.

Another issue concerns the potential for government or private corporations to be able to manipulate and disclose ITS records, or to make decisions about people based on that information. For example, this information could be analyzed and used in making decisions about what particular benefits and services you deserve or should continue to receive. It could be used "for law enforcement investigatory purposes; governmental licensing purposes; various civil justice purposes; employment purposes; insurance purposes; and a host of other public and private purposes".[15] This would be particularly serious if those decisions were to be based on irrelevant, outdated, or incorrect data.

The potential for traveller data to become used or misused in non-ITS-related ways, increases the longer these data remain identifiable in a database. Your individual travel data can also be cross-matched with the movements of other persons, revealing even more personal information.

Informational privacy — Questions to ask

As with personal privacy, there are a number of critical questions you may wish to ask in relation to the protection of your personal information under ITS:

1. Does the ITS application record personal information about travellers or specific information about vehicles? If so, what does it record (e.g., vehicle identity, location, or speed; identity of vehicle occupants; transactional data, etc.)? Will I have any control over the contents of my ITS file?

2. For what purpose is the information collected and is it really necessary to have it? Have other ways of achieving the same objectives been explored (i.e., ways which do not require the collection of personal information)?

3. How and by whom will the information be collected, stored, accessed, used, and disclosed? What choice or control will I have over any of these practices? Will my informed consent be required before any of these are done?

4. Will my information be accessible by name or other personal identifier?

5. What safeguards will there be to ensure that my records are secure, accurate, complete, relevant, up-to-date, and protected from unauthorized use or misuse? Can I correct or amend a record about me? Will there be proper procedures for disposing of old and irrelevant data?

6. What redress will be provided if my information is misused or if harmful decisions are made about me on the basis of inaccurate information?

7. How long will my information be retained by the system? Is long-term storage truly necessary?

8. Will my ITS information be combined with other data about me, such as biographic details or other driver record information?

9. Will the records collected through every ITS application be centralized? What standards exist to govern the interconnectivity and integration of ITS databases?

Applications of ITS

The preceding analysis on the privacy implications of ITS contained references to assorted ITS applications. We now turn our attention to a more detailed discussion of the applications of ITS in general, in Canada, and abroad.

The Intelligent Transportation Society of America (ITS America) has identified at least 28 ITS "user services" that can be grouped into about six categories.[16] Each category, briefly described below, consists of a broad mix of technology applications.[17] The technologies, user services, categories, and their labels all continue to evolve.

Travel and Traffic Management Systems (TTMS)

This category consists of technologies used to monitor and control traffic in real-time (i.e., as it is happening) by communicating with travellers, providing continuous information about highway and weather conditions, adjusting traffic operations, and responding to problems. Services in this category include Advanced Traveller Information Systems (ATIS), Advanced Travel Management Systems (ATMS), and Travel Planning.

These services are intended to help commuters avoid delays and improve their travel efficiency. For example, a service called route guidance proposes to provide travellers with a suggested route plus simple instructions on how to reach their destination. In developing the ideal route, the service considers such factors as traffic conditions, road closures, and transit system status/schedules. In addition to drivers of all types of vehicles, cyclists and pedestrians are also expected to be able to access this service, using a hand-held device.

Public Transportation Management Systems (PTMS)

This category essentially involves the automation of public transit system management, planning, and operations. It includes computer analysis of real-time vehicle and facility status so that transit maintenance and operations may be improved. For example, the analysis can identify deviations from schedule and provide drivers and dispatchers with possible solutions.

In conjunction with other traffic control services, PTMS is expected to help maintain transportation schedules and assure transfer connections between different modes of transportation. Improved service and administrative reporting is also expected to result from the recording of information about bus schedules, passenger loading, and mileage accumulated. As well, PTMS contemplates the use of smart cards for fare payment.

Electronic Payment Systems

Also called Travel Payment Systems, these involve electronic payment for all transportation modes and functions, including toll collection, transit fares, and parking. Electronic or automatic road toll collection enables drivers to pay tolls without stopping or using change. Instead, a two-way communication receiver allows a vehicle to communicate with toll booths using a smart card or similar device to pay a toll.

A typical feature of electronic toll collection systems is their use of transponders to identify individual vehicles (AVI). A transponder is a small communications device that can be attached to a vehicle. The device works by transmitting a signal which can be picked up at a remote location by a receiver. The receiver is then able to automatically locate the vehicle and identify it to the ITS infrastructure.

Electronic payment is also utilized in road pricing schemes. Road pricing refers to the real-time pricing of any road, bridge, or on-ramp that has an associated toll. Parking facilities and public transportation can also be priced in real-time. This technology relieves congestion by discouraging the use of heavily used transportation options by increasing the price of those options.

