CONTENTS

1 SUMMARY 252

2 IDENTIFYING BENEFITS 253

3 REALISING BENEFITS 262

4 BENEFITS REALISATION FRAMEWORK 264
   4.1 Governance and evaluation 264
   4.2 Business change manager group 264
   4.3 Business change manager group deliverables 265
   4.4 Membership 265
   4.5 Benefits realisation management strategy 265
   4.6 Benefits review process 268

5 CONCLUSION 269
1 SUMMARY

Implementing a national ANPR capability is a major long-term programme of national change that requires a strategic approach. It will benefit every Australian by enhancing community safety, but particularly by enhancing road safety and increasing crime prevention and detection. A national ANPR approach will enhance capability and responsiveness across all law enforcement and road transport agencies, and has further potential to benefit the health sector through reduced road trauma and reduce insurance premiums for the community.

Part 1 of this report discusses a range of strategic change drivers for implementing a national ANPR capability. These change drivers inform Part 4 of the report, which examines the nationally agreed business requirements that, through a national ANPR capability, would enable participating agencies to meet their strategic objectives. Strategic objectives relating to this initiative are:

- enhanced community safety
- improved whole-of-government efficiency and community benefits.

Stakeholders identified the following five benefits and agreed they would help achieve the above strategic objectives:

- improved whole-of-government coordination
- financial/cost efficiencies
- enhanced road safety
- increased crime detection
- improved national security.

CrimTrac then consulted with key stakeholder agencies and identified a further 67 intermediate benefits. Thirty-eight of these have been agreed as being key intermediate benefits that will be measured and reported on.

This scoping study report recognises that delivering capability alone will not help realise benefits and that a deliberate programme of change is required to do this. Accordingly, CrimTrac has developed a benefits realisation framework, which includes defined roles, responsibilities and mechanisms for measuring, optimising and realising benefits.

The strategic objectives of enhancing community safety and improving whole-of-government efficiency are influenced by government policy, reform processes and agency activities at many levels. The benefits realisation framework recognises external influences and seeks to qualify and quantify benefits realised directly through the change process. In addition, the framework provides a mechanism to identify whether the expected benefits are being realised. This, in turn, can inform decision makers on whether to continue with or alter implementation strategies and plans.
2. IDENTIFYING BENEFITS

Following workshops that agreed on a set of national business requirements (see Part 4), CrimTrac led a series of whole-of-government workshops involving all law enforcement and road transport agencies to define and map expected benefits.

The workshops enabled the identification of benefits expected by all stakeholders. Strategic change drivers identified in Part 1 of this report were the starting point for developing an outcome relationship model which, in turn, supported the development of a benefits map. Insights gained from this supported the production of benefit profiles. This process is shown in Figure 10.1.

Figure 10.1 Process for producing benefit profiles

The benefit profiling process within the ANPR programme is to be iterative. Broad or immeasurable benefits will firstly be broken down into more specific benefits so that the whole profile can be completed. A benefit is a measurable improvement resulting from an outcome perceived as an advantage by one or more stakeholders. A benefit that cannot be measured cannot be tracked as part of management or review. As part of the profiling process, each benefit must be reconsidered and redefined or broken down further so that it can be quantified. If it is not possible to clearly define and quantify a benefit, it will not be considered any further.

In developing the benefits map, CrimTrac captured a wide range of benefits from workshop discussions. Stakeholder agencies were then asked to determine which benefits were strategically important to their agency. Where an agency considered a benefit to be strategically important, it was noted as a key intermediate benefit and was retained in the benefit map. All other benefits were discounted from further consideration.

The ANPR benefits map, which represents capability change, and key intermediate and end benefits is shown in Figure 10.2.

---

1 The use of the term 'ANPR programme' or 'programme' is used to describe any implementation activities associated with delivering a national ANPR capability. CrimTrac uses MSP® (Managing Successful Programmes) methodology in implementing complex reforms that require benefits realisation.
### Figure 10.2 ANPR Benefits Map Critical Path

<table>
<thead>
<tr>
<th>Strategic Requirement</th>
<th>Business Requirement Change</th>
<th>Key Intermediate Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture vehicle sightings in real-time and detect vehicles of interest</td>
<td>Build national infrastructure to support operations, detection and generation of alerts</td>
<td>Nationally accessibles databases enabling ANPR data capture, sharing and use</td>
</tr>
<tr>
<td>Share nationally, information associated with vehicles of interest sightings, warnings and associated airmen and regulations/licensing data</td>
<td>Ability to analyze real-time and generate time series of vehicle sightings and associated airmen and regulatory agencies</td>
<td>Enhanced standards for national ANPR system and technical architecture</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Disk (including --;military); --</td>
<td>Reduced cost for procurement of ANPR hardware</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Increased data capture</td>
<td>Increased data capture</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of unregistered vehicles</td>
<td>Greater detection of unregistered vehicles</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of unknown vehicles</td>
<td>Greater detection of unknown vehicles</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of unlicensed drivers</td>
<td>Greater detection of unlicensed drivers</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of speeding offenses</td>
<td>Greater detection of speeding offenses</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of heavy vehicle related offenses</td>
<td>Greater detection of heavy vehicle related offenses</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of stolen vehicles</td>
<td>Greater detection of stolen vehicles</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of stolen vehicles</td>
<td>Greater detection of stolen vehicles</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Increased driver satisfaction and compliance</td>
<td>Increased driver satisfaction and compliance</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater efficiency in investigations (criminal, military and serious crime)</td>
<td>Greater efficiency in investigations (criminal, military and serious crime)</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>More accurate data gathering and analysis</td>
<td>More accurate data gathering and analysis</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Increased driver satisfaction and compliance</td>
<td>Increased driver satisfaction and compliance</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater efficiency in investigations (criminal, military and serious crime)</td>
<td>Greater efficiency in investigations (criminal, military and serious crime)</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of unregistered vehicles</td>
<td>Greater detection of unregistered vehicles</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater detection of unregistered vehicles</td>
<td>Greater detection of unregistered vehicles</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Increased driver satisfaction and compliance</td>
<td>Increased driver satisfaction and compliance</td>
</tr>
<tr>
<td>Ability to integrate data and vehicle movements</td>
<td>Greater efficiency in investigations (criminal, military and serious crime)</td>
<td>Greater efficiency in investigations (criminal, military and serious crime)</td>
</tr>
</tbody>
</table>

---

**Note:** The diagram and text are from a source not fully visible due to the cropping of the image. The information provided is a compilation of visible parts of the document.
Table 10.1 shows all key intermediate benefits, with relevant agencies notation, against benefits which are deemed of strategic importance.

