Hi there

Please find attached the report requested. The report has been released previously by the Ministry.

Kind regards, Andrew

---

From: < >
Sent: Friday, 21 June 2019 2:03 PM
To: OCU <ocu@transport.govt.nz>
Subject: OCU request from the website

Dear MoT Officer,

Could I please have access to the MoT internal report: Broom A (September 2016) Privacy Implications of Variable Road Pricing, New Zealand Ministry of Transport

Thank you,
Privacy Implications of Variable Road Pricing

Anne Broome
for
Ministry of Transport

September 2016
Contents

Introduction......................................................................................................................... 1
New Zealander's attitudes to privacy.................................................................................. 4
Survey for the Office of the Privacy Commissioner......................................................... 4
Automobile Association member feedback........................................................................ 6
New Zealand's privacy legislation...................................................................................... 6
Privacy Act 1993.................................................................................................................. 6
Application of the Privacy Principles............................................................................... 8
Role of the Privacy Commissioner................................................................................... 8
Previous advice on privacy implications of road pricing.................................................. 9
Submission by the Privacy Commissioner on the final report of the Roading Advisory
Group 1998......................................................................................................................... 9
Draft report on privacy implications of 2003 electronic road user charging options for
heavy vehicles..................................................................................................................... 10
Potential models from home and abroad.......................................................................... 10
Conclusion......................................................................................................................... 11
Introduction

The Auckland Transport Alignment Project is likely to recommend further investigation of "variable network pricing (directly charging for road use and varying charges by location and time of day)".¹

In other jurisdictions privacy has emerged as a significant issue for road-pricing systems, particularly road pricing systems that collect information about road users' movements in place and time.

Recent surveys suggest New Zealanders are also concerned about privacy and location is an important dimension of this.

Most jurisdictions that have implemented road-pricing systems have done so in a relatively limited way, for example, within a cordon, on a particular stretch of road and/or applying to heavy commercial vehicles and not light private vehicles. In these cases, where the privacy impacts have been relatively contained, the systems are, nevertheless, subject to local privacy laws that govern what can be collected, how it must be managed and how it can be used.

For example, the London congestion charging cordon and the warm and toll road operators provide information on their websites about what information is collected, how it is used and stored, how long it is kept, and how it may be shared. In both of these examples, this transparency is required by law.

In New Zealand and some European countries, where mileage-based road-pricing systems operate for commercial vehicles, and some use satellite-based technologies to track location, personal privacy is not a concern (though issues of commercially sensitivity and concerns about surveillance of vehicles can be).

In road pricing trials that are currently underway in some states in America, for example Oregon, California and Washington where the systems are ultimately intended to replace fuel tax for private and commercial vehicles, privacy has emerged as a significant concern. This concern has been especially prominent where satellite-based systems, which track the location of vehicles, are proposed as a good technology option for implementing road pricing.

However, the road pricing systems that are being trialled in America are focused on revenue generation and there is no suggestion that they will be used "to influence travel demand patterns and improve network productivity", which is the reason for considering road pricing, particularly variable network pricing in Auckland. In the American trials (where participation is still voluntary), there is, therefore, a solution to privacy concerns, which will not be an option for variable pricing that depends on location. This involves providing options for measuring


² Ibid
distance without tracking vehicle location, and in one case, to use time-based vouchers that do not even record miles.

There is one notable exception to the idea that road pricing has only been implemented thus far in a contained ways, and that in these cases local laws have determined the approach to privacy issues. This is Singapore's congestion charging scheme, which operates across the network and applies to most private and commercial vehicles but does not incorporate any legal or business requirement for protecting individual privacy. Singapore's government agencies, including the Singapore Land Transport Authority which runs the congestion charging scheme, are not covered by Singapore's privacy laws.

New Zealand's privacy settings have much in common with other jurisdictions that have implemented road pricing and where this has required comprehensive policies to address privacy concerns, including the United Kingdom and Australia. The examples of London and Melbourne provide good models for some aspects of what will be required in New Zealand.

