Australian Government

Office of the Privacy Commissioner

Inquiry into Automatic Number Plate Recognition Technology

Submission to the Queensland Parliamentary Travelsafe Committee Issues Paper No.12

February 2008

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988* (Cth) (the Privacy Act), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

Background

2. The Office welcomes the opportunity to make a submission to the Queensland Parliamentary Travelsafe Committee's Issue Paper 12 ('the Issues Paper') released for the purposes of its *Inquiry into Automatic Number Plate Recognition Technology* ('the Inquiry').
3. The Office notes the purpose of the Queensland Parliamentary Travelsafe Committee ('the Travelsafe Committee') is to monitor, investigate and report on all aspects of road safety and public transport.
4. In terms of this Inquiry, the Travelsafe Committee is seeking, among other matters, to investigate and report on the effectiveness of using Automatic Number Plate Recognition (ANPR) technology for road safety applications and what role ANPR enabled teams should play in enforcement of traffic law. It is also intended that the Inquiry should report on what other opportunities and considerations arise for the use of ANPR by Queensland Government agencies to promote road safety.

About this submission

5. In this submission, the Office notes the general discussion of privacy provided in section 12 of the Issues Paper, 'Data Management and Privacy'. The Issues Paper explains that privacy plans are being developed for the proposal, though no detail is provided.
6. Further, in making this submission, the Office has been mindful of the broader environment, particularly in regard to moves towards national interoperable ANPR systems. In particular:
    - CrimTrac received funding in mid-2007 to "...identify a strategic approach to integrate ANPR technology across Australia, identifying

the necessary infrastructure and associated cost benefits analysis";[1] and

- the Australian Parliament Joint Standing Committee on the Australia Crime Commission recommended in its September 2007 report into *The future impact of serious and organised crime on Australian society* that "...the Commonwealth, state and territory governments implement a national number plate recognition system."[2]

7. The Office notes that such a national approach will raise a number of privacy issues that would need to be considered. These include, but are not limited to, the need for consistency in protections afforded to personal information exchanged between different jurisdictions, and what rules or protocols will govern such exchanges.
8. Further, in making the following comments in the is submission, the Office recognises that privacy is not an absolute right. It is a right that must be balanced against other important social interests such as the safety and security of the community.

Application of the Privacy Act to ANPR

9. As noted above, the Privacy Act regulates Australian and ACT Government agencies. It does not regulate state or Northern Territory agencies, including their respective police services. In general, most state police services are not subject to state based statutory privacy regulation (or where such legislation exists, it may not extend to 'operational requirements'). In some jurisdictions, police services may be covered by state based administration schemes that establish privacy protections. However, it should be noted that such administrative arrangements do not create statutory rights and remedies for individuals whose privacy may be interfered with.

Queensland Government agencies

10. The Issues Paper notes that Queensland Government agencies are covered by a privacy scheme set out in *Queensland Government: Information Standard 42 - Information Privacy* (the Information Privacy Standard), which contains principles based on those in the Privacy Act that regulate Australian Government agencies
11. In terms of law enforcement agencies, section 1.2.1 of the Queensland Government Information Privacy Standard states that these agencies "are exempt from IPPs 2, 3, 8, 10 and 11 for all functions except administrative functions".[3] Collectively, these exemptions obviate the

[1] This funding was provided by funds confiscated under the *Proceeds of Crime Act (2002)*; see, http://www.crimeprevention.gov.au/agd/WWW/ncphome.nsf/Page/POCA_funding_for_Non-Government_Agencies.

[2] See recommendation 19, available at http://www.aph.gov.au/Senate/committee/acc_ctte/organised_crime/report/b02.htm.

[3] Queensland Government Chief Information Office (2001) Information Standard No.42: Information Privacy, Brisbane: Queensland Government.

need to provide individuals with notice that their personal information has been collected, as well as removing limits on how personal information may be used or disclosed.

Private sector organisations

12. The Issues Paper expressly identifies, in section 5, the possibility of ANPR being used by private sector organisations.
13. In this regard, it should be noted that the Privacy Act applies to private sector 'organisations' with a turnover of more than $3 million, as well as to all private sector health service providers and to businesses that trade in personal information, regardless of turnover.
14. Accordingly, the handling of personal information collected by organisations using ANPR may be regulated by the 10 National Privacy Principles (NPPs) prescribed in schedule 2 of the Privacy Act.
15. These requirements include that:
    - any collection must be reasonably necessary for defined purpose;
    - reasonable steps must be taken to provide individuals with notice of certain things, including why their information has been collected and to whom it may be disclosed;
    - once collected, the personal information may generally only be used or disclosed for the purpose for which it was collected, unless a prescribed exception to this principles applies; and
    - personal information must be handle securely and destroyed when no longer required.
16. The Office submits that if it is envisaged that ANPR data will be exchanged between private sector organisations and Queensland Government agencies then consideration should be given to how the NPPs may apply to such exchanges.
17. Further information on the obligations established under the NPPs is available in the Office's *Guidelines to the National Privacy Principles*, available at http://www.privacy.gov.au/publications/nppgl_01.html.

