Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

21 October 2010

Mr Jon Stanhope MLA
The Chief Minister and Minister for Transport
A.C.T. Government

Dear Mr Stanhope

Re: Point-To-Point Cameras

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF has recently become aware of a report entitled 'Forward Design Study: Introduction of Point to Point Speed Cameras in the ACT', published by the Department of Territory and Municipal Services (TAMS) on 30 July 2010, at:
http://www.tams.act.gov.au/__data/assets/pdf_file/0016/204505/ACT_Forward_Design_Study.pdf

The APF has also had drawn to its attention a Media Release published on 21 September 2010 11:17 am, and entitled 'First Point-To-Point Cameras Operational By Mid 2011' (although this appears to be missing from the Media Release site at http://www.chiefminister.act.gov.au/media.php).

Some time ago, the APF published a Policy Statement relating to Automated Number Plate Recognition (ANPR) schemes generally. It is at http://www.privacy.org.au/Papers/ANPR-0803.html, and a copy is attached. The authors of the TAMS Report should have been aware of the APF's policy in the area, not least because they referred to the Queensland Parliamentary TravelSafe Committee and submissions to that Committee.

The APF is very concerned about a number of aspects of the proposals.

Those concerns are expressed in greater detail in the Submission attached to this letter.

We look forward to your response to the Foundation's Submission.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF's Board comprises professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87)
  http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90)
  http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07)
  http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-)
  http://www.privacy.org.au/Campaigns/Media/

Australian Privacy Foundation

Submission to the A.C.T. Government re Point-To-Point Cameras

21 October 2010

A. Introduction

The APF has recently become aware of a report entitled 'Forward Design Study: Introduction of Point to Point Speed Cameras in the ACT', published by the Department of Territory and Municipal Services (TAMS) on 30 July 2010, at:
http://www.tams.act.gov.au/__data/assets/pdf_file/0016/204505/ACT_Forward_Design_Study.pdf

The APF has also had drawn to its attention a Media Release published on 21 September 2010 11:17 am, and entitled 'First Point-To-Point Cameras Operational By Mid 2011' (although this appears to be missing from the Media Release site at http://www.chiefminister.act.gov.au/media.php).

Some time ago, the APF published a Policy Statement relating to Automated Number Plate Recognition (ANPR) schemes generally. It is at http://www.privacy.org.au/Papers/ANPR-0803.html, and a copy is attached.

The authors of the TAMS Report should have been aware of the APF's policy in the area, not least because they referred to the Queensland Parliamentary TravelSafe Committee and submissions to that Committee.

B. Traffic-Related Applications

The APF expresses serious concern about the proposals.

1. The ANPR Architecture being considered is not appropriate to a free society

It appears that the technology being considered is what the APF refers to as 'Mass Surveillance ANPR'. It would be highly inappropriate to deploy such technology, because it breaches privacy laws and expectations by collecting data without due cause, and for speculative reasons.

The alternatiive 'Blacklist-in-Camera ANPR' architecture described in the APF's Policy Statement and elsewhere is feasible, and appropriate to the purpose. Using this approach, no privacy-sensitive data escapes from the camera-assembly unless it relates to a vehicle on a blacklist.

2. A Privacy Impact Assessment (PIA) must precede consideration by the Assembly

It is essential that a Privacy Impact Assessment (PIA) be conducted, in compliance with the guidelines provided by the Privacy Commissioner. The APF can see no evidence that one has been undertaken.

A PIA includes the provision of sufficiently detailed information to the public, engagement with relevant advocacy organisations, and reflection of their concerns in decisions made about the design of the scheme.

A PIA will show that there is no justification for even the capture of registration data of vehicles that are not infringing the law, let alone the retention of that data, even for milliseconds, let alone a month.

3. An audit of speed-limits is essential prior to deployment

Many road-segments have inappropriate speed-limits, for reasons such as roadway improvements without subsequent review.

Traffic on such segments of roads commonly finds its own level, and driving more slowly than the norm creates tensions, frustrates drivers, and leads people to attempt overtaking manoeuvres.

It would be grossly unfair to drivers to fine them, and in a proportion of cases remove their licences, because of what are in many cases arbitrary and unfair speed-limits.

Point-to-point cameras must therefore not be implemented until after reviews of the speed-limits, and of the starting- and ending-points of speed-limits, along all relevant pathways between cameras.

C. Non-Traffic Related Applications

The APF expresses the most serious concern about the proposals.

4. No case has been made in support of any retention of data

These proposals, despite the use of the bland term 'Non-Traffic Related Offences', are for the conduct of mass surveillance of vehicle movements.

Interception of vehicles of interest is entirely dependent on:

- immediate processing of the alert, not retrospective analysis
- a police vehicle downstream from the camera
- immediate transmission of the alert to that vehicle, in order to facilitate an intercept

All of this can be achieved by means of 'Blacklist-in-Camera ANPR' architecture. Such forms of non-traffic related application do not justify the deployment of grossly privacy-intrusive 'Mass Surveillance ANPR' architecture.