However, if New Zealand does implement variable network-wide road pricing for commercial and private motor vehicles, the privacy implications will be more significant than has been the case elsewhere. New Zealand will be on the cutting edge in using this approach and in addressing potential privacy impacts such as this. New Zealand's privacy framework provides a good basis for getting this right.

New Zealanders' attitudes to privacy

From March to April 2010, two separate surveys collected information about New Zealanders' attitudes to privacy. These both showed that New Zealanders, particularly younger New Zealanders, are concerned about privacy. However, people are increasingly less concerned about sharing of personal information between government agencies and more comfortable with government agencies sharing personal information than personal information being shared between businesses.

Survey for the Office of the Privacy Commissioner

The first survey was undertaken on behalf of the New Zealand Privacy Commissioner. It consisted of a telephone survey of a nationally representative sample of 761 New Zealanders aged 18 years and over.3

Information from the survey that is either generally or particularly relevant for electronic road pricing showed that:

- approximately two thirds (65%) of respondents were concerned about individual privacy and the protection of personal information

3 The margin of error for a 50% figure at the 95% confidence level for a sample of 761 is approximately ± 3.6%
- Nearly half of all respondents (46%) were more concerned about individual privacy issues over the last few years, especially younger people and people with more education.

- 81% of respondents were concerned about credit card or banking details being stolen.

- 63% of respondents were sensitive about the sharing of physical location information over time.

- 59% of respondents were concerned about government agencies sharing personal information without permission but this represents a decrease of 8% since 2014 and compare well with the 78% of people who were concerned about businesses sharing personal information with other businesses without permission.

- Factors that influence respondent's willingness to share information included:
  - reasons the information is required (66%)
  - type of personal information (87%)
  - whether or not the information will be shared with a third party (85%)
  - how securely the information is stored (82%)
  - benefits to the individual from sharing (69%)
  - anonymisation of the data (61%)
  - strict control on who can access the data and how it is used (60%)
  - ability to opt out of sharing (57%).

Automobile Association member feedback

The New Zealand Automobile Association (AA) also sought feedback from its Auckland members in the same period as the survey was done for the Office of the Privacy Commissioner. The AA received 1300 responses. They showed that:

- One-third of respondents were very concerned and one-third of respondents were a little concerned about a third party having access to information about where and when they travel.

- People were generally more comfortable with the Government accessing their private travel information than a commercial provider.

- Older respondents were generally less concerned about privacy than younger respondents.
New Zealand's privacy legislation

Privacy Act 1993

The Privacy Act 1993 (the Act) governs how government agencies, local councils, businesses and individuals can collect, use, disclose, store, retain and provide access to personal information.

New Zealand’s Privacy Act incorporates twelve privacy principles:

Principle 1
Personal information must only be collected when:
- the collection is for a lawful purpose, connected with what the agency does, and
- it is necessary to collect the information for that purpose.

Principle 2
Personal information must usually be collected from the person the information is about. But sometimes it is all right to collect information from other people instead, for instance, when:
- getting it from the person concerned would undermine the purpose of the collection
- it is necessary to a public security body can uphold or enforce the law
- the person concerned authorises collection from someone else.

Principle 3
When an agency collects personal information from the person the information is about, it has to take reasonable steps to make sure that person knows things like:
- why it is being collected
- who will get the information
- whether the person has to give the information or whether this is voluntary
- what will happen if the information isn't provided

Sometimes there are good reasons for not letting a person know about the collection, for example, if it would undermine the purpose of the collection, or it’s just not possible to tell the person.
Principle 4

Personal information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances.

Principle 5

It's impossible to stop all mistakes. But agencies must ensure that there are reasonable safeguards in place to prevent loss, misuse or disclosure of personal information.

Principle 6

People usually have a right to ask for access to personal information that identifies them. However, sometimes, agencies can refuse to give access to information, for instance because giving the information would:

- endanger a person's safety
- prevent detection and investigation of criminal offences
- involve an unwarranted breach of someone else's privacy.