Personal information and ANPR technology

18. The protections afforded by the Privacy Act, as well as the Queensland Information Privacy Standard, extend to data that is 'personal information'. Under the Privacy Act, personal information is information or opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained.[4]

[4] See Section 6 of the Privacy Act "*personal information* means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".

19. Accordingly, a key issue in regard to ANPR technology and information privacy is whether or not licence plate numbers could be considered 'personal information'.

20. In the Office's view, licence plate numbers, when collected by government authorities with the means to link those numbers to individual's names and addresses, would likely be personal information. This is because the individual's identity could be reasonably ascertained in many circumstances.

21. This view is further supported where the Issues Paper expressly states that images will be taken of both the number plates and the occupants of the vehicle. Given, that the occupants (including passengers) are also recorded, it is more likely that the number plate would be personal information as the linking of the two sets of information significantly increases the possibility of the identity of the individual being 'apparent' or reasonably ascertainable' from the information at hand.

22. Accordingly, in considering the ANPR proposal, the Office submits that consideration should be given as to how appropriate privacy protections can be afforded to the handling of this personal information.

Preliminary matters for consideration

23. The Office submits that before implementing proposals that may affect the privacy of individuals' personal information, careful consideration should be given to a number of key questions. These include:

24. **What are the objectives of the proposal?** For example, the Issues Paper presents a range of matters for which ANPR technology might, to varying degrees, be useful. Before progressing to implementation, it would be important to clarify the primary objectives of using such technology. As well as facilitating good policy decision making, this clarification would also ensure that the technology can be subject to effective post-implementation review; without clearly stated objectives, it is difficult to assess whether a project has been successful.

25. **What are the risks of the proposal?** Such risks should extend beyond financial costs, and could include risks such as the potential for a loss of community trust and confidence in public bodies through unnecessary surveillance or the mishandling of personal information.

26. **Is the proposal a proportionate response to the problem?** For example, in regard to ANPR, it would seem appropriate to consider whether the routine, broad scale collection of personal information about large numbers of individuals is an appropriate response to the scope of the identified problem.

27. **Are there alternate and less-intrusive ways of achieving the same objectives?** For example, in various places, the Issues Paper suggests that ANPR could be used to identify speeding vehicles. However, it is unclear what advantage ANPR would have over normal speed cameras. In a privacy context, these cameras have the advantage of only recording vehicles committing an offence, rather

than routinely collecting information on all passing vehicles and their occupants (driver and passengers).

28. The Office suggests that a Privacy Impact Assessment (PIA) could be a valuable tool in considering these types of questions.

Privacy Impact Assessments

29. A Privacy Impact Assessment is an assessment tool that describes in detail the personal information flows in a project, and analyses the possible privacy impacts of the project. A PIA may do this by helping an agency to identify when the collection of particular information is unnecessary for a given project, or where accountability or oversight processes may reduce privacy risks. The elements that make up a PIA (including identification, analysis and management of privacy risks) help agencies to drive good privacy practice and underpin good public policy.

30. The over-arching benefit of a PIA is that it will identify and analyse privacy impacts during a project's design phase, which in turn assists agencies to determine the appropriate management of any negative privacy impacts.

31. The example of the Canadian Longitudinal Labour Force File Databank project illustrates the risks of not comprehensively considering privacy issues before implementation.[5] In that case, community privacy expectations were not addressed during development of an information handling system and led to the dismantling of a national database on 34 million Canadians (at a cost of many millions of dollars) and a greater appreciation of the need for "…transparency and accountability, and the application of privacy-protection rules for the use of such information".[6]

32. Accordingly, the Office suggests that a PIA be conducted before any widescale implementation of ANPR technology as a way of identifying and defining the purposes and scope of such an initiative. As part of conducting the PIA, it be would necessary to describe and map the flows of personal information, determine where privacy risks exist and consider options to improve privacy outcomes.

33. The Office has produced guidance material on conducting PIAs, which is available at http://www.privacy.gov.au/publications/PIA06.pdf.

34. The Office has proposed a number of matters below that might usefully be considered as part of any PIA.

---

[5] Human Resources Development Canada (2000) *Media Release: HRDC Dismantles Longitudinal Labour Force File Databank* 29 May [available at http://www.hrsdc.gc.ca/en/cs/comm/news/2000/000529_e.shtml]; *Wired News Report* (2000) 'Canada Scraps Citizen Database' 30 May [available at http://wired.com/news/politics/0,1283,36649,00.html].