### Table 10.1 Agency Based Business Benefits Matrix

<table>
<thead>
<tr>
<th>BUSINESS BENEFITS</th>
<th>WA</th>
<th>NSW</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capability Change</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nationally consistent legislation enabling ANPR data capture, sharing and use</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Ministerial arrangements for national ANPR data use</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Established standards for national ANPR system and technical architecture</td>
<td>x</td>
<td>x x</td>
</tr>
<tr>
<td><strong>Business Change</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data consistency across jurisdictions</td>
<td>x</td>
<td>x x</td>
</tr>
<tr>
<td>National panel of ANPR vendors</td>
<td>x x x</td>
<td>x x</td>
</tr>
<tr>
<td>Nationally agreed business requirements for system capability</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Increased data quality</td>
<td>x x x</td>
<td>x</td>
</tr>
<tr>
<td>Reduced cost for procurement of ANPR hardware</td>
<td>x x</td>
<td></td>
</tr>
<tr>
<td>Improved protection of critical infrastructure sites through level of ANPR coverage</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Greater detection of unregistered vehicles</td>
<td>x x x</td>
<td>x x</td>
</tr>
<tr>
<td>Greater detection of uninsured vehicles</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>Greater detection of unlicensed drivers</td>
<td>x x</td>
<td></td>
</tr>
<tr>
<td>Greater detection of speeding offences</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>Greater detection of heavy vehicle fatigue related offences</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>Greater heavy vehicle route compliance</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>Improved fatigue management</td>
<td>x</td>
<td>x x</td>
</tr>
<tr>
<td>Increased up take of vehicle registration</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Increased road safety compliance</td>
<td>x</td>
<td>x x</td>
</tr>
<tr>
<td>Increase number of infringement notices issued</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Increased monitoring of heavy vehicles and dangerous good vehicles</td>
<td>x x x</td>
<td>x x</td>
</tr>
<tr>
<td>Reduced fatal crashes</td>
<td>x x x</td>
<td>x</td>
</tr>
<tr>
<td>Reduced crashes involving serious injury</td>
<td>x x</td>
<td>x x x</td>
</tr>
<tr>
<td>Reduced car insurance premiums</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

256
<table>
<thead>
<tr>
<th>SA</th>
<th>NT</th>
<th>QLD</th>
<th>TAS</th>
<th>VIC</th>
<th>ACT</th>
<th>CWLTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLICE</td>
<td>DPI</td>
<td>POLICE</td>
<td>MR</td>
<td>TRANSPORT</td>
<td>POLICE</td>
<td>DIER</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>BUSINESS BENEFITS</td>
<td>WA</td>
<td>NSW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----</td>
<td>------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduce damages to road infrastructure</td>
<td>x</td>
<td>x x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased mass distance charging</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater detection of stolen vehicles</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater detection of vehicles of interest to law enforcement agencies</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased detection of offences</td>
<td>x</td>
<td>x x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater efficiency for investigations (general, major and serious crash)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased deterrence to criminal activity</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced investigation times [specified offences]</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater offence clearance rate</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased accuracy of trip times</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased verification of vehicle movements</td>
<td>x x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased visibility of vehicle movements</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater detection of crime patterns</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater efficiency in targeting of offenders</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater efficiency in delivering services to enhance community safety</td>
<td>x</td>
<td>x x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduction in crime</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased opportunities for intra-jurisdiction enforcement activities</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased ability to derive intelligence</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More accurate data regarding traffic flows</td>
<td>x</td>
<td>x x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater counter security and counter intelligence assessments</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater operational security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increase in average on-time running of public transport</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater efficiency of transit times</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Efficient public transport systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased opportunities for cross jurisdictional collaboration</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased success in collaborative law and traffic enforcement</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA</td>
<td>NT</td>
<td>QLD</td>
<td>TAS</td>
<td>VIC</td>
<td>ACT</td>
<td>CWLTH</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>POLICE</td>
<td>POLICE</td>
<td>POLICE</td>
<td>MR</td>
<td>TRANSPORT</td>
<td>POLICE</td>
<td>DIER</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BUSINESS BENEFITS</td>
<td>WA</td>
<td>NSW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased opportunities for cross-agency and cross-jurisdictional learning</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased monitoring capability</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased origin destination survey data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased national saturation of ANPR technology</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Faster procurement time</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased data capture</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased access to data holdings</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>'Real time' access to intra and inter jurisdictional data</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater detection of offences relating to non-transfer of licence and registration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced unregistered vehicles on roads</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced uninsured vehicles on roads</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased identification of offenders</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced disqualified drivers on roads</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduction in non-compliance rates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased up take of vehicle insurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced levels of road traffic accident casualties at hospitals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater detection of stolen number plates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduction in retrieval time for stolen vehicles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduction in number of stolen vehicles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater efficiency for surveillance teams through greater time on 'target'</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased point-to-point surveillance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased ability to effectively deploy resources in response to intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More accurate planning of road networks/development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More accurate scheduling of public transport</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The ANPR implementation programme’s approach to programme management is based on Managing Successful Programmes (MSP™), a sibling to the PRINCE2™ method that underpins the CrimTrac Project Management Method (PMM).

The ultimate success of a programme is judged by its ability to realise business benefits. There is a fundamental difference between delivering a new capability and actually realising measurable benefits as a result of implementing and embedding that capability. To ensure that benefits realisation is managed appropriately, CrimTrac will implement the role of business change manager.

Business change managers will be responsible for realising benefits by embedding new and/or enhanced capability into business operations. The role of a business change manager is primarily benefits-focused. The business change manager is responsible, on behalf of the senior responsible officer, for defining the benefits, assessing progress towards realising the benefits, and achieving measured improvements.

Business change managers are an important catalyst for change, and must actively work to embed new capabilities, while retaining operational responsibilities for business-as-usual activities.

The need to define and realise benefits in terms of measured improvements in business performance means that business change managers must be ‘business-side’ in order to provide a bridge between the ANPR programme and business operations.

Due to the number of business areas targeted for benefits realisation, the scale and complexity of the proposed changes, and the nature of this programme’s benefits hierarchy, multiple business change managers would need to be appointed. The appointments would be across Australian Government and state and territory agencies to ensure business understanding, ownership and adoption of change brought about as part of the ANPR programme, and commitment to it.

To coordinate the work of business change managers, the ANPR programme will include the role of coordinating business change manager. Broadly, the coordinating role is to act as a bridge between the ANPR programme and business change managers representing agencies/organisations affected by the changes brought about by the program.

Figure 10.3 shows the business change manager model.
Figure 10.3 Business change manager model

Depending on the complexity of change required at an agency and state level, a number of additional business change managers or teams may be required. At a state level, where there will be significant change process, a state business change manager would oversee the appointed agency business change managers. Where change is minimal, the state business change manager role is not necessary.
4 BENEFITS REALISATION FRAMEWORK

To deliver on the full potential of a national ANPR capability, the implementation programme requires national governance arrangements with guiding principles, defined roles, responsibilities and accountabilities. This is required to ensure a benefits-driven focus.

The following sections outline the benefit’s realisation framework that will be adopted.

4.1 Governance and evaluation

Governance will be applied in line with current MSPM methodology and the ANPR Sponsoring Group will provide strategic guidance and decision making. Part 11 of this scoping study report describes programme governance arrangements more fully.

Benefits realisation is supported through the benefits realisation strategy and the benefits realisation plan. Projects in the implementation programme are grouped into tranches, with each tranche delivering a step change in capability, after which benefits realisation can be assessed. Business change managers play a key role in this process. Benefits management, which includes measuring, reviewing and reporting, is repeated for each tranche. The end of each tranche provides a major review point where the programme can be formally assessed in terms of its progress towards achieving the desired outcomes and measurable realisation of benefits.

4.2 Business change manager group

Due to the significant number of business change managers required, as well as their geographical disbursement, an ANPR programme Business Change Manager Group (BCM Group) will be instituted.

The BCM Group will be established to:

- engage key law enforcement and regulatory agency representatives across Australia in the work of the ANPR programme
- ensure that those involved in law enforcement and regulatory agencies in Australia have an appropriate opportunity to comment on changes that affect them
- refine ANPR programme benefit profiles
- provide a consultative forum that can effectively advise the ANPR programme (and its constituent projects), with particular reference to ANPR user requirements across Australia
- provide recommendations on the transitioning and implementation of new and/or enhanced ANPR capability across relevant agencies/organisations
- transition new and/or enhanced ANPR capability into relevant agencies/organisations
• establish mechanisms to measure the delivery of ANPR programme benefits
• measure and report on the delivery of ANPR programme benefits
• review metrics and programme trends to assure delivery of the ANPR programme benefits realisation plan.