Principle 7

People have a right to ask the agency to correct information about themselves, if they think it is wrong.

If the agency does not want to correct the information, it does not usually have to. But people can ask the agency to add their views about what the correct information is.

Principle 8

Before it uses or discloses personal information, an agency must take reasonable steps to check that information is accurate, complete, relevant, up to date and not misleading.

Principle 9

An agency that holds personal information must not keep that information for longer than is necessary for the purposes for which the information may be lawfully used.

Principle 10

Agencies must use personal information for the same purpose for which they collected that information.

Other uses are occasionally permitted (for example because it is necessary to enforce the law, or the use is directly related to the purpose for which the agency got the information).
Principle 14

Agencies can only disclose personal information in limited circumstances. One example is where another law requires them to disclose the information. Also, an agency can disclose information if it reasonably believes, for example, that

- disclosure is one of the purposes for which the agency got the information;
- disclosure is necessary to uphold or enforce the law;
- disclosure is necessary for court proceedings;
- the person concerned authorised the disclosure;
- the information is going to be used in a form that does not identify the person concerned.

Principle 12

Some agencies give people a "unique identifier" instead of using their name. Examples are a driver's licence number, a student ID number, or an IP number. An agency cannot use the unique identifier given to a person by another agency. People are not required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).

Application of the Privacy Principles

It will be possible to design a variable road pricing system that minimises the use of personal information. For example, a vehicle could be associated with an account, with information about the vehicle owner and the source of funds in the account being segregated until an account is in arrears must be followed up.

However, designing a system that minimises the use of personal information will not happen by chance. It can only happen by design. Nor will minimising the use of personal information eliminate the requirement to identify individuals to follow up arrears. To this extent, all of the principles of the Privacy Act apply and require due consideration.

Role of the Privacy Commissioner

The Act empowers the Privacy Commissioner to provide advice and education on privacy, investigate complaints, evaluate new legislation that may impinge on an individual's rights, review data-matching programs, and issue codes of practice. Codes of practice cover specific industries, agencies, activities, or types of personal information and often adapt the provisions of the Act to a particular circumstance, group of organisations or type of information.
The Privacy Commissioner also reports to the Prime Minister, including on matters the Commissioner considers should be drawn to the Prime Minister’s attention.

It will, therefore, be important to ensure that the Privacy Commissioner is kept abreast of road pricing system developments and provided with the opportunity to assess and contribute to solutions for privacy issues that arise as appropriate. The Privacy Commissioner may well decide that development of a code of practice in relation to road pricing systems is appropriate.

**Previous advice on privacy implications of road pricing**

Previous proposals for implementing road pricing in New Zealand have occasioned reports on the privacy implications, notably in 1988 by the then Privacy Commissioner in response to the report of the Roading Advisory Group, which had implications for all motor vehicles.

A 2003 draft report by John Edwards, the current Privacy Commissioner in his former role as a Barrister and Solicitor, was also produced on electronic road user charging (EUC) options under the RUC Act, which applied to freight and diesel powered vehicles only.

Taken together the two reports indicate that potential privacy impacts are manageable under New Zealand’s existing privacy framework but increase markedly when the system involves:

- tracking of vehicle movements
- application to private motor vehicles
- elements of compulsory

**Submission by the Privacy Commissioner on the final report of the Roading Advisory Group 1998**

The 1998 submission by the Privacy Commissioner noted “the proposed changes in road pricing may lead to the creation of an infrastructure which would allow for the tracking of all vehicle movements ... (and) have the potential to enable massive data surveillance of the movements of individuals, as vehicle owners and drivers”.