[6] Bennet C and Raab *The Governance of Privacy: Policy instruments in global perspective* (2003) Ashgate, London: p.115.

ANPR technology and the collection of personal information

35. While the Office recognises the important policy objective of improving road safety, the collection of large amounts of data can also present significant risks for individuals, agencies and organisations. ANPR can result in the routine collection of the personal information of large numbers of people. For many of these people, there may be no cause for suspicion and hence no reason to collect information about them.

36. A widespread ANPR system may permit government agencies to track a large number of vehicles (and individuals), revealing where individuals have been, when and potentially with whom. Other than in specific circumstances, this does not seem to be information that government agencies would routinely need to know about members of the community.

37. The privacy risks of this form of routine surveillance may be further exacerbated where data collected for ANPR purposes is combined with other databases, either in the public or private sectors. Such combinations may form rich 'data trails' that reveal much about individuals' behaviour, including behaviour that is not unlawful. The collection and recording of such information regarding individuals going about their day to day lives may not meet the expectation many in the community may have in terms of interacting in society free from unnecessary and intrusive surveillance.

38. Accordingly, the Office suggests that clear distinctions should be drawn between the routine use of ANPR to collect information about all individuals, and the storage of personal information about identified 'persons of interest'. Whereas the latter may be justifiable where such measures are subject to appropriate oversight and accountability (such as requiring authorisation from a senior public servant and limited to more serious offences), it seems more difficult to offer justification for the former. In this regard, the Office has noted the view of the Queensland Police Minister, the Hon Judy Spence MP, that the application of ANPR technology in the Northern Territory had "...created a lot of data without a clear use".[7]

39. This highlights the importance of clearly defining the purposes of ANPR to ensure that the scope of its application is limited to individuals who are suspected of having committed an offence, either against road laws or other criminal matters.

40. The overseas experience regarding surveillance and ANPR, particularly in terms of law enforcement agencies in the United Kingdom (UK), is informative and relevant in this regard.[8] It has been

[7] *Drive* 'Qld police may get number plate trackers' 31 October 2007, available at http://www.drive.com.au/Editorial/ArticleDetail.aspx?ArticleId=45143.

[8] The use of ANPR in the United Kingdom is discussed in *The Guardian* 'Surveillance on drivers may be increased' 7 March 2006, available at http://www.guardian.co.uk/transport/Story/0,,1725229,00.html; The Independent

reported that it is anticipated that ANPR databases in the UK would soon be collecting and storing around 35 million images per day and stated that they planned to keep this data for two years. Further, the ANPR data that is collected is not only mined and matched with a number of databases, but also then stored for future use. The Office would caution against establishing infrastructure that could used in such an expansive and invasive manner.

Accuracy of personal information collected using ANPR

41. The Office understands that the accuracy of information collected using ANPR technology can vary depending on a range of factors, including the actual technology employed and the prevailing conditions where it is used. The Office also notes that overseas experience has suggested that data held by relevant authorities may not always be precisely accurate.

42. Accordingly, ANPR should be accompanied by measures that ensure individuals have rights of review in regard to decisions that are made using information collected by ANPR. Such rights should be accessible and able to be exercised in a timely way that minimises inconvenience and burden. This is particularly the case where ANPR may be disclosed to or linked with other databases, with potentially significant consequences for the individual.[9]

43. Further, unless assurances can be offered regarding the accuracy of personal information collected by ANPR technology, it may be appropriate for it not to be employed for matters that have less significant public benefits, such as relatively minor offences, for example parking offences.

The Potential for 'function creep'

44. 'Function creep' describes the process of incremental expansion in the purpose for which a system is used, to the point that it is employed for purposes that were not initially agreed to or envisaged. Such expansion is generally organic in nature and lacks overall direction, planning or oversight. Individuals may not expect these incremental uses nor consider them appropriate.

45. As suggested by the Issues Paper, the use of ANPR has many current and potential uses in the private sector from car park monitoring to

'Surveillance UK: why this revolution is only the start' 22 December 2005, available at http://www.independent.co.uk/news/science/surveillance-uk-why-this-revolution-is-only-the-start-520396.html; *The Register* 'No hiding place? UK number plate cameras go national', 24 March 2006, available at http://www.theregister.co.uk/2005/03/24/anpr_national_system/.

[9] The Australian Government Information Management Office has released better practice guidance for the use of automated assistance in administrative decision making, see, http://www.agimo.gov.au/publications/2007/february/aaadm.

motorway toll systems. Further, in the public sector, there is potential for building large databases of personal information if these systems are linked to the personal information contained in motor registry and other databases.