4.3 Business change manager group deliverables
The specific outputs required from the ANPR programme BCM Group are:
• monitoring the interests of senior business management
• ensuring project scopes will deliver benefits
• optimising the timing of project deliverables from a business perspective
• preparing business areas for change transition
• establishing mechanisms for delivering and measuring benefits
• maximising the benefits realised.

4.4 Membership
Membership of the ANPR BCM Group will align with the implementation approach recommended in Part II of this scoping study report. Where infrastructure implementation is about to occur in a state, business change managers from each of the participating agencies will join the BCM Group. At full implementation, membership of the ANPR BCM Group will consist of one representative from each of the following agencies:
• CrimTrac
• each Australian state police force
• Australian Federal Police
• Australian Crime Commission
• Australian Customs Service
• each Australian road transport or infrastructure department as appropriate
• Victorian Department of Justice.

4.5 Benefits realisation management strategy
The purpose of the benefits realisation management strategy is to define processes for managing the expected benefits from the ANPR programme, including roles and responsibilities for effectively dealing with benefits realisation.

The strategy outlines the:
• process for profiling benefits through to the breakdown of measurable benefits
• functions for benefit planning, capability transition planning and benefit realisation
- roles and responsibilities for benefits planning, capability transition planning and benefit realisation, and how they align with the programme's organisation structure
- review and assessment process for measuring benefit realisation.

The functions involved with benefits planning and realisation for the ANPR programme include:
- developing the benefits realisation management strategy
- identifying business benefits [illustrated in an outcome relationship model and then refined in a benefits map]
- quantifying the benefits [documented in benefit profiles]
- planning for transition [ensuring new capability is effectively transitioned and embedded into affected business areas]
- planning for benefits realisation [documented in the benefits realisation plan]
- realizing benefits [confirmed via monitoring, measuring and reporting]
- reviewing benefits.

While the ANPR Sponsoring Group, and in particular the senior responsible officer, is ultimately accountable for the overall realisation of benefits for the programme, specific responsibilities are assigned to specific roles in the programme, as shown in Table 10.2.

Table 10.2 Benefits realisation management strategy roles and responsibilities

<table>
<thead>
<tr>
<th>ROLE</th>
<th>SENIOR RESPONSIBLE OFFICER</th>
<th>ANPR SPONSORING GROUP</th>
<th>ANPR PROGRAMME MANAGER</th>
<th>COORDINATING BUSINESS CHANGE MANAGER</th>
<th>BUSINESS CHANGE MANAGER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing the benefits realisation management strategy</td>
<td>Owns the strategy</td>
<td>Endorses the strategy</td>
<td>Develops the strategy</td>
<td>Works to achieve the strategy</td>
<td></td>
</tr>
<tr>
<td>Identifying the business benefits</td>
<td>Approves benefits map</td>
<td>Endorses the benefits map</td>
<td>Develops the benefits map with business change managers</td>
<td>Participates in developing benefits map</td>
<td></td>
</tr>
<tr>
<td>Quantifying the business benefits</td>
<td>Approves the business benefits</td>
<td>Endorses the business benefits</td>
<td>Drafts the benefits profiles</td>
<td>Coordinates validation &amp; compilation of profiles by business change managers</td>
<td>Validates and completes</td>
</tr>
<tr>
<td>ROLE</td>
<td>SENIOR RESPONSIBLE OFFICER</td>
<td>ANPR SPONSORING GROUP</td>
<td>ANPR PROGRAMME MANAGER</td>
<td>COORDINATING BUSINESS CHANGE MANAGER</td>
<td>BUSINESS CHANGE MANAGER(S)</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------</td>
<td>-----------------------</td>
<td>------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Planning transition</td>
<td></td>
<td></td>
<td>Aligns transition activities for project deliverables with the coordinating business change manager</td>
<td>Transitions and embeds capability</td>
<td>Advises coordinating business change manager of preferred transition methods</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Engages business change managers in transition planning</td>
<td>Champions activities in business area</td>
</tr>
<tr>
<td>Planning for benefits realisation</td>
<td>Approves plan</td>
<td>Endorses plan</td>
<td>Develops plan with coordinating business change managers</td>
<td>Produces plan</td>
<td>Work with coordinating business change managers to plan and establish monitoring processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Monitors progress against plan</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Owns benefits realisation</td>
<td></td>
</tr>
<tr>
<td>Realising benefits</td>
<td>Approves progress against plan</td>
<td>Endorses progress against plan</td>
<td>Monitors progress against plan</td>
<td>Manages issues and risks</td>
<td>Realises benefits through embedded change</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Monitors and reports progress against plan</td>
<td>Maximises and reports on benefit realisation</td>
</tr>
<tr>
<td>Reviewing benefits</td>
<td>Leads reviews</td>
<td>Endorses results</td>
<td>Participates in reviews</td>
<td>Plans and coordinates reviews</td>
<td>Participates in reviews</td>
</tr>
</tbody>
</table>

**CrimTrac**

Responsive - Innovative - Accountable

Released by the CrimTrac Agency under the Freedom of Information Act 1982
4.6 Benefits review process

Realisation of anticipated business benefits will be reviewed as part of the broader end tranche review process. The ANPR programme’s senior responsible officer is responsible for conducting these benefits reviews and is to ensure that the review checks:

- that the overall set of benefits remains aligned to the programme’s objectives
- that benefits realisation progress is acceptable (that is, in line with the baseline benefits realisation plan)
- the effectiveness of the way benefits realisation management is being handled
- potential improvements or lessons learned.

Business change managers and other programme stakeholders may be asked to attend certain elements of the review to support the assessment process.

At each review, the senior responsible officer is to assess the:

- alignment of the overall set of benefits with programme objectives
- benefit profiles and benefits realisation plan to ensure that the planned benefits remain achievable, and the scope remains unchanged
- progress in realising benefits
- level of benefits achieved against the planned benefit profiles
- potential for further benefits
- performance of changed business operations against baseline performance levels.

If the senior responsible officer assesses that the overall set of benefits does not align with the ANPR programme’s objective, the benefits are to be realigned or re-prioritised, as necessary. If required, the coordinating business change manager (supported by the programme manager) is responsible through the benefits planning process for realigning and re-prioritising benefits. Approval must be obtained from the senior responsible officer to re-baseline benefits on completion of the re-planning.

Where the benefit profiles have been assessed and require updating, the coordinating business change manager is to seek input from relevant business change managers to update the benefit profiles.

Where the benefits realisation plan has been assessed and requires updating, the coordinating business change manager is to update the benefits realisation plan and seek senior responsible officer approval of the updated plan. It is important to note that refinement of the benefits realisation plan will almost certainly require revision of benefit profiles and vice versa.