The discussion in the TAMS document is in any case purely speculative.

Under no circumstances should the Government or the Assembly countenance such a proposal.

The Government should withdraw all such applications from any further consideration until and unless an evidence-based justification is published, and subjected to public scrutiny.

Australian Privacy Foundation

Automated Number Plate Recognition (ANPR)

Background

Automated Number Plate Recognition (ANPR) uses digital cameras and software similar to Optical Character Recognition (OCR) software to extract the registration data of vehicles. This can be done by pointing the camera at parked cars, but is most commonly done by deploying the camera adjacent to a road, and monitoring passing traffic. Variants have been used in most Australian States since the 1980s for heavy vehicle traffic. The technology is related to, but differs in some ways from, that used for 'speed cameras' and 'red light cameras'.

ANPR has reached epidemic proportions in the U.K., has been implemented in an uncontrolled manner, and relies on seriously error-prone underlying data. It has very serious implications for privacy, and for democratic freedoms more generally. It is crucial that Australian implementations not make the same gross mistakes as the U.K.

Until 2008, Australian Parliaments appear to have given virtually no consideration to ANPR, and law enforcement agencies have been conducting trials without guidance from their legislatures or oversight from anyone at all. (It appears that one Committee of the federal Parliament may have held hearings, but it is unclear which one it was, what information was publicly available, and who was invited. The APF wasn't).

In late 2007 and early 2008, the Queensland Parliamentary Travelsafe Committee has been undertaking an Inquiry into ANPR. This was naturally focussed on the traffic applications, rather than the broader policing and 'national security' justifications that are often advanced for ANPR. The Inquiry was conducted in an open and informative manner, and received 32 Submissions. The APF was invited to submit, and did so on 18 January 2008. The APF was subsequently invited to present verbal evidence, and did so on 14 March 2008.

This document contains the notes prepared for the Hearings. It should be read in conjunction with the APF's formal submission. See also the submission by QCCL. (The Submission by the OFPC contains material of value. The brief Submission by the OVPC swallows the unjustified assertions of the UK police, but also has some material of value in it).

APF POLICY re Automated Number Plate Recognition (ANPR)

1. **ANPR has the potential to make contributions in several areas**:

- **directly, to the enforcement of traffic administration law**:
  - Vehicles can be detected that are carrying registration plates for which the current annual payment has not been made. If resources are available to intercept such vehicles, enforcement may improve
  - Because many such vehicles are known to be driven by unlicensed drivers, this also assists in the interception of unlicensed drivers. If unlicensed drivers have a higher incidence of unpaid traffic fines, it could lead to a higher level of collection of traffic fines
- **indirectly, to traffic safety**:
  - Unregistered vehicles are known to have a higher incidence of defects, and a higher level of involvement in traffic accidents, than registered vehicles. To the extent that fewer road-miles are driven by unregistered vehicles (e.g. because they are confiscated, or miscreants are deterred from using them), there could be a reduction in traffic accidents
  - Unlicensed drivers are known to have a higher incidence of involvement in traffic accidents than licensed drivers. To the extent that fewer road-miles are driven by unlicensed drivers (e.g. because they are gaoled, or deterred from driving), there could be a reduction in traffic accidents

- **indirectly, to traffic law**. Unlicensed drivers are known to have a higher incidence of traffic offences than registered drivers. To the extent that fewer road-miles are driven by unlicensed drivers (e.g. because they are gaoled, or deterred from driving), there could be a reduction in traffic offences
- **indirectly, to policing generally, in relation to the enforcement of criminal laws**. Vehicles can be detected that are carrying registration plates that are, for example:
    - 'stolen vehicles' (i.e. reported stolen and not yet withdrawn from the list)
    - 'associated with a crime' (e.g. reported as a 'getaway vehicle')
    - associated with an individual for whom a warrant is outstanding
    - associated with an individual wanted for questioning
    - associated with a person of interest
- **indirectly, to security agencies, in relation to the exercise of powers that are in most cases excessive and inadequately controlled**. The historical patterns of movement of vehicles can be detected that are of interest to security agencies. Associations among vehicles can be detected that are of interest to security agencies. Many inferences can be loosely drawn, haystacks-full of which are likely to be wrong, and a few needles of which are potentially valuable intelligence

2. **Wild claims have been made about the potential benefits of ANPR** in some countries (not, thankfully, in Australia). Among them is the assertion by senior UK police executives that ANPR can "deny criminals use of the road". This does not stand up to any analysis. It is vital that assertions of benefits not be taken at face value, and that they be subjected to consideration, and testing.