The submission also noted that:

- the proposals need not, and should not, lead to massive data surveillance of people’s movements
- the creation of infrastructure which would allow for the tracking of all vehicle movements should involve “most careful privacy assessment at each stage and the building of strong privacy safeguards – both legislative and technical”
- it is not necessary to inevitably allow compulsorily gathered data on people’s movements to become available for secondary tasks
it would be "undesirable to allow road pricing objectives to be undermined through a link to the system of massive state or private surveillance"

"privacy issues created by placing the management of existing pricing and charging systems within a commercial structure can … be satisfactorily accommodated through the proper application of the information privacy principles".

"I will wish to have a role and be consulted closely at the appropriate time."

Draft report on privacy implications of 2003 electronic road user charging options for heavy vehicles

This draft report assessed the privacy implications of enhancing the existing RUC system to provide for an electronic RUC option.

This is revealing in as much as it concluded that the privacy implications of the changes were unlikely to be significant because the proposed system involved:

• collection of little new information as a result of providing for electronic collection

• collection of little personal information. This is because much of the information would relate to the vehicle or the commercial operator and it is not a value which attaches to corporate entities. Likely vehicles will be driven by individuals and there will be elements of indirect collection of personal information but drivers undertaking paid activity on a public road as part of their employment is not a private activity.

• none of the options were predicated on the development of widespread technological infrastructure capable of responding to chips in cars or debiting commuters bank accounts or recording the movements of private vehicles

• uptake of the new system and new technology to support the new system is to be voluntary, which is an almost complete answer to many of the privacy concerns with any of the reform options. However, it was recognised that the system could ultimately become mandatory, in fact if not in law.

• if this new system was to involve an option that necessitated the centralised collection of a large volume of personal information that was not formerly collected, legislation can add a layer of protection to that information to ensure that it is used only for the purposes for which it is collected.

Potential models from home and abroad

While various jurisdictions have implemented road pricing schemes to achieve various purposes, and new developments are happening all the time, models that are relevant for New Zealand will incorporate:
• a privacy framework and legislative context that applies to government, local government and any organisation that is acting on behalf of government

• road pricing systems that apply to private motor vehicles

• compulsory collection of location information or vehicle tracking and/or require electronic payment methods.

Contexts where all three of the above apply include London, Stockholm and some Australian States. There may be other examples in other parts of Europe, where European Union directives on data privacy have been incorporated into law and location-based road pricing systems (including congestion charging and tolls that apply to private motor vehicles) have been implemented.

There may also be examples in Asia. However, Singapore, which has the most advanced price-based congestion charging system in the world, is not one of them. This is because Singapore’s privacy laws do not apply to government or public authorities, or any agency processing information on their behalf.*

The USA has a reasonable framework for the protection of individual privacy and is the location of some interesting road pricing trials. However, they do not generally require location information (or electronic payment methods).

New Zealand’s current RUC system for diesel-powered and heavy vehicles incorporates an electronic option that involves collection of location information. However, it is not compulsory to use the electronic RUC option. Considerable care was taken, nevertheless, in the drafting of the legislation about the information that is collected as part of the electronic RUC option. This was because of the potential commercial sensitivity of some of the information. Freight operators needed assurance that these sensitivities would be respected, so concerns about the use of the information did not act as a barrier to the adoption of the electronic option.

Conclusion

New Zealanders care about privacy, including privacy in relation to their location.

Network-wide direct road pricing, which requires the collection of location information and/or tracking of motor vehicles, applies to private motor vehicles, and, has happened in a context where privacy is a concern that constrains the approach, is not yet a reality anywhere in the world. Famous examples that appear to suggest otherwise include:

Singapore’s system, which applies to all vehicles and is compulsory but is run by a government agency to which Singapore’s privacy laws do not apply

- Some states in the USA, which are trialling direct road pricing for all vehicles but where participation in the trials is still voluntary and vehicle tracking is optional.

Nevertheless, New Zealand's existing privacy framework can accommodate the privacy issues that arise from direct road pricing systems that involve compulsory tracking of all vehicle movements.

The Privacy Commissioner should be kept informed about developments in relation to road pricing and be invited in a proactive and timely fashion to engage about potential privacy impacts and contribute to solutions as appropriate.