The assessment of the progress of benefits realisation is to be advised to all members of the ANPR Sponsoring Group, and the programme management team more broadly, including business change managers. The programme manager and the program support officer are responsible for disseminating the senior responsible officer assessment following reviews of benefits.
5 CONCLUSION

Benefits realisation in the context of the ANPR programme is a critical component of embedding new capability. To this end, a rigorous and comprehensive benefits realisation framework will be embedded into the implementation programme. Interim business change managers engaged through stakeholder agencies during the benefits mapping and profiling process have assisted in mapping and profiling the very significant benefits to be realised. The benefits realisation framework will allow those benefits to be quantified and validated, and will form part of CrimTrac’s regular reporting through to government and ministers.
PART II
IMPLEMENTATION PLAN
& COSTINGS
This part of the CrimTrac Automated Number Plate Recognition (ANPR) scoping study report details the preferred approach for implementing a national ANPR capability in Australia, and the associated cost.
## CONTENTS

1. SUMMARY .......................................................... 274
2. ANPR IMPLEMENTATION OPTIONS ....................... 276
3. ANPR IMPLEMENTATION ISSUES AND RISKS .......... 279
4. ANPR IMPLEMENTATION GOVERNANCE ............... 280
5. RECOMMENDED ANPR IMPLEMENTATION OPTION .... 281
6. ANPR IMPLEMENTATION ACTIVITIES .................... 282
7. ANPR IMPLEMENTATION PHASES ......................... 284
8. COSTING OF RECOMMENDED OPTION ................. 288
The ANPR Scoping Study has identified six implementation options that could be adopted to implement a national ANPR capability. Each option assumes that a central coordinating system will be established, whilst varying the amount and mix of ANPR infrastructure and the subsequent implementation schedules. Each option has been designed to provide for a national ANPR capability while at the same time enhancing agency capabilities. They provide a base for realising road safety, law enforcement and national security objectives. However, full realisation of these objectives requires comprehensive ANPR coverage, real time information sharing and effective sighting analysis capability as well as the ability of the agencies to respond to the required business change. These options are listed below:

1. National ANPR system [NAVIR]
2. In-field coverage
3. Fixed coverage
4. Fixed and in-field coverage
5. Effective national coverage
6. Reduced national coverage

All options will require a minimum investment of $123.204 million to facilitate the implementation of the national system capability. The overall costing will depend on a range of factors which can be varied for each option. These include the level of camera infrastructure deployed, the level to which business requirements are supported, particularly requirements relating to data transfer and storage, and management options relating to funding, scheduling, infrastructure rollout, and the degree to which programme and project management is centrally coordinated. Funding and scheduling options would need to be analysed should a preferred option be identified. Expected benefits would also depend on the level of ANPR infrastructure and the business model adopted by each agency.

Each option has a common set of enabling activities which would be required to successfully implement a national ANPR capability. These include implementing a national procurement strategy, coordinating necessary changes in Commonwealth and state legislation, the rollout of national ANPR infrastructure, and national ANPR engineering coordination.

Option 5 'Effective national coverage' is presented as the recommended option in this report as it provides the most comprehensive coverage and use of ANPR technology. If the scoping study recommendations are endorsed, the activities could commence in July 2009 and be completed by June 2012. This option would comprise of six projects that could be delivered in three phases over eight years, with an estimated cost of $764.8 million. This is discussed in greater detail in Section 7 of this part of the report – ANPR Implementation Phases.

The recommended ANPR infrastructure rollout for a full national system will cover the strategic road networks, major roads and population centres, critical infrastructure and state borders. This
will require an integrated mix of fixed and mobile capability across all agencies and states with suitable network connectivity as defined in the gap analysis.

A phased implementation approach for the recommended option will enable:

- CrimTrac and participating states and territories to manage implementation and privacy risks;
- the ANPR programme to adapt to any changes in priorities and conduct ongoing privacy impact assessments; and
- refinement of the implementation schedule following regular measurement and reporting of benefits to transport and policing ministers by the CrimTrac Board of Management.

The benefit/cost ratio in part 12 of the scoping study report reflects the implementation approach of option 5 which is discussed in the following sections. This ratio would change depending on the option adopted by stakeholders and further cost benefit analysis would need to be conducted during the business case development stage.

State and territory participation in recommended implementation phases identified in this part of the report, will be subject to further planning, consultation and, ultimately, ministerial and government decisions.
2 ANPR IMPLEMENTATION OPTIONS

The ANPR Scoping Study identified six implementation options that could be adopted to implement a national ANPR capability. Each implementation option seeks to achieve a national ANPR capability while at the same time enhancing agency capabilities. All options assume a central National Automated Vehicle Recognition (NAVR) system, but offer increasing levels of capability and coverage through varying the mix and/or increasing the amount of ANPR infrastructure deployed in agencies.

Each option provides a base for realising road safety, law enforcement and national security objectives, although full realisation of these objectives requires comprehensive ANPR coverage, real-time information sharing and effective sightings analysis capability. All options allow agencies to increase their ANPR capability at any time based on future operational priorities. A national ANPR capability will enhance current business processes and assist in the development and implementation of new business processes. All options require the minimum criteria to be met which can be implemented in four years. The activities and associated costs are represented in Figure 11.1 below. These costs are common to all options.

Figure 11.1 Common ANPR implementation activities and associated costs to all options

<table>
<thead>
<tr>
<th>ACTIVITY</th>
<th>COST ($M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development and implementation of the NAVR system including infrastructure and system development.</td>
<td>117.313</td>
</tr>
<tr>
<td>ANPR programme management</td>
<td>3.519</td>
</tr>
<tr>
<td>Legislative changes to allow the collection and sharing of ANPR data for national security, law enforcement, and roads and traffic management purposes.</td>
<td>2.374</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>123.206</strong></td>
</tr>
</tbody>
</table>

There are a range of factors which can be varied for each option. These include the level of camera infrastructure deployed, the level to which business requirements are supported (particularly requirements relating to data transfer and storage) and management options relating to funding, scheduling, infrastructure rollout and the degree to which programme and project management is centrally coordinated. Further funding and scheduling options would be analysed as part of any subsequent business case development.

Some options presented require less time than others to implement with the longest being eight years (option 5). To allow for effective comparison between options, additional operating costs have been added to cost all options to eight years. The first two years of each option will be dedicated to the development of the NAVR system and enabling activities. New ANPR infrastructure rollout and installation will commence in the second year to allow immediate integration of ANPR infrastructure with NAVR, when completed.

It is important to note that some costs relating to stakeholders and participating agencies have been identified but not presented due to the uncertainty of estimating these costs without a detailed analysis of each agency's expected business needs and regulatory environment. These include
integration of NAVR functionality with agency systems (including Austroads NEVDIS); increased agency system capacity for sightings capture and processing; increased business capacity to adjudicate and process alerts; and business process changes including alert processing centres.

OPTION 1: NATIONAL ANPR SYSTEM (NAVIR), $123.206M [4YRS IMPLEMENTATION]

This option covers the foundation from which a more comprehensive national ANPR capability could be developed over time. It integrates existing infrastructure with the national ANPR system, however it provides no new camera infrastructure nor upgrades to current mobile and in-vehicle units or fixed site systems. The option will only provide initial disparate ANPR coverage, limited data analysis capability and limited real time information sharing. Realisation of benefits would be minimal and localised. This option, however, provides a central system capability and would allow agencies to incrementally build upon their respective coverage and networks in accordance with their own priorities.

OPTION 2: IN-FIELD COVERAGE, $271.591M [5YRS IMPLEMENTATION]

This option covers the elements of option 1, but also provides for new mobile and in-vehicle units. These units will provide additional mobile in-field ANPR coverage, however overall coverage and real time information sharing will be limited.

OPTION 3: FIXED COVERAGE, $650.128M [5YRS IMPLEMENTATION]

This option covers the elements of option 1, but also provides strategic fixed ANPR coverage at priority State and Commonwealth sites and on the national road network. Generally, new fixed sites would be focused on the Austlink road network, State border crossings and critical infrastructure. It does not include other fixed site coverage. Sights collected will provide benefits for national security, crime prevention and road safety initiatives. This option does not include any additional in-field coverage as outlined in option 2. In-field and data analysis capability remains limited under this option. Agency responsibilities for alert investigation and infrastructure ownership would need to be clearly defined due to the greater focus on Commonwealth priorities in this option.

