Impact of Electronic Road Toll Technology on Privacy

Paul Won-Bin Sung

Department of Information Systems and Operation Management

University of Auckland

Email: wonbin81@gmail.com

John Paynter

Department of Information Systems and Operation Management

University of Auckland

j.paynter@auckland.ac.nz

Abstract

As the government begins implementing information technology projects, individual privacy issues are at risk. Privacy concerns are nothing new, but novel information technologies have found new ways to collect and monitor information about individuals. As technology develops, it is important that the privacy principles are assessed in order to maintain the applicability of these principles. This paper addresses the impact of an electronic road toll system on privacy. Transit NZ (a New Zealand government agency) is considering a project to collect road tolls electronically by keeping track of vehicles that pass the toll points. This paper explains the basic privacy principles and outlines a brief overview of the technology. Privacy issues are then identified and their impact on the privacy principles is discussed. Overseas examples are also discussed to shed light on the potential privacy impact in New Zealand. Finally, some of the ways to protect and improve privacy are discussed.

Keywords: Information Privacy, Privacy Act 1993, Road Tolling, Congestion Pricing

1 Introduction

Privacy issues can arise from implementation of information technology and these issues must be studied in detail. Privacy issues are important because they affect all individuals. It is our right as citizens to have control over personal information and be anonymous to others. Privacy is defined as "moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state" (Laudon & Traver, 2002). Information Privacy includes "both the claim that certain information should not be collected at all by governments or business firms, and the claim of individuals to control the use of whatever information that is collected about them."(Laudon & Traver, 2002)

This quality assured paper appeared at the *19th Annual Conference of the National Advisory Committee on Computing Qualifications* (NACCQ 2006), Wellington, New Zealand. Samuel Mann and Noel Bridgeman (Eds).

.Information technology currently under consideration is the electronic road toll system. Privacy implications are important in implementing the electronic road toll system and they should be carefully analysed.

Although the electronic road toll system brings economic benefit, it may be considered intrusive of privacy and has the risk of identity theft for all drivers passing through the toll points. The electronic road toll system creates large personal information database that could be useful to the government and the private industry. (Garfinkel, 1995) Vehicle tracking information could become important in many court cases, such as criminal investigations, work compensation and personal disputes. (Agre, 1995)(Garfinkel, 1995) Private information could be sold illegally and there is potential risk for identity theft. There is also the possibility of transponders being used not only in electronic road toll system, but further developed to monitor speed, parking and general vehicle movement.

An electronic road toll system affects many different parties. Some of the major stakeholders include the motorists passing through the electronic road tolls, Transit NZ, AA (Automobile Association), insurance companies, VINZ (Vehicle Inspection New Zealand), Ministry of Transport, Privacy Commissioner, toll collectors and possibly private investigators. Motorists passing through the electronic road toll will have their vehicle information collected automatically. Movement will be recorded and vehicle registration information will be used to invoice road tolls. Transit NZ is the organisation implementing the project and therefore responsible for the feasibility study. The AA is affected, because it represents the country's drivers. Insurance companies wish to locate stolen cars and possibly ensure that vehicles are being driven by authorised drivers and for purposes for which they are ensured and legally with respect to the road laws. VINZ monitors vehicle registration and warrant of fitness. Ministry of Transport is involved, since it is the government organisation overlooking the whole process. The Privacy Commissioner is also affected because he/she needs to consider privacy impact assessments. The toll collectors are affected, because they will be in charge of the system implementation. The toll collectors may not necessarily be the government; the system may be maintained by the private sector. Private investigators could also become

involved if the information collected from electronic road tolls become the deciding factor in court cases. Finally with various schemes floated for introducing congestion pricing (Dearnaley, 2006) the use of the system could become much more widespread with local authorities levying congestion charges for use of roads at certain times and prohibiting the use of roads (e.g. Grafton Bridge) to private vehicles.

2 Background

2.1 Information Privacy Principles

The 1993 Privacy Act in NZ has twelve principles (Fig 1). These principles deal with general rules regarding collection, holding, use and disclosure of private information.