Commercial Vehicle Operations (CVO)

CVO applies TTMS (Travel and Traffic Management Systems) features within the commercial vehicle sector. Services include the automatic location, classification, and weighing of vehicles for tax collection purposes. Vehicle emissions may also be monitored. All of this can be done while the vehicle is still in motion at highway speeds. CVO requires the individual identification of commercial vehicles.

Emergency Management

The objective of these systems is to enable emergency units (e.g., police, firefighters, and ambulance) to respond more swiftly to incidents on the highway. Services include public transit security as well as emergency notification of the appropriate authorities in cases of vehicle breakdown and hazardous spills. Technologies used here include route guidance and "signal priority", which acts to clear traffic signals in an emergency vehicle's path.

Advanced Vehicle Safety Systems

Known also as Advanced Vehicle Control Systems (AVCS), these feature a diverse range of safety and collision avoidance mechanisms through automation of some or all driver functions. Included under this category are technologies which manage vehicles in dangerous or potentially dangerous situations, such as anti-lock brakes and adaptive cruise control. AVCS can also monitor the physical and psychological condition of drivers and take over operation of their vehicles altogether.

Status of ITS in Canada

Currently, functional applications of ITS in Canada are limited largely to Ontario and British Columbia. However, universities, industry, and government organizations across the country are conducting ITS research, development, or testing. As well, an ITS Canada group has been formed by the Transportation Association of Canada. The group serves as a forum for information exchange, liaises internationally, and facilitates the research, development, manufacture, application, and standardization of ITS across Canada.[18]

British Columbia

HELP (Heavy Vehicle Electronic License Plate Program) was Canada's first automatic truck weigh-in system. It was installed along the TransCanada Highway in British Columbia and several Interstates in six western American states. The purpose of the system is to improve the flow of transport trucks in the British Columbia to Texas corridor by automatically identifying and weighing vehicles as they pass weigh stations and border entry points. Data collected at each site are processed centrally and used by both governments and the trucking industry for regulatory, weight enforcement, and fleet management purposes. The system involves road-mounted sensors and radio tags attached to truck licence plates.[19]

Ontario

A variety of ITS projects are being planned or tested in Ontario. These projects involve functions in such areas as PTMS (Public Transportation Management Systems), ATIS (Advanced Traveller Information Systems), CVO (Commercial Vehicle Operations), and Emergency Management.

In Toronto, monitoring devices and electronic signs that update drivers on road conditions have been installed on major highways, such as Highway 401. As well, two video traffic monitoring systems have been introduced in Toronto and the surrounding area. Automatic toll collection has been set up at border points between Canada and the United States in the Great Lakes area. A fully electronic toll highway (Highway 407) is also being planned. Some of these initiatives are further described below.

COMPASS Traffic Management System

The COMPASS system operates along three highways: Highway 401–Toronto, QEW–Mississauga, and QEW–Burlington. The system videotapes traffic for the purposes of ensuring safety and rapid detection/response to traffic incidents, such as vehicle breakdowns, accidents, and spilled cargo. The main goals of the COMPASS system are to reduce congestion and accidents.

While COMPASS cameras are capable of obtaining "close-ups" (of license plates, for example), zooming in on faces is against standard operating directions. Cameras are supposed to maintain a wide field of view so that all traffic flow may be properly monitored.

Gardiner Traffic Management System

The Gardiner–Lakeshore Corridor Traffic Management System monitors traffic volume by means of remote cameras installed along the corridor. The system also informs drivers about road conditions and alternative routes, permits the quick detection of stalled cars, and facilitates the arrival of ambulance, police, and environmental units to accident or oil/toxic spill locations. Like COMPASS, the intent is to minimize congestion and danger. These cameras can also zoom in on license plates and faces, but are not meant to be used in this manner.

Highway 407

The construction of North America's first entirely electronic toll road has begun just north of Toronto. Highway 407 is expected to be free of the congestion and bottlenecks associated with traditional toll roads because it will have no manual components, such as toll booths. The first phase of the highway is scheduled for completion in December 1996.[20]

Several methods of completely electronic toll payment have been proposed for regular users of the highway. One method involves charging the appropriate toll to a driver's credit card or deducting the toll from his or her bank account. However, this would leave a data trail.

Another option available is privacy-protective. It permits anonymous transactions using a transponder tag that is charged up (like a cash card) before entering the highway. The toll is then automatically deducted from the "card" balance.

In both cases, a transponder is affixed to the vehicle and scanned when entering and exiting the highway. Occasional highway users will likely have their license plates photographed, so that a bill can be sent to the vehicle owner when a predetermined amount has been reached.