OPTION 4: FIXED AND IN-FIELD COVERAGE, $656.861M [5YRS IMPLEMENTATION]

This option covers the elements of option 1 and option 3, but also provides new, automatically connected mobile and in-vehicle units. The option in essence complements fixed site capability with additional in-field ANPR coverage, offering broader overall coverage. The mobile and in-vehicle units will have real time access to NAVR’s analytical functions, allowing real time evaluation, detection and dissemination of alerts to the appropriate agency and therefore enabling quicker responses. While significant fixed and in-field coverage is provided under the option, coverage is not yet optimal.

OPTION 5: EFFECTIVE NATIONAL COVERAGE, $964.854M [8YRS IMPLEMENTATION]

This option covers the elements of option 1, but also comprehensive and effective national ANPR coverage with upgrades to existing infrastructure, additional fixed and in-field ANPR infrastructure, in line with the Scoping Study findings. This option also provides real time information sharing and data analysis capability, with the potential to deliver significant benefits for road safety, crime prevention and national security. This option would provide the most comprehensive national coverage. This option is modelled in detail in the Scoping Study report.
CBA findings may be better proven through a series of trials and evaluation activities. Suitability approved locations for such an activity would need to be identified. An assessment of suitable locations should consider leveraging current activities being undertaken in some jurisdictions.

**OPTION 6: REDUCED NATIONAL COVERAGE, $610.528M (BYRS IMPLEMENTATION)**

This option covers the elements of option 5, with reduced national ANPR coverage of approximately 50% fewer upgrades and new ANPR infrastructure as outlined in option 5. As there is a reduction in ANPR coverage there would also be a commensurate reduction in the ability to deliver national benefits for road safety, crime prevention and national security.

Table 11.1 below provides indicative cost estimates for each of the options, and may be used as a tool to assist in identifying a preferred option. The costings provided represent a national costing and do not reflect future models that may be agreed in respect of asset ownership and maintenance. A real discount rate of 4.5% per annum has been used in the cost benefit analysis. All other costs contained in this paper are nominal costs.

Depreciation estimates have been excluded on the basis that analysis of business cases rely on assessment of the costs and benefits. Depreciation is a function of capital costs and inclusion would not contribute to this analysis. Cost figures in the table have been rounded to the nearest thousand.

<table>
<thead>
<tr>
<th>Table 11.1</th>
<th>Comparison of ANPR implementation options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Option 1</td>
</tr>
<tr>
<td>Current Fixed Sites</td>
<td>23</td>
</tr>
<tr>
<td>Current Mobile and In-Vehicle</td>
<td>152</td>
</tr>
<tr>
<td>Upgrades to Fixed Sites</td>
<td>n/a</td>
</tr>
<tr>
<td>New Fixed Sites</td>
<td>n/a</td>
</tr>
<tr>
<td>New Mobile Units</td>
<td>n/a</td>
</tr>
<tr>
<td>New In-Vehicle Units</td>
<td>n/a</td>
</tr>
<tr>
<td>Implementation Schedule</td>
<td>4 years</td>
</tr>
<tr>
<td>Base ANPR Costs</td>
<td>123,206</td>
</tr>
<tr>
<td>Cost Associated with Additional Infrastructure</td>
<td>n/a</td>
</tr>
<tr>
<td>Total Implementation Cost</td>
<td>123,206</td>
</tr>
<tr>
<td>Additional Cost to 8 years5</td>
<td>101,697</td>
</tr>
<tr>
<td>Total cost adjusted to 8years</td>
<td>224,813</td>
</tr>
<tr>
<td>Ongoing operating costs from year 92</td>
<td>0.517</td>
</tr>
</tbody>
</table>

1. This line extends all option costings to 8 years for comparison purposes over this timeframe. This includes operating and programme expenses and where appropriate assumptions have been made on additional costs such as an increase in the central system capacity to accommodate increase in ANPR capture infrastructure added by jurisdictions overtime.

2. Per annum costs excluding depreciation.
3. ANPR IMPLEMENTATION ISSUES AND RISKS

The scoping study identified the following implementation issues and risks that will be considered during detailed implementation planning:

- **Legislation:** Commonwealth and state legislative change would need to be considered and if required would likely take a number of years to complete (see Part 8 and Appendix C of this scoping study report).

- **Privacy:** Part 7 of this report contains a privacy impact assessment summary and the full assessment is in Appendix B.

- **Impact on current business processes:** The introduction of a national ANPR capability will affect existing stakeholder business processes and resources. The risk that stakeholders will not be able to meet national requirements will need to be closely managed.

- **Procurement:** Part 9 of this report outlines a national procurement strategy for acquiring products and services to implement a national ANPR capability. The strategy aims to achieve the optimum balance of risk, innovation, control and cost-efficiency in procuring ANPR equipment.

- **NAVR architecture:** Ensuring system architecture and design effectively meets requirements is a critical activity during the initial implementation of NAVR. These include interoperability, minimum national data standards, and the ability of the system to meet projected load.

- **Project linkages and dependencies:** A number of dependencies identified during the scoping study will be identified in the detailed programme schedule, and managed according to the CrimTrac risk management framework.

- **Stakeholder engagement:** The ANPR Sponsoring Group and the ANPR programme change managers will manage all relationships with stakeholders, whose roles are defined in the national stakeholder engagement strategy developed by the ANPR programme.

- **Funding models:** The funding models have yet to be finally determined and must be considered in the light of business cases relevant to all stakeholders.
4. ANPR IMPLEMENTATION GOVERNANCE

ANPR implementation will be managed using the Managing Successful Programs (MSP™) framework, with individual projects managed according to the PRINCE2™ project management methodology.

The ANPR Sponsoring Group, chaired by the former NSW Police Commissioner, Mr Ken Moroney, AO, APM, includes representatives from:

- all state and territory police services
- Australian Federal Police
- Australian Crime Commission
- Department of Infrastructure, Transport, Regional Development and Local Government
- Commonwealth Attorney-General’s Department
- Australian Customs Service
- Austroads
- National Transport Commission
- Department of the Prime Minister and Cabinet, National Security Division
- CrimTrac.

This national representation maximises stakeholder engagement and ensures all stakeholder requirements inform the implementation of the ANPR programme.
5. RECOMMENDED ANPR IMPLEMENTATION OPTION

The scoping study recommends the implementation of option 5, Effective National Coverage. This option will provide comprehensive and effective national ANPR coverage, real-time information sharing and data analysis capability, with the potential to deliver significant benefits for road safety, crime prevention and national security. The implementation activities of this option are detailed below.
6. ANPR IMPLEMENTATION ACTIVITIES

The following core activities shown in Figure 11.2 will be delivered through six major projects:

1. developing and implementing a National Automated Vehicle Recognition (NAVR) system
2. rolling out national ANPR infrastructure
3. undertaking a national procurement process
4. coordinating ANPR Commonwealth and state and territories legislative changes
5. coordinating national ANPR infrastructure rollout
6. coordinating national ANPR engineering.

Figure 11.2 ANPR implementation activities
Figure 11.3 shows the schedule for implementing the various activities.

**Figure 11.3 ANPR Implementation schedule**

<table>
<thead>
<tr>
<th>Task Name</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAVR Implementation Project</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Project Initiation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Project Implementation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• System Implementation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• System Deployment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PROJECT 1 -- DEVELOPING AND IMPLEMENTING NAVR SYSTEM**

**Timeframe:** Commence 1 July 2009 and move to production on 1 August 2011

**Cost:** $65.6 million

This project involves developing a NAVR system and acquiring the ICT hardware and software for the first phase of the implementation.

The national integration of camera infrastructure requires the development of an integrated central computer system to provide optimal tools and to share and store information nationally. The system will support the detection of vehicles of interest in real time, the development and maintenance of national hotlists, the creation of a national alert system, and the analysis of vehicle movements within and across state borders.