Implementing the electronic road toll system affects all the twelve privacy principles, but it should not violate any of them. First of all, the data should only be collected for the purpose of collecting road tolls. Also, the data collected should only be the data that is necessary. The purpose and collection of data should conform to the privacy principles 1-4. The data collected should be kept in a secure place and should be safeguarded in a proper manner according to principle 5. Individuals must have access to their personal information and should be able to correct it if mistakes are made. (Principles 6, 7)

PRINCIPLE 1 - Purpose of collection of personal information

PRINCIPLE 2 - Source of personal information

PRINCIPLE 3 - Collection of information from subject

PRINCIPLE 4 - Manner of collection of personal information

PRINCIPLE 5 - Storage and security of personal information

PRINCIPLE 6 - Access to personal information

PRINCIPLE 7 - Correction of personal information

PRINCIPLE 8 - Accuracy, etc., of personal information to be checked before use

PRINCIPLE 9 - Agency not to keep personal information for longer than necessary

PRINCIPLE 10 - Limits on use of personal information

PRINCIPLE 11 - Limits on disclosure of personal information

PRINCIPLE 12 - Unique identifiers

Fig 1: Information Privacy Principles (Information Privacy Principles, 2005)

Principle 8 states that personal data should be accurate, up-to-date and reliable. The government should not keep the information about the vehicles for longer than the necessary time period and the use of private information should be limited according to principles 9 and 10. The level of private information disclosed should be restricted in accordance with principle 11 and all private information should not be uniquely identified. (Principle 12) (Information Privacy Principles, 2005)

2.2 Overview of Electronic Road Toll Technology

The objective of an electronic road toll system is to reduce traffic congestion, increase convenience and safety. The vehicles do not have to slow down or stop to pay the tolls, so it increases the overall efficiency of the motorway. (Wright, 1995) There are several different types of electronic toll systems, including roadside transponders and satellites. Commercial vehicle tracking systems also work via GPS for both fleet operations and private cars – see www.snitch.co.nz). This paper will concentrate on the transponder technology which is most popular and well-known.

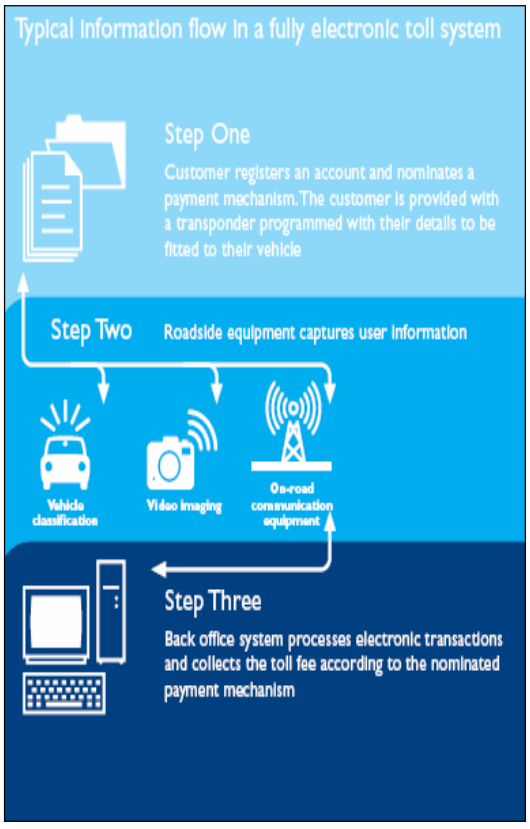


Fig 2: Electronic toll system (Toll Systems Project, 2005)

Electronic road toll technology will involve vehicles being mounted with a transponder on their windscreen. All vehicles passing though the tolling point will be detected by the transponder and road toll will be deducted automatically from an account set up by the owner. If the

vehicle does not have an electronic transponder, the vehicle will be detected by a camera taking a photograph image of the vehicle's number plate. The driver will be traced using the vehicle registration information from the number plate and an invoice will be sent to the owner. An overview of an electronic road toll system is shown in Fig 2.

2.3 Technology Issues

There are few risks associated with electronic toll system technology.

2.3.1 Capturing Images

For vehicles that do not have transponders, a video image of the number plate will be captured. However, there could be difficulty in capturing images, if the number plate is dirty or visibility is poor due to extreme weather conditions.

2.3.2 Security Risks

There is also the security risk of information being intercepted while being transferred back to the office. An electronic toll system involves transferring private data over a wireless network and therefore carries the risk of interception or spoofing. Appropriate security measures must be in place.

2.3.3 General Reliability

There could also be the issue with general reliability of the technology. As vehicles pass through the tolling point, the system must know whether to take a picture or to receive information from the transponder. The toll system must be accurate and efficient. It must also be user friendly and the public must have confidence in the technology.