ITS in other jurisdictions

A considerable amount of ITS field testing has already taken place worldwide, with varying degrees of success and failure. Many more demonstrations are being planned. There has been substantial variety among the projects in terms of approach, scope, and applications/technologies used. A small sample of these initiatives is presented below.

Europe and Asia

Europe has several large scale projects underway, a number of which are being co-ordinated by the Commission of European Communities. Projects fall under such categories as TTMS (Travel and Traffic Management Systems), PTMS (Public Transportation Management Systems), and CVO (Commercial Vehicle Operations).

One of the earliest uses of ITS technology was in road pricing and automatic toll collection in several Asian and European countries. Singapore, the United Kingdom, Portugal, Italy, Finland, and Norway have tried one or both. Sweden plans to introduce automatic toll collection by 1996. Hong Kong conducted one of the first experiments with road pricing, but found privacy concerns to be a major impediment to its success. For example, "vehicle owners began feeling uneasy regarding the system when they realized that the driving charges sent to their homes included an itemized listing of the time, date and location of the driver for each charge".[21]

ITS technology is also being used to assist with law enforcement. In Japan, police have been actively developing such technology, including vehicle sensors to be installed at traffic signals. Police in China use ITS to monitor key intersections in major cities. Officers stationed in control centres scan the scene for traffic violations and notify police on patrol who can then immediately apprehend offenders.

Various traffic management systems are being deployed around the globe. In Japan, such systems have been installed in all large cities and on most urban and interurban freeways. The Japanese have made substantial investments in the development of driver information systems. One expressway monitors traffic speed and volume electronically and gives drivers instant warnings about traffic accidents and delays. The warnings, as well as other driver information, are displayed on variable message signs. In Britain, such information has been transmitted directly to screens located on the dashboards of subscribing motorists.[22]

In Australia, experiments have begun with a global positioning system that uses satellite technology to establish location and operational information on trucks and railway fleets.

United States

As part of the *Intermodal Surface Transportation Efficiency Act* of 1991, the United States Congress authorized a $660 million ITS program. The *Act* directed the Secretary of Transportation to conduct research, development, and testing on ITS, and to promote its integration into the country's surface transportation system. A key goal of this *Act* was to have the first fully automated roadway or test track in place by 1997. The law also required the Secretary to report to Congress on privacy and other concerns related to the ITS program.[23]

There are many operational tests underway in the U.S., particularly in the categories of TTMS (Travel and Traffic Management Systems) and CVO (Commercial Vehicle Operations). Several states have already installed some form of automatic toll collection, including Texas, New York, Louisiana, Oklahoma, Colorado, Georgia, and Illinois.

With respect to law enforcement, certain American cities are using electronic tracking systems to retrieve stolen vehicles. When a car theft is reported to police, this information is entered into a police computer network. The computer then sends out a signal via radio towers. That signal activates a transmitter-receiver which has been hidden in the stolen car. This triggers the car's homing signal, which may then be picked up by police cars that have been specially equipped with an electronic tracking device.[24]

In addition, there is the Intelligent Transportation Society of America (ITS America), a broad-based coalition of ITS contractors, government agencies, academics, and others. This group conducts research and education, and promotes/co-ordinates the development and deployment of ITS applications across the U.S. The group also acts as a federal advisory committee to the U.S. Department of Transportation.[25] As well, the Legal Issues Committee of ITS America has drafted a set of ITS Information Privacy Principles, "in recognition of the importance of protecting individual privacy in the face of expanding transportation technology capabilities".[26]

Conclusion

This paper provides a brief introduction to ITS and the key privacy issues associated with it. It also raises several questions related specifically to the implications of ITS for personal and informational privacy. ITS developers, operators, regulators, and users need to address these questions to properly safeguard privacy.

ITS technology is continuously expanding. Listed below are some general questions you can ask to assess the privacy implications of new ITS applications:

1. Has a thorough evaluation been conducted on the effects that the application could have on privacy?

2. Have adequate legislative standards or codes been developed to control the impact of ITS on privacy in my area? Does the application comply with existing privacy legislation? Has the government explored other, perhaps more effective, cost-efficient, and privacy-respecting ways of achieving the same results expected from ITS?

3. Will I be allowed to choose whether or not to use an ITS service? If so, will I be given all the information I need about both its "pros and cons" so that I can make an informed choice? How much privacy am I willing to forfeit in exchange for the convenience of using the system?

4. What kinds of privacy safeguards have been built into the technology and its application?

5. During implementation, what efforts will be undertaken to minimize or eliminate the application's impact on privacy?

6. Will I have to pay for privacy protection?

7. Is it really necessary for the technology to identify me or my vehicle in order to fulfil its functions?

8. Who can I call if I have questions or concerns about the impact of an ITS application on my privacy?

We are all entitled to ask these questions and to expect privacy protection. After all, the information that is going to be collected and used is our own. As one reporter recently expressed, "In the end, you see, my identity belongs to me".[27]

The Information and Privacy Commissioner/Ontario looks to the government and private sector to work with the public to ensure that privacy is protected throughout the development and implementation of ITS technologies.

