submission

Submission to the Queenland Parliament's –

Travelsafe Committee Inquiry into Automatic Number Plate Recognition Technology

January 2008

privacy victoria

Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission for the Travelsafe Committee Queensland Parliament Inquiry into Automatic Number Plate Recognition Technology (ANPR)

There is general consensus that ANPR technology can collect data with a high degree of accuracy and that the data can be readily integrated with other information collections created by government agencies and private sector organisations. This can be extremely useful for law enforcement purposes.

John Dean, the UK national coordinator of the ANPR system, said he understands that the widespread public use of CCTV cameras and ANPR enabled CCTV cameras is not readily accepted in many countries but he believes "it will revolutionise policing". He knows critics call it an Orwellian invasion of privacy. But he further believes that people are entitled to security and safety as they go about their normal lives.[1]

While ensuring the safety of the public is obviously a matter of public interest, there are numerous and very significant countervailing privacy issues related to ANPR that also need to be taken into account.

Since the introduction of the *Information Privacy Act 2000* (Vic) in September 2001, the Victorian community has enjoyed the privacy rights bestowed by the IPA and has come to expect protection of their personal information. Likewise, the United Kingdom, from which a number of the examples in this submission are taken, has statutory protection of privacy in both the *Data Protection Act 1998* (UK) and the *Human Rights Act 1998* (UK). Queensland has no such statutory protections, nor does it have an independent, statutory office charged with advocating for and protecting privacy, though there is some limited regulation of the public sector through administrative Information Standards. This makes it even more important that any legislative scheme to introduce ANPR into Queensland incorporate privacy protections.

This submission will attempt to address some of the privacy issues raised in the issues paper on ANPR compiled for the Queensland Travelsafe Committee.[2]

Data analysis, automation, data-matching

One of the advantages of ANPR is that data analysis is automatic but is often independent of the collection device. It generally takes place on a server or other machine at a remote location linked to the camera via a high speed line. In isolation, taking images of passing cars would not be particularly meaningful. ANPR systems are significant because of the

[1] UK Home Office/Association of Chief Police Officers – *Denying criminals use of the road – 10,000 arrests.* PA Consulting Group, London, 2004.

[2] Queensland Travelsafe Committee, *Inquiry into Automatic Number Plate Recognition Technology*. Issues Paper No. 12, October 2007.

data exchange and analysis component. Data capture can provide a one-off or ongoing list of number plates at a particular location, specific time and direction.

That list can be matched with other databases, which might include lists of expired number plates, plates on vehicles that have been reported as stolen or involved in accidents and on vehicles that are likely to be driven by someone of interest to law enforcement personnel.

Checking may be almost instantaneous. Proponents of the UK National ANPR Data Centre for example note that automated searches of several 'hotlists' by police using mobile ANPR devices typically returns results within 5 seconds, quick enough for decisions on whether investigation is required (and whether particular vehicles should be approached with extra caution).

Alternatively, the list might feed a new database, for example one that automatically bills the owners of all vehicles entering a particular precinct during a period of traffic congestion or that compares data from cameras at two locations and thereby determines that the vehicle has broken speed limits.[3]

However, while the speed and efficiency of analysis enhance ANPR's law enforcement capabilities, they also present a significant risk to privacy, as potentially ANY database could be linked to the system. This would allow almost instantaneous use of personal information for an almost unlimited number of purposes, including the tracking of individuals for reasons unrelated to law enforcement.

Moreover, such instantaneous analysis and matching compounds the potential damage caused of any inaccuracies in the data being matched, as this could lead to the wrong individual being identified as a criminal or in some other way as having "transgressed", without time for this conclusion to be checked and verified. Before any data base is linked to an ANPR system or used for any form of data matching, steps should be taken to ensure its accuracy. This includes vehicle registration and drivers licence databases, which are notoriously inaccurate.[4]

Regulatory and function creep

In practice, data collected by ANPR is a potentially rich source of information for a wide range of users. Accordingly, the information collected for a specific purpose on a short term basis can be shared with other agencies (including federal and state law enforcement bodies, welfare and tax agencies), analysed by those bodies through matching with their data sets and stored by them. This can lead to function or regulatory creep.

[3] UK Home Office/Association of Chief Police Officers – *Engaging Criminality - Denying Criminals Use Of The Road.* PA Consulting Group, London, 2004.

[4] See .Ombudsman Victoria, *Own Motion Investigation Into VicRoads Registration Practices*, June 2005, available at http://www.ombudsman.vic.gov.au/resources/documents/Own_motion_investigation_into_VicRoads_registration_practices.pdf, last accessed 24 January 2008; and Ombudsman Victoria, *Investigation into VicRoads driver licensing arrangements*, December 2007, available at http://www.ombudsman.vic.gov.au/resources/documents/Investigation_into_VicRoads_driver_licensing_arrangements.pdf, last accessed 24 January 2008;

Regulatory creep is where a system like ANPR is initially deployed and accepted by the community for a specific reason (and regulated on that basis) and then subsequently discovered to have a range of uses that were not envisaged by the community at the time of implementation.