2.4 General Privacy Issues

There are several privacy concerns regarding an electronic toll system. These are:

2.4.1 Individually identifiable information

Electronic road tolls will essentially collect uniquely identifiable information about the vehicles and therefore carry privacy concerns. Individual vehicles will be recognised through the transponder and the movement of the vehicles are tracked. This results in loss of privacy and being free from surveillance. However, technology such as digital cash or smart cards can be used to avoid individually identifiable information being recorded. (Agre, 1995) The use of smart cards will be discussed in a later section.

2.4.2 Persistent Information

Although the information is collected for road toll charges, it is likely that the information will be kept, even after the toll fees have been collected. The information is needed to monitor/control vehicle movements and maybe used for congestion pricing. As long as this is done at an aggregate level to record number and type of vehicles, privacy will be maintained.

2.4.3 Security

This refers to general security of private information in the database. The security risks under "2.1 Technology Issues" refer to risks arising from new technology, but this section is focused on keeping private information safe once it has been collected. The database maybe stored in a centralised location making it more vulnerable to security risks. Electronic form of information is considered "easier to access, share and therefore steal." (Wright, 1995) However, security is only a small part of overall privacy issues. (Agre, 1995)

2.4.4 Standards

Standards must be created early in the implementation process. General standards regarding electronic toll system and specific standards relating to privacy should be set up. It is nearly impossible to change or reverse a standard after it has been implemented, because many parties would have been treated in accordance with the original standard. (Agre, 1995) Lack of clarity in the standards could have negative implications, especially regarding collection and use of private information.

2.4.5 Secondary Use

There is great opportunity for secondary use of the data collected from the electronic road toll system. Information collected can be invaluable for marketers. The owner of the vehicle must be notified if the information is to be used by a secondary party. Sometimes, the government may try and use the information for different purposes, such as policing, licensing purposes and other various civil justice purposes. (Wright, 1995) Whatever the case, the secondary use of private information must be thoroughly investigated. (Agre, 1995)

2.4.6 Law Enforcement

It must be clear what the consequences are for breaching the rules regarding use of private information, and how restrictions or law enforcement will be administered. These must be clearly outlined before the implementation of the technology. (Agre, 1995)

2.4.7 Commercial applications

There is a possibility that vehicle tracking technology may be used commercially. Many truck companies currently use GPS (Global Positioning System) to track drivers. If the technology like electronic toll systems becomes commercialised, privacy maybe greatly affected. For example, rental companies might keep track of their vehicles to find out the common routes or destinations. (Agre, 1995). Other commercial applications include tracking family (for safety reasons) and employees (for efficiency reasons).

2.5 Latest Development in New Zealand

The Cabinet approved the construction of tolled roads in April 2005 and the ALPURT project is currently underway. Transit NZ claims the tolled road has met two prerequisites, an alternative route and high level of support from the community. (Young, 2005) However, a lobby group which has been formed to combat this project claims the two prerequisites are in fact not met. The current focus so far has been the construction of the tolled motorway itself rather than the implementation of the electronic road toll system. However, the privacy implications are crucial in the implementation of the electronic road toll system and these must be carefully analysed.

3 Privacy Impact Assessment

In this section, the positive and the negative aspects of use and misuse of private information will be discussed. Each issue will be identified and related to the privacy principles affected.

3.1 Use of Private Information

Clearly states the research question and the background to the problem being researched and its relevance to the conference audience. The major positive aspect through use of private information is:

3.1.1 Paying road tolls is more convenient.

Drivers do not have to stop to pay for road tolls. Tolls will automatically be deducted from a designated account and will not slow the traffic flow. This issue closely relates to privacy principle 1. As long as the information is only used for collecting road tolls, individuals benefit from implementation of electronic road toll system.

There are many potential negative aspects through use of private information.

3.1.2 Government is able to track vehicle movement.

Each vehicle is identified as it passes through a tolling point. Therefore, the government has access to private information such as date and time a vehicle took a certain route. This issue relates to privacy principles 1 and 11. As long as the government only uses this information for its intended purpose, it should not cause any harm to individual. Private information should not be disclosed to anyone else.

3.1.3 Security of private information

The information collected from electronic road tolls must be kept in a secure place. The collection of private information creates a database that is tempting for many private and government organisations (Agre, 1995) Privacy principle 5 is particularly important in maintaining security of private information.