The implementation project will adopt an iterative system development approach under a formal system development life cycle methodology. The use of such a methodology will ensure that the entire development process, including analysis, design, construction, testing, integration, implementation and maintenance, is managed within a best practice framework.

Figure 11.4 shows the schedule for implementing the NAVR system.
PROJECT: ROLLING OUT NATIONAL ANPR INFRASTRUCTURE

Timeframe: Commence in July 2010 and finish in June 2017 [three phases]

Cost: $601.4 million

This will include delivering fixed and mobile ANPR cameras and other infrastructure, including poles and gantries, to identified sites within each state covering major roads and population centres, critical infrastructure and state borders.

For the national environment to be effective it must have sufficient camera infrastructure to cover the strategic road networks, major roads and population centres, critical infrastructure and state borders. This will require an integrated mix of fixed and mobile detection across agencies and states with suitable network connectivity as defined in the gap analysis. The focus in this project will be to provide sufficient ANPR infrastructure to form an effective base for national use in three phases.

ANPR infrastructure rollout also involves local government planning and engineering activities to establish the physical infrastructure at each site (for example, the poles or gantries, as well as power, network connectivity and civil works). This infrastructure will be purchased through a national procurement process using the guidelines defined in the ANPR national procurement strategy in Part 9 of this scoping study report.

The objective of the overall rollout plan is to:

- provide in-vehicle capability to 25% of all state law enforcement and regulatory agency vehicles
- upgrade all existing sites and infrastructure
- provide two-thirds of all new fixed site requirements identified by states, excluding new red-light and speed camera sites.

Figure 11.5 presents the yearly costing of each of the three phases of the national ANPR infrastructure rollout project.

Figure 11.5 ANPR national infrastructure rollout costing per annum
PROJECT 3 – UNDERTAKING NATIONAL PROCUREMENT ACTIVITIES

Timeframe: Commence in January 2009 and complete by June 2010

Cost: Approximately $4.9 million

Acquiring ANPR technology that supports the implementation of a national ANPR capability will involve two stages:

1. The first stage of the strategy has commenced. A request to seek information from ANPR camera system vendors and vendors that could supply business intelligence tool sets has also been initiated. The outcome of this process will influence future procurement activities.

2. The second stage of the strategy will include developing a plan to go to the market, determining common national ANPR technical standards for technology, testing the products against the agreed standards, selecting one or more panel providers, developing a maintenance plan, and identifying and mitigating any legislative, organisational, contractual and jurisdictional constraints on Commonwealth or state procurement requirements.

PROJECT 4 – COORDINATING CHANGES TO COMMONWEALTH AND STATE LEGISLATION CHANGE

Timeframe: Commence in early 2010 and continue until early 2014

Cost: Approximately $2.4 million

Commonwealth and state legislative changes are enablers to implementing a national ANPR capability across all states. Coordination activities at a project level are required to ensure harmonisation and consistency of required legislative and administrative changes.

PROJECT 5 – COORDINATING NATIONAL ANPR INFRASTRUCTURE ROLLOUT

Timeframe: Between January 2010 and June 2017

Cost: Approximately $5.3 million

This will include planning and delivering ANPR infrastructure to states and will require ongoing consultation with stakeholders. Activities will include site selection, ensuring the purchased infrastructure meets the requirements, and installation as required.

PROJECT 6 – COORDINATING NATIONAL ANPR ENGINEERING

Timeframe: Between January 2010 and June 2017

Cost: Approximately $5.85 million

This will include coordinating engineering activities of ANPR infrastructure rollout in consultation with stakeholders. Activities include local government planning and engineering activities to specify, design and construct the physical infrastructure at each site (for example, the poles, ballards or gantries as well as power and network connectivity).
While a national rollout remains the preferred model for implementation, consideration needs to be given to undertaking a pilot or evaluation activity. Suitably approved locations for such an activity would need to be identified. An assessment of suitable locations should consider leveraging current activities being undertaken in some jurisdictions, such as NSW and the ACT.

As part of this consideration, the six projects could be delivered in three or more phases depending on jurisdictional requirements and agreement. For modelling purposes a national rollout giving indicative costs is exemplified below (drawn from jurisdictional inputs).

- **Phase 1**: Implement the central NAVR system and provide sufficient ANPR infrastructure to the Australian Capital Territory (ACT) and New South Wales (NSW) to form an effective base for national use including the assessment of any pilot or evaluation activity.

- **Phase 2**: Provide sufficient ANPR infrastructure to Victoria (VIC), South Australia (SA) and Western Australia (WA) to form an effective base for national use and initial ANPR infrastructure to the Northern Territory (NT), Tasmania (TAS) and Queensland (QLD).

- **Phase 3**: Provide the remaining ANPR infrastructure to all states and territories.

The priority and timing of the recommended phases are designed to realise benefits as early as possible, while managing risk and maintaining adequate project control. The actual construction of each phase and jurisdictional involvement will ultimately be a decision for governments.

**PHASE 1 – DEVELOP THE CENTRAL NAVR SYSTEM AND ROLLOUT ANPR INFRASTRUCTURE TO THE ACT AND NSW [JULY 2010 – JUNE 2012, APPROXIMATE COST $202 MILLION]**

**Phase 1 includes:**

- constructing and implementing the NAVR system
- introducing legislation and regulatory enablers
- rolling out ANPR infrastructure to the ACT and NSW
- operating the NAVR system in the ACT and NSW for 18-24 months
- critically evaluating operations against foreshadowed benefits realisation
- making informed decisions based on lessons learnt in phase 1 to inform and direct subsequent implementation phases.

**Objectives of phase 1 are to:**

- provide in-vehicle capability to 50% of vehicles in the first year and the remaining 50% in the second year (total 100%)
- upgrade 25% of the current infrastructure, including red-light and speed camera sites, in the first year and an additional 25% in the second year (total 50%)
• provide 25% of new fixed site ANPR infrastructure requirements, including all state borders and critical infrastructure, in the first year and an additional 25% in the second year.

Overall, NSW and the ACT will receive all their in-vehicle capability and 50% of the upgrades and 50% of the new fixed site infrastructure at the end of this phase.

Table 11.2 shows the detailed costing for activities undertaken in phase 1.

Table 11.2 Phase 1 implementation costing

<table>
<thead>
<tr>
<th></th>
<th>2009-10</th>
<th>2010-11</th>
<th>2011-12</th>
<th>2012-13</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
</tr>
<tr>
<td>Programme costs</td>
<td>2,775</td>
<td>3,364</td>
<td>2,774</td>
<td>0</td>
<td>12,342</td>
</tr>
<tr>
<td>NAVR system</td>
<td>7,013</td>
<td>16,866</td>
<td>1,549</td>
<td>25,448</td>
<td>1,450</td>
</tr>
<tr>
<td>development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAVR infrastructure acquisition</td>
<td>2,556</td>
<td>6,227</td>
<td>1,006</td>
<td>12,365</td>
<td>5,705</td>
</tr>
<tr>
<td>Infrastructure coordination</td>
<td>200</td>
<td>371</td>
<td>918</td>
<td>151</td>
<td>1,440</td>
</tr>
<tr>
<td>Infrastructure rollout</td>
<td>34,285</td>
<td>6,881</td>
<td>13,763</td>
<td>13,763</td>
<td>68,770</td>
</tr>
<tr>
<td>Engineering coordination</td>
<td>443</td>
<td>831</td>
<td>907</td>
<td>0</td>
<td>2,231</td>
</tr>
<tr>
<td>Legislative change</td>
<td>1,326</td>
<td>369</td>
<td>349</td>
<td>0</td>
<td>2,024</td>
</tr>
<tr>
<td>National procurement</td>
<td>3,500</td>
<td>1,605</td>
<td></td>
<td>0</td>
<td>4,900</td>
</tr>
<tr>
<td>TOTAL</td>
<td>9,569</td>
<td>8,523</td>
<td>15,229</td>
<td>48,299</td>
<td>26,788</td>
</tr>
</tbody>
</table>

PHASE 2 – ANPR INFRASTRUCTURE ROLLOUT TO VIC, SA AND WA [JULY 2013 – JUNE 2017]

The second phase is the largest of the rollout and will integrate the remaining agency systems with NAVR and roll out ANPR infrastructure to VIC, SA and WA. It will also include an initial but limited mobile and fixed infrastructure rollout to NT, TAS and QLD.