3. **Whether the potential benefits can be achieved is questionable**. Factors include the following:

- considerable **infrastructure** is needed
- considerable human **resources** must be directed (or re-directed) to ANPR. This preferably involves teams of police committed to interception duties downstream from the detection equipment, or alternatively larger teams committed to susbequent analysis and follow-up
- the technology is known to be highly **error-prone** (in terms of missed readings and perhaps also of erroneous readings)
- the inferences drawn from detected plates are entirely dependent on **the quality of the databases** against which the registration plate data is compared. Concerns include:
    - registration databases contain errors, and timeliness of update is a particular weakness
    - stolen car lists are highly unreliable, because recovery is not reliably reported and updated
    - registration plates of interest to law enforcement and security agencies are even more unreliable in regard to their accuracy, currency and relevance
- the errors result in **'false-positives'** (i.e. detections that would not have been detections had the error not arisen). As a result:
    - the resources committed to analysis and interception have to cope with large numbers of cases to choose, it is difficult to distinguish in advance likely real-positives from false-positives, and the proportion of false-positives may result in the real-positives not being addressed
    - when an interception is made, procedures must be used to establish whether the case is a real-positive or a false-positive, which uses up more resources
    - the inference that a vehicle is being driven by the registered owner is a highly unreliable one, and hence the likelihood of a false-positive is higher, and additional procedures need to be taken to distinguish real-positives from false-positives
- only a proportion of vehicles are being driven by their registered owner, and hence **assumptions about the identity of the driver** are frequently wrong

4. Despite deployment in a significant number of countries, and ample evidence of difficulties in the technology's application to policing, **little or no independent testing has been reported, and no reliable independent assessments have been published**. There is a serious shortfall in reliable information about:

- operational error-rates of various kinds under various conditions
- database error-rates
- resource-wastage through false-positives
- the consequences of false-positives for the individuals who are the subject of the undue suspicion and/or interception

5. **As commonly practised, and as supported by currently available technologies, ANPR represents a gross privacy intrusion, and in some jurisdictions breaches privacy law**, in the following ways:

- it involves arbitrary collection of personal data not for a specific, defined purpose to which it is clearly relevant, but opportunistically and for vague purposes
- it generates a very large database of personal data, containing:
    - registration data
    - one set – but very probably multiple sets – of:
        - the date and time of sighting
        - the location
        - the direction of movement
- the database can be used to draw inferences and generate suspicions
- the database is a 'honeypot' that attracts attention from many organisations for many purposes, resulting in 'scope creep'
- the database is impossible to protect against unauthorised access, resulting in leakage of content

6. **As commonly practised, and as supported by currently available technologies, ANPR is a mass surveillance technique and breaches the human right of liberty of movement (UDHR 13.1, ICCPR 12.1**). More specifically, with conventional ANPR:

- an unknown proportion of the large data-holdings is unreliable, and there is no simple or inexpensive way of sifting the accurate from the inaccurate
- suspicions can be readily generated, some of which are reasonable and some of which are not, and there is no simple or inexpensive way of sifting the reasonable from the unreasonable
- embarrassment is created for law-abiding citizens who are intercepted on the basis of incorrect data and unreasonable suspicion
- danger is created for law-abiding citizens who are intercepted by a law enforcement officer who has been given wrong information about the possible dangerousness of the vehicle's occupants
- the deterrent effect on miscreants appears unlikely to be all that great
- the unjustified chilling effect on law-abiding citizens appears likely to be much greater than the deterrent effect on miscreants. This applies especially to the many categories of persons at risk, including victims of domestic violence, protected witnesses, celebrities, and undercover law enforcement operatives

7. **The practice of ANPR can readily become arbitrary interference by law enforcement officers**, in such ways as the following:

- undue interception of false-positives
- misunderstandings, unpleasantness and altercations between officers and vehicle-occupants
- further actions in relation to the intercepted vehicle, such as roadworthiness inspections, bookings for minor transgressions (e.g. broken light-covers and mirrors), and search on the off-chance of finding infringing materials such as drugs
- further actions in relation to the driver, such as delay, questioning and search
- further actions in relation to other vehicle occupants, such as delay, questioning and search

8. **The effects of the practice of ANPR on the public reputation of law enforcement agencies and individuals can be positive**, in that they will be seen to be active, and to be effective; **but run a great risk of being seriously negative**, in that they will be seen to be intrusive into the activities of law-abiding citizens, and a key part of a 'police state' apparatus that gathers vast quantities of information about people's movements.

9. **An alternative approach to ANPR addresses many of these issues. The 'blacklist in camera' design** involves:

- release from the on-site camera device of only those detections that match to the current 'blacklist' of registration plates that are being sought
- certified non-accessibility and non-recording of any personal data other than that arising under the above circumstances
- substantial controls over the download of the blacklist to the device and the maintenance of the blacklist
- substantial controls over the quality of data used to prepare the blacklist, and exclusion of sources of data that are of insufficient quality

10. **Considerable commitment and investment are required in order to implement the alternative approach to ANPR** in the face of the momentum that has been achieved in some countries overseas by the orthodox, grossly privacy-invasive form of ANPR.

11. **It is vital that ANPR projects be conducted in a transparent manner**, including published information, consultation, privacy impact assessment, and published results.

12. **It is vital that Parliaments expressly preclude inappropriate designs for uses of ANPR, and expressly authorise appropriate designs for and uses of it**.

Created: 17 March 2008 - Last Amended: 18 March 2008 by Roger Clarke - Site Last Verified: 11 January 2009