3.1.4 Historical data

It is likely that the information of vehicle movement will be kept after the road toll has been paid. In deciding whether the government should keep data for historical purposes, privacy principle 9 is affected. Principle 9 states that "An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used" (Information Privacy Principles, 2005) and the government must decide how much historical data is required.

3.1.5 Control over information

Individuals should have access to information about themselves and their vehicles. However, individuals should not be able to alter the record for illegal purposes. According to privacy principles 6 and 7, individuals should have access to their private information. They should be able request correction of information, if their personal details are incorrect.

3.1.6 Reliability of technology involved and data collected

The public must be certain that the technology is reliable and accurate. If data collected are incorrect due to technology, it can lead to some serious consequences. This indirectly affects privacy principle 8 where the accuracy of personal information should be checked before use.

3.2 Misuse of Private Information

Misuse of private information can have serious consequences, but it can also have some benefits. Positives aspects of misuse of information are:

3.2.1 Track stolen vehicles

The government may give information to the police to track stolen vehicles. Although this violates privacy principle 10, it can be beneficial for the vehicle owner and perhaps public safety. It may fall under the exempt category since it can lead to overall benefit.

3.2.2 Track criminal activity/Evidence for court cases

If a vehicle was involved in a criminal activity, or the vehicle movement information is crucial to the outcome of a criminal court case, misuse of private information may seem beneficial. This issue also violates principle 10, because the information is not used for its original purpose. However, it may benefit the society as a whole.

3.2.3 Verify company information

If a company vehicle is involved, the information collected may be helpful regarding calculation of fringe benefit taxes. It may also be beneficial for resolving disputes over the use of a company vehicle. This violates principle 10, but benefits the individual parties and the

government. The government benefits by collecting more tax.

Misuse of private information may raise serious issues. These are outlined below.

3.2.4 Information may be sold to the private sector

The information collected can be useful to the private sector and the government may be tempted to sell information at a profit. The electronic road toll system creates a large personal database that some marketing companies could use to generate profit. This seriously violates privacy principle 10 and individuals will be adversely affected with unwanted marketing campaigns.

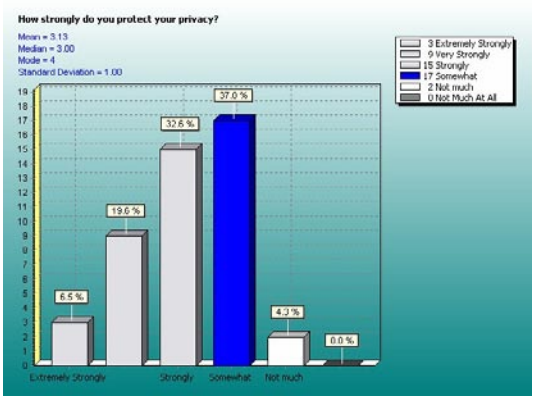
3.2.5 Identity theft

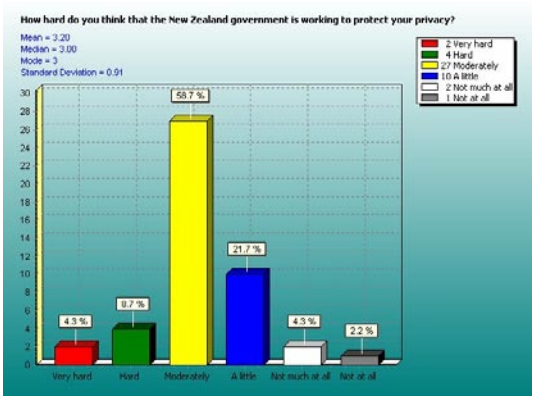
Private information could be sold illegally and lead to identity theft. Stolen transponders or number plates may lead to the wrong person's account being deducted with road toll charges. This affects privacy principles 5, 6 and 7 as the security of information is at risk. If the information is stolen and misused, then the individual must have immediate access to correct his/her information.

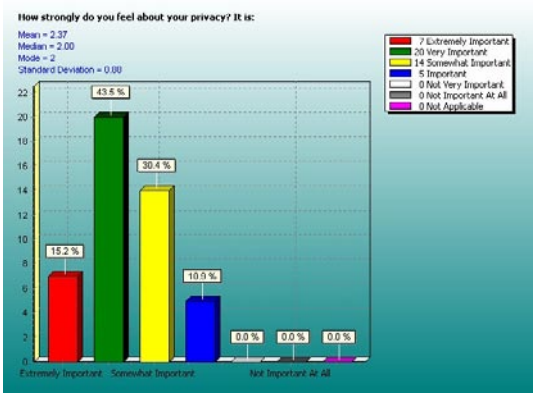
4 Survey Results

A pilot survey was carried out among students, staff and affiliates in the Department of Information Systems and Operations Management at the University of Auckland. The survey asked series of question regarding privacy and respondents' attitudes toward privacy. The respondents were also asked for their views on the impact of new technologies on privacy (Fig 3).