The second phase will deliver infrastructure each year until the programme is completed. This includes delivering 50% of in-vehicle capability requirements and 50% of all infrastructure upgrades to the remaining six states, and the remainder of the ACT and NSW infrastructure requirements.

PHASE 3 – ANPR INFRASTRUCTURE ROLLOUT TO NT, TAS AND QLD [JULY 2015 – JUNE 2017]

The third phase is the smallest of the infrastructure rollout project and will deliver the remaining new fixed ANPR infrastructure to NT, TAS and QLD.
8. COSTING OF RECOMMENDED OPTION

This report recommends a hybrid architecture which supports both direct access to a central system by agency users and the ability to access the central system from agency systems. Table 11.3 provides a high-level costing of the recommended option.

There is a difference in costs for phase 1 of the implementation and those for the full hybrid option shown above. This is due to the assumption in estimates for the 8-year programme (including the full hybrid option) that all agencies will roll out in year 3 of the programme (2012-13). The net cost for systems development and infrastructure in all agencies at the end of phase 1 is approximately $59 million above the equivalent cost for just the ACT and NSW in the phase 1 rollout.

Appendix E contains more details on the costings for the following implementation approaches:

- Phase 1 implementation (Hybrid architecture)
- Full implementation (Hybrid option)
- Full implementation (Distributed option)
- Full implementation (Central option).
Table 11.3 ANPR hybrid option costing

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
<td>$'000</td>
</tr>
<tr>
<td>CAPITAL OPERATING</td>
<td>2,775</td>
<td>3,387</td>
<td>3,427</td>
<td>2,774</td>
<td>4,947</td>
<td>5,062</td>
<td>5,119</td>
<td>5,002</td>
<td>32,492</td>
</tr>
<tr>
<td>OPERATING CAPITAL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>26,447</td>
</tr>
<tr>
<td>NAVR system</td>
<td>7,013</td>
<td>407</td>
<td>16,886</td>
<td>954</td>
<td>1,349</td>
<td>89</td>
<td></td>
<td></td>
<td>24,898</td>
</tr>
<tr>
<td>development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAVR infrastructure</td>
<td>17,886</td>
<td>373</td>
<td>30,232</td>
<td>1,357</td>
<td>15,726</td>
<td>8,271</td>
<td>15,095</td>
<td>11,722</td>
<td>21,436</td>
</tr>
<tr>
<td>acquisition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>17,476</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>200</td>
<td>371</td>
<td>918</td>
<td>151</td>
<td>918</td>
<td>918</td>
<td>918</td>
<td>918</td>
<td>5,312</td>
</tr>
<tr>
<td>coordination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5,312</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>34,385</td>
<td>4,881</td>
<td>34,385</td>
<td>13,763</td>
<td>13,763</td>
<td>89,372</td>
<td>91,088</td>
<td>91,088</td>
<td>50,130</td>
</tr>
<tr>
<td>rollout</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>90,504</td>
<td>50,130</td>
<td>50,130</td>
<td>52,240</td>
</tr>
<tr>
<td>Engineering</td>
<td>443</td>
<td>881</td>
<td>907</td>
<td>907</td>
<td>907</td>
<td>907</td>
<td>907</td>
<td>907</td>
<td>5,857</td>
</tr>
<tr>
<td>coordination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5,857</td>
</tr>
<tr>
<td>Legislative change</td>
<td>1,326</td>
<td>349</td>
<td>349</td>
<td>349</td>
<td>927</td>
<td>927</td>
<td>927</td>
<td>927</td>
<td>2,374</td>
</tr>
<tr>
<td>National</td>
<td>3,500</td>
<td>1,400</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4,900</td>
</tr>
<tr>
<td>procurement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>26,899</td>
<td>9,024</td>
<td>61,503</td>
<td>15,592</td>
<td>51,640</td>
<td>27,454</td>
<td>15,019</td>
<td>28,759</td>
<td>110,808</td>
</tr>
</tbody>
</table>

Released by the Crime
Agency under the Freedom
of Information Act 1982
Released by the CrimTrac Agency under the Freedom of Information Act 1982
PART 12
COST BENEFIT ANALYSIS
SUMMARY
This part of the CrimTrac Automated Number Plate Recognition (ANPR) scoping study report evaluates the impact ANPR technology could have on the community through safer roads, greater adherence to road rules and increased police efficiencies.
CONTENTS

1 SUMMARY .................................................. 294
2 BACKGROUND ............................................. 295
3 EVALUATION METHOD ................................. 296
4 COSTS QUANTIFIED ...................................... 297
5 BENEFITS QUANTIFIED ................................. 298
6 FINDINGS ................................................ 299
   6.1 A range of outcomes ................................ 299
   6.2 Benefit-cost ratios .................................. 300
   6.3 Key recommendations ............................. 300

Released by the CrimTrac Agency under the Freedom of Information Act 1982
1 SUMMARY

The proposed ANPR system would cost society $770 million to $849 million over its operating life, in net present value terms, depending on the design option. A single central system is the least expensive of the options modelled.

The system results in various improvements in road safety and crime prevention. Due to some uncertainties surrounding the extent of these improvements, the benefits to society are valued between $312 million and $2,120 million.

Under several scenarios the cost of ANPR outweighs the benefits created. To ensure the system benefits society more than it costs, and that the potential of the system is realised, a phased implementation is recommended.
Automated Number Plate Recognition (ANPR) technology is the capability behind a National Automated Vehicle Recognition (NAVR) system. ANPR, combined with NAVR, uses optical character recognition to monitor road movements of vehicles of interest. This part summarises an evaluation of the cost-benefit of implementing a national ANPR capability, undertaken by Access Economics. Appendix D contains the complete Access Economics report.

The following NAVR design options are evaluated:

- **Option 1** – Single central NAVR system. All data (including sightings, images, hotlists and alerts) are held centrally, and users interact directly with NAVR for all ANPR functions (via Gateway). Users work to a single consistent user interface and operate the same data repository. Existing agency ANPR hub systems may be replaced and made redundant by NAVR.

- **Option 2** – Distributed system. Under this option, central NAVR holds aggregated sightings and shared hotlists (as in Option 1) but user interaction is with the locally provided ANPR system rather than the central NAVR system. Hence, each agency must provide local ANPR capability.

- **Option 3** – Hybrid system. This option comprises a central NAVR system integrating with distributed local hub ANPR systems and/or capture systems. In addition, NAVR optionally supports direct access by agency users to cater for situations where local systems are not available.