46. The Office notes concerns by some that there may be inadequate or inconsistent regulation that ensures transparency about how this technology is applied, and how the data collected will be used in the future.[10] Without such regulation and oversight, given the potentially wide applications of ANPR, what begins as a technology to identify unregistered vehicles may, over time, come to be used for a variety of surveillance and law enforcement purposes. Some of these purposes may go beyond that which the community expects or is comfortable.

47. Notably, the Office makes a distinction between function creep and the exercise of a considered, deliberate and appropriate decision to change the manner for which something is used. The Office does not suggest that further uses should never be accommodated, rather that any such expansion should be subject to appropriate scrutiny so as to remain within community expectations.

48. Therefore, to reduce the possibility of function creep, the Office suggests that:

- the collection and retention of personal information should be limited to that which is necessary to achieve clearly articulated purposes. For example, the circumstances or offences where information is collected should be prescribed so that information is only collected or retained for that purpose, with personal information about other individuals either not being collected, or deleted as soon as possible; and
- the potential uses of information collected using ANPR should be clearly articulated in enabling legislation. Should additional compelling public interests be served in the future by new applications of ANPR, these should only be pursued after public consultation and the scrutiny of parliament. Such an approach reduces the risk of incremental and unplanned expansion in the use of ANPR, instead requiring a careful and transparent deliberative process.

Cross-jurisdictional data sharing in law enforcement contexts

49. As noted earlier, given the apparent momentum toward national interoperable ANPR systems, the Office believes that it is useful to consider the proposal in its broader context, rather than in isolation.

50. While formal findings in this regard may be beyond the terms of this current Inquiry, the Office would highlight the need to ensure that there

[10] Clarke, Roger & Wigan, Marcus 'Social Impacts of Traffic Surveillance' *Prometheus* 24, 4 (December 2006)

are clear rules, protocols or laws determining the circumstances when personal information collected using ANPR may be exchanged with other jurisdictions.

51. For example, personal information shared with other jurisdictions should be afforded equivalent protections in those jurisdictions to that which may apply in Queensland.

52. Such measures also should establish clear accountability and oversight for the sharing of information between jurisdictions. This could usefully include such measures as complaint handling mechanisms and remedies for individuals for individuals whose privacy may be interfered with.

Possible privacy law reform and implications for ANPR

53. On 31 January 2006, the Australian Law Reform Commission received Terms of Reference from the Australian Government Attorney-General for an inquiry into the extent to which the Privacy Act and related laws continue to provide an effective framework for the protection of privacy in Australia.

54. In December of 2007, the Office published its response to the ALRC's *Review of Privacy - Discussion Paper 72* (ALRC DP72).[11] In this response to ALRC DP72, the Office discusses the privacy issues raised by the use of technologies, such as ANPR, that involve large-scale data collection and surveillance.

55. While the Office recognises that some applications of new technology will serve valuable public interests, a number of potentially significant privacy risks emerge from technology that permits the large scale collection of personal information. For example, APNR can be a form of routine and indiscriminate surveillance of large numbers of people in public spaces. For the vast majority of these people, there would be no cause for suspicion that they have committed an offence and hence no reason to collect information about them. This raises challenges for policy makers as to when such measures are justified and proportionate.

56. The Office submitted to the ALRC that while the principle based regulation provided by the Privacy Act remains generally appropriate, consideration should be given to developing additional specific privacy protections (in the form of binding 'codes') where new technologies, or new applications of existing technology, raise particular privacy issues.

[11] "*Submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72*" December 2007, available at http://www.privacy.gov.au/publications/alrc211207.html.

Recommendations

57. In terms of providing recommendations to this inquiry the Office would offer the following:

    a. The potential application of ANPR technology should be considered with regard to the broader environment for such technology in Australia, particularly moves toward national interoperability of ANPR systems.

    b. ANPR technology should only be introduced where

        - There are clearly defined purposes;
        - Privacy risks and other risks have been fully considered;
        - It is determined that these same objectives cannot be met using alternate and less invasive means; and
        - the use of the technology and its impact on individual privacy constitutes a proportionate response to the problem being addressed.

    c. The introduction of new ANPR technology should be subject to a thorough Privacy Impact Assessment, as part of developing underpinning legislation.

    d. The risk of function creep should be managed by:

        - clearly defining the purposes of ANPR technology, and limiting any uses or disclosures to what is reasonably necessary to meet those purposes. To provide for any future purposes that may serve important public interest, a deliberative process should be set out that includes public consultation and parliamentary scrutiny;
        - only the minimum necessary personal information should be collected that is necessary to achieve the stated purposes; and
        - personal information collected on individuals not suspected of committing an offence should be deleted as soon as possible.