Fig 3: Survey Results







Privacy impact of electronic road toll systems was compared against other new technologies such as biometric passports, electronic surveillance in public places, credit ratings and tracking bad tenants. (Table 1)

The results from the survey show that people feel very strongly about privacy, but are not protecting their privacy to a commensurate extent. 58.7% of the respondents felt privacy was very or extremely important but only 26.1% of the respondents protected their privacy to that extent. (Fig 3)

Although people were concerned about their privacy, especially after the global terrorist scares, people were somewhat less concerned about the impact of electronic road toll systems on privacy. The average response for this question was 3.8 indicating that people were only somewhat concerned with their privacy from electronic road tolls. (Table 1) It maybe that information from electronic road toll systems are considered less private and people are less concerned with protecting their privacy. Also, the majority of people (58.7%) have the perception that the government is only working moderately in trying to protect individual privacy. (Fig 3)

Table 1: Survey Results (Comparison)

Privacy Impact of New Technologies :Survey Results

	Mean	Median	Mode
Electronic Road Tolls	3.8	4	3,4
Biometric Passports	3.07	3	2
Electronic surveillance in Public places	3.98	4	3,4
Credit Ratings	3.63	4	4
Tracking Bad Tenants	3.17	3	4

Extremely Strongly	1
Very Strongly	2
Strongly	3
Somewhat	4
Not Much	5
Not Much at All	6

It showed that the electronic road tolls, along with electronic surveillance in public places have the two highest means, (3.8 and 3.98) indicating people were only somewhat concerned about privacy from these new technologies. People were most concerned with biometric passports and their privacy (mean of 3.07) indicating strong feeling towards biometric passports. In comparison with other new technologies, electronic road toll systems had relatively minor impact on privacy.

Although the survey was not comprehensive, it does give a general idea that Auckland University students consider

privacy as an important issue, although this particular aspect (electronic road charges) was less of an issue.

5 Discussion

In order for the implementation of an electronic road toll system to be successful, privacy issues must be assessed properly. Before potential solutions to privacy problem are explained, it is important to analyse overseas examples, where electronic road toll systems have already been implemented.

5.1 Overseas Example

Overseas tolling systems should be investigated in order to identify any major issues and measure the impact on privacy. Countries including Australia, America, Canada and UK have already implemented the electronic toll system. New Zealand must learn from their successes and avoid any mistakes made by those countries. However, New Zealand is a unique country, so adopting successful models from overseas does not guarantee success.

Road tolls in Queensland, UK and Canada are operated by private companies. (M6toll, 2005; 407 ETC, 2005; Queensland Motorways, 2005) In Canada, a highway was built by the government, but bought by a private company. Midland Expressway Limited in UK and 407 ETR (Express Toll Route) in Canada both have their own privacy policies that are developed in accordance with their national privacy law (M6toll, 2005; 407 ETC, 2005). The privacy policies clearly cover important aspects such as accountability, purpose, use, disclosure and security of private information. Although the Queensland Motorways had some problems with electronic toll system where some users' accounts were being overcharged, none of the overseas examples reported major issues regarding privacy. The companies created a privacy policy and made sure that the customers were aware of the privacy issues involved. Therefore, creating public awareness is an important factor when implementing the electronic toll system.

In New Zealand, Transit NZ is implementing the project and it must ensure that individual privacy needs are met. Transit must clarify the privacy issues involved and outline a policy to ensure that these issues are under control. Transit must also provide a safe alternative route, so drivers are given the option whether to travel on the tolled road or not. Overseas examples show that privacy concerns can be kept under control while still achieving objectives with the electronic road toll system.

5.2 Potential Solution to Privacy Problems

Some of the possible solutions to privacy problems are outlined below.

Privacy Enhancing Technology (PET)

One way to reduce the impact of technology on privacy is to incorporate Privacy Enhancing Technology. PET avoids the need to collect personally identifiable information. An example of PET for electronic road toll system is the smart card. Instead of uniquely identifying individual vehicles, the system just recognises the serial number on the smart card. The driver can top up the smart card and therefore personally identifiable information is not collected. (Information Privacy Principals, 2005; Agre, 1995). The serial number from the smart card is used to pay for the tolls and therefore no information about the vehicle movement needs to be recorded.