Notes

1. ITS has also been referred to by a variety of other names, including, Intelligent Vehicle-Highway Systems (IVHS), smart highways/cars, Advanced Transport Telematics, Road Transport Informatics, Advanced Road Traffic Systems, or simply, Advanced Transportation Systems.

2. "IVHS Business Booms With Infusion of Hundreds of Millions of Scarce Federal Dollars — But Safety Claims Aren't Backed By Science," pp. 1–4, 6; "Flawed Study of Crashes in Germany Underlies Many IVHS Safety Claims," pp. 4–5; "Spurious Claims About Safety Benefits Aren't the Only Problems With IVHS Technologies; Two Added Concerns Dampen Enthusiasm," p. 7; *Status Report — Insurance Institute for Highway Safety — Special Issue: Intelligent Vehicle Highway Systems*, Vol. 29, No. 8, July 30, 1994.

3. IVHS America and the U.S. Department of Transportation, *IVHS Architecture Development Program — Interim Status Report* (Washington, D.C.: April 1994), p. i.

4. AVI typically involves the use of transponders. See page 11 of this paper for further discussion.

5. Sheri A. Alpert, *Privacy on Intelligent Highways: Finding the Right of Way*, July 1994, p. 16.

6. *The Privacy Bulletin*, Special Issue, Vol. 6, No. 2, August 1990; Sydney, Australia, as cited in Alpert, p. 1.

7. Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992), pp. 18–19, as cited in Alpert, p. 14.

8. For a description of road pricing, see page 11 of this paper.

9. David Chaum, Digicash, "The Toll Payment/Road Pricing Technology Everyone Has Been Waiting For," 1994, p. 1.

10. Colin Plumb, Boulder Software Engineering, "Protocol for Fare Collection Using a Contactless Memory Card," unpublished paper, January 16, 1995, p. 2.

11. For a description of transponders, see page 11 of this paper.

12. For a description of route guidance, see page 10 of this paper.

13. Thad Dunning, "The Information Highway Isn't the Only One Wired," *Privacy Journal*, June 1994.

14. "Privacy Poses Test for IVHS Industry," *Privacy & American Business*, Vol. 1, No. 2, January/February 1994, p. 3.

15. Robert R. Belair, Alan F. Westin, John J. Mullenholz. *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, (Washington D.C.: prepared for the U.S. Department of Transportation, December 8, 1993), p. 40.

16. IVHS America and the U.S. Department of Transportation, *IVHS Architecture Development Program - Interim Status Report* (Washington, D.C.: April 1994), p. 11.

17. Several different technologies are used under ITS and each technology can appear under more than one category. For example, satellite-based global positioning systems and variable message signs may be applied under more than one category.

18. IVHS Roundtable, Transportation Association of Canada, *Intelligent Vehicle-Highway Systems (IVHS) - A Synopsis* (Transportation Development Centre of Transport Canada, June 1992), p. 20.

19. Lawrence Surtees, "Computers Take Heat Off Highways," *Globe and Mail*, May 13, 1992, p. B6, as cited by the Information and Privacy Commissioner/Ontario, *SmartCards*, April 1993, p. 17.

20. jobsOntario News Release, *Toll Technology Firms Prepare to Join Highway 407 Partnership* (Ontario: Government of Ontario, September 1, 1994), p. 30.

21. Elizabeth A. Barton, "Privacy Concerns About IVHS Outside the United States," *Santa Clara Symposium on Privacy and Intelligent Vehicle-Highway Systems, Symposium Materials - Part I*, (California: Santa Clara University School of Law, July 1994), pp. 1–11.

22. "Big Brother is Clocking You," *The Economist*, August 7, 1993, pp. 71–72.

23. Sheri A. Alpert, *Privacy on Intelligent Highways: Finding the Right of Way*, July 1994, p. 3.

24. Alan Gathright, "Police Follow Car Alarm's 'Beep' As Crimebusting Goes High-tech," *The Toronto Star*, May 12, 1990, p. G24.

25. Robert R. Belair, Alan F. Westin, John J. Mullenholz, *Privacy Implications Arising from Intelligent Vehicle-Highway Systems*, (Washington D.C.: prepared for the U.S. Department of Transportation, December 8, 1993), p. 38.

26. ITS America Legal Issues Committee, *Comment Form — Intelligent Transportation Systems Information Privacy Principles*, Fall 1994, pp. 1–4.

27. Patricia Elliot, "Privacy Matters," *Canadian Living*, February 1995, p. 89.