In the UK, data derived from ANPR systems, although initially marketed as a deterrent to serious crime, has also been used for civil penalty recovery. Cameras can spot drivers speeding, making illegal turns, driving in designated bus lanes or driving into the centre of London without paying an £8 congestion charge. Violators discover that they have been caught only after they have received an infringement notice in the mail.[5]

This also violates another fundamental privacy principle, that wherever reasonable and practicable, individuals should be given notice that their personal information is being collected and the purposes for which it will be used or disclosed.

Aggregation of data

Other concerns about ANPR centre on the aggregation of data in large, consolidated ANPR networks. The UK National ANPR Data Centre for example has faced criticism because it will centralise ANPR data from 43 police forces in England and Wales, drawing on several thousand cameras. A database in north London will hold the details of millions of British drivers' journeys as recorded by thousands of ANPR camera systems seeded on motorways across the country. City-centre and filling station cameras are also being integrated into the system. The database is stored in a National ANPR Data Centre next to the Metropolitan Police training centre in Hendon. Some 35 million number plates will be recorded each day with details of the time and location. This provides authorities with the time, date and precise location of vehicles as camera sites are also linked to global positioning satellites.[6] This will mean that it will no longer be possible to travel on a road anywhere in Britain without being surveilled.

Moreover, such a large, aggregated collection of data is itself extremely attractive to those seeking to put it to criminal or unlawful uses. This means that access and security controls on the data need to be extremely high. This is extremely difficult to achieve if, as in the UK, the system is used by a range of agencies for a variety of different purposes.

Retention of data

Another concern over ANPR systems is the period for which data collected will be retained. In the UK, the government has announced that all data collected, even where no illegality or impropriety is revealed, will be retained in a "live, searchable system" for a period of at least two years, which can be extended to six years or longer.[7] The longer

[5] UK Home Office/Police Standards Unit - *Thematic Review of the Use of Automatic Number Plate Recognition within Police Forces.* PA Consulting Group, London, 2006.
[6] UK Home Office/Police Standards Unit - *Thematic Review of the Use of Automatic Number Plate Recognition within Police Forces.* PA Consulting Group, London, 2006.
[7] See Association of Chief Police Officers, Automatic Number Plate Recognition (ANPR), ACPO National ANPR User Group, ***E.C.H.R., Data Protection & RIPA Guidance Relating to the Police use of A.N.P.R.*** *(Excluding speed enforcement devices) "Denying Criminal the Use of the Road"*, October 2004, available at

data is retained, the more risk there is of security breaches and function or regulatory creep.

Management of data misuse

In Australia it is likely that *CrimTrac* will provide a national clearing house that features information from discrete ANPR networks maintained by the Australian Federal Police, the state police forces and other agencies. There are serious concerns as the extent to which statutory privacy protections apply to CrimTrac. While the agency itself is subject to the federal *Privacy Act 1988*, some of the jurisdictions who provide data and have access to the personal information held by it, including Queensland, do not have statutory privacy protections. While misuse of personal information may amount to a breach of the agreements between jurisdictions by which CrimTrac was established, this does not provide any redress for an individual affected.

These privacy concerns are further compounded by the fact that large databases, particularly those accessed by a wide range of users with varying enrolment, access and security protocols and controls, are susceptible to both abuse and inaccuracy.[8]

Conclusion

In essence, ANPR combined with camera networks turns a number plate into an ID number. The whole concept of an individual's right to anonymity is sacrificed: it is no longer possible to drive on a public road anonymously, even if one is doing nothing wrong. Moreover, depending on the databases linked to the system, the uses of personal information can go well beyond law enforcement and policing the roads.

In order to balance the potential privacy risks with the acknowledged potential benefits of an ANPR system, I recommend that the scheme be established by specific legislation which:

- Identifies specific, limited purposes for which the data collected can be used and disclosed;
- Identifies specific, limited agencies and organisations to whom disclosures can be made;
- Imposes strict limits on the period for which data can be retained;
- Imposes severe penalties for misuse; and
- Establishes a regulatory system, incorporating a complaints scheme by which individuals affected can seek redress

HELEN VERSEY
Victorian Privacy Commissioner

http://www.spy.org.uk/spyblog/acpo_anpr_hra_dpa_ripa/EHCR%20DP%20&%20RIPA%20Oct%202004.doc, last accessed 24 January 2008;

[8] See note 4, above*;*