Clear Standards

One of the most important tasks when implementing new technology is to first address the legal/privacy issues. Privacy principles must be addressed, and if existing principles are not relevant, separate policies may need to be created. There must be clear rules relating to collection, share and use of information. Exception cases and secondary use of information must be clearly identified to avoid confusion. There must also be punishments for breach of these privacy policies.

At the moment, there is some flexibility in the use and disclosure of information with the privacy principles. For example banks may share information with the associated company providing financial services. (Information Privacy Principles, 2005) There must be clear a purpose and constraint on sharing or using information for secondary purposes. It is likely that the database created by the electronic road toll system will be available to the police, but the decision to do so must be carefully analysed. (Information Privacy Principles, 2005) It must be remembered that the electronic toll system is put in place to collect road tolls, not for other lawful purposes. However, information can be useful in cases of tracking serious traffic offences or monitoring activities that put public safety at risk. E.g. highway speed chases.

Although privacy principles form the basic foundation to protect individual privacy from electronic road toll system, some areas specific to electronic road toll system need to be addressed separately.

Continuous review

Privacy impact assessment must be thoroughly investigated and this process must be iterative rather than a single step (Information Privacy Principles, 2005) Punishments or a method of resolution must be consider before the implementation as well. There must be continuous consultation with the Privacy Commissioner and the government must make public aware of the process and development.

Choice

Another way to solve the privacy problem is to offer the driver an alternative choice. If some people are not comfortable travelling using the electronic road toll system, then an alternative route should be provided so that the driver can get to his/her destination. For those people who are highly concerned about their privacy, they should be given the choice not to travel on these roads.

6 Conclusion

Implementing an electronic road toll system may have privacy implications. These privacy issues can be kept under control. For instance, protection mechanism such

as PET may be involved and the government has clear privacy policies in place. It is difficult to predict the effect of an electronic road toll system in NZ before implementation, but this paper identifies possible privacy risks and benefits involved. Keeping privacy issues under control would involve continuous assessment on the progress of the project and collaboration from the involved parties especially as the technology involved further evolves.

This paper, takes a cautious view on privacy implications. Different people perceive different levels of privacy as acceptable and it is possible for some people not to be concerned about their vehicles being tracked on the tolled roads. However this discussion paper has taken the point of view, where implementation of electronic toll system brings serious privacy implications.

Therefore further research could be done to expand and elaborate on the survey and investigate people's perceptions and tolerance towards privacy issues from introduction of new information technology. The broad area of ITS (Intelligent Transportation System) can be studied to see the implications on privacy. ITS covers all aspects of vehicle tracking including distance travelled and speed. This affects privacy more than just the electronic road toll system.

7 References

407 ETC, Retrieved 17 May, 2005, from http://www.407etr.com/about/about_privacy.asp

Agre, P. (1995). Technology and Privacy in Intelligent Transportation Systems. Conference on Computers, Freedom, and Privacy, San Francisco.

Dearnaley, M (2006). Row looms over road-toll plans, The New Zealand Herald, March 13, 2006 Retrieved 8 May, 2006, from http://subs.nzherald.co.nz/category/story.cfm?c_id=194&ObjectID=10372353

Garfinkel, S. L. (1995). The Road Watches You: 'Smart' Highway Systems May Know Too Much, The New York Times, Retrieved 30 Apr, 2005, from http://www.littletechshoppe.com/ns1625/electrictoll.html

Information Privacy Principles, Retrieved 30 Apr, 2005, from http://www.privacy.org.nz/people/peotop.html.

Laudon, K. C. and C. G. Traver (2002). E-Commerce: business, technology, society. Boston, Addison Wesley.

M6toll, Retrieved 17 May, 2005, from https://secure.m6toll.co.uk/account/terms_june2005.asp.

Queensland Motorways, Retrieved 17 May, 2005, from http://www.qldmotorways.com.au/www/index.aspx?ItemID=25.

Wright, T. (1995). "Eyes on the Road: Intelligent Transportation Systems and Your Privacy." Retrieved 30 Apr, 2005, from http://www.ipc.on.ca/docs/its-e.pdf.

Young, A. (2005). Motorway toll to last 30 years.