Additionally, a Phase 1 option was analysed, whereby the ANPR system is implemented only in New South Wales (NSW) and the Australian Capital Territory (ACT).
Economic Cost Benefit Analysis is used to estimate the impact of ANPR. The impact is the expected future outcomes in a world with ANPR implemented versus the outcomes in a business as usual (or "do nothing") scenario. This deviation considers a range of outcomes as a result of ANPR, such as the safety benefits from a reduction in the number of unregistered vehicles and unlicensed drivers. Importantly, the measurement of benefits includes non-monetary benefits such as a reduction in road fatalities and injuries. The study also looks at the costs of implementing the system and then compared the cost of the system with the benefits generated. The net benefits (benefits minus costs, measured in dollars) and the benefit:cost ratio summarises the merits of a national ANPR capability.
4. COSTS QUANTIFIED

The cost of a national ANPR system includes the capital and operational costs of implementing and using it. For each of the options outlined above, there is an assumed phased infrastructure rollout and system development, beginning in the ACT and NSW in 2009–10, with all states joining the phased rollout in 2012–13. There are a number of assumptions regarding the asset, namely:

- 2-year period between building and commissioning the infrastructure;
- 5-year operational asset life; and
- after decommissioning, the asset is not replaced (that is, one life cycle is modelled).

For example, if infrastructure is installed in 2009–10, it is commissioned in 2010–11, decommissioned in 2014–15 and not replaced.

All capital outlays are assumed to run from 2009–10 to 2017–18 and the benefits from 2010–11 to 2020–21.

Option 1 (Central system) is the least expensive main option, with a net present value of $770 million using a 4.5% real discount rate. Option 2 (Distributed system) is the most expensive option at $849 million. Option 3 (Hybrid system) is estimated to cost $823 million.

The first phase of the nationwide implementation (roll-out across NSW and the ACT) has an estimated cost of $218 million (in net present value terms).
5 BENEFITS QUANTIFIED

The ANPR technology is expected to provide law enforcement authorities with increased capabilities to monitor, detect and apprehend antisocial activity such as unlicensed drivers, unregistered vehicles and theft. Additionally, given the lower antisocial behaviour, a reduction in serious injury and death is incorporated into the modelling. For similar reasons a reduction in nominal defendant claims is also modelled, while the ability to apprehend more offenders with the same given police officer resources means police efficiencies were also incorporated into the modelling.

Court costs are measured as a negative benefit, given their relationship to anti-social behaviour (that is, the cost of processing offenders, which is necessary to ensure the safety benefits are achieved). The increased apprehension of unlawful drivers and vehicles results in higher court activity and, subsequently, higher costs.

Some important benefits of a national ANPR system could not be quantified in this model. For example, the planned installation of cameras at critical infrastructure sites is expected to result in national security benefits. The dollar value of any such benefit, however, was not able to be quantified in this study.

The effectiveness of the new technology in reducing licence and registration violations may allow the police force to reallocate resources to other priorities or to achieve a targeted level of offenders in less time. However, no assumptions were made about the impacts of ANPR on the efficiency or productivity of traffic policing operations. For non-traffic based police it was assumed that the technology would enhance the ability to apprehend more offenders with the same given police officer resources, resulting in a productivity improvement.

---

1 In an earlier version of this analysis, an improvement in traffic police efficiency was estimated. This was based on organisational characteristics of traffic policing that were assumed to be similar across jurisdictions. During subsequent consultation, this assumption was regarded as unrealistic. As a result, no assumptions are made in this analysis about the efficiency or productivity of traffic policing operations. Should these assumptions be made, we would expect the projected benefits to increase.
The most significant benefit of national ANPR is estimated to be in road accidents in the low and central cases, accounting for $4.14 million in the central case. The uncertainty of assumptions in the model is highlighted by the fact that unregistered vehicles vary enough to become the largest benefit in the high case. The benefits under the central case total $879.6 million.

<table>
<thead>
<tr>
<th>2007-08 $ MILLION</th>
<th>ACT/SA</th>
<th>ACT/NSW</th>
<th>NSW (CENTRAL)</th>
<th>ACT/NSW</th>
<th>NSW (HIGH)</th>
<th>ACT/NSW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlicensed driving</td>
<td>$1.1</td>
<td>$0.5</td>
<td>$21.5</td>
<td>$9.3</td>
<td>$277.9</td>
<td>$110.3</td>
</tr>
<tr>
<td>Unregistered vehicles</td>
<td>$37.8</td>
<td>$14.2</td>
<td>$1899</td>
<td>$71.9</td>
<td>$488.0</td>
<td>$222.9</td>
</tr>
<tr>
<td>Vehicle theft</td>
<td>$43.7</td>
<td>$7.4</td>
<td>$130.9</td>
<td>$22</td>
<td>$323.5</td>
<td>$39</td>
</tr>
<tr>
<td>Nominal defendant</td>
<td>$2.9</td>
<td>$1.0</td>
<td>$5.6</td>
<td>$1.9</td>
<td>$8.6</td>
<td>$2.9</td>
</tr>
<tr>
<td>Court time and fees</td>
<td>$(1.7)</td>
<td>$(0.3)</td>
<td>$(15.3)</td>
<td>$(2.9)</td>
<td>$(101.7)</td>
<td>$(19.1)</td>
</tr>
<tr>
<td>Police efficiencies</td>
<td>$48.3</td>
<td>$16.9</td>
<td>$105.7</td>
<td>$36.9</td>
<td>$274.3</td>
<td>$94</td>
</tr>
<tr>
<td>Road accidents</td>
<td>$180.3</td>
<td>$48.7</td>
<td>$441.4</td>
<td>$121.2</td>
<td>$740</td>
<td>$204.2</td>
</tr>
<tr>
<td>Total</td>
<td>$312.6</td>
<td>$88.4</td>
<td>$879.6</td>
<td>$260.3</td>
<td>$2,119.5</td>
<td>$654.2</td>
</tr>
</tbody>
</table>

Insofar as benefit-cost ratios, the most efficient option for nationwide implementation is Option 1 as detailed above, with a wholly centralised system and single data repository. This is because the benefits of the system are delivered at lower capital costs under Option 1.

6.1 A range of outcomes

The analysis in this report is based on modelling unknown future outcomes of the implementation of new technology. By necessity, estimating the benefits involves a range of informed assumptions. Where assumptions have been made, they are on the conservative side.

In addition, the lack of hard data and the number of assumptions used in modelling the benefits outlined above has been tested through sensitivity analysis. Apart from the central scenario, key assumptions have been increased under a high case scenario and a low case scenario. The
uncertainty about key benefits of the system is reflected in the high variability in the low, central and high modelling scenarios. For example, the estimated benefits under the high case scenario are two times greater than the central case.

There are also a number of other issues that are not included in the cost-benefit analysis that may potentially affect the community that have not been quantified, including privacy and data security issues.

6.2 Benefit–cost ratios

The benefit–cost ratios under each option (under central case assumptions) are summarised in Table 2. A ratio higher than 1 indicates that the benefits outweigh the costs, while a ratio above 2 is preferable, indicating that for each $1 of cost $2 of benefits accrue.

The benefit–cost ratio is highest under Option 1, which is a function of lower implementation costs, given the benefits are constant across each scenario. In other words, the central system is relatively cheaper to implement and therefore generates the greatest relative benefit–cost ratio.

Another key element of the results is that the benefit–cost ratio for the Phase 1 rollout of the program to NSW and the ACT is relatively high.

Table 12.2 Benefit–cost ratios of national ANPR under central case assumptions

<table>
<thead>
<tr>
<th>BENEFIT–COST RATIO (BENEFITS/COSTS)</th>
<th>LOW</th>
<th>CENTRAL</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 1  Central System</td>
<td>0.41</td>
<td>1.14</td>
<td>2.75</td>
</tr>
<tr>
<td>Option 2  Distributed System</td>
<td>0.37</td>
<td>1.04</td>
<td>2.50</td>
</tr>
<tr>
<td>Option 3  Hybrid System</td>
<td>0.38</td>
<td>1.07</td>
<td>2.58</td>
</tr>
<tr>
<td>Phase 1  ACT/NSW, retain alert overheads for 5 years</td>
<td>0.41</td>
<td>1.19</td>
<td>3.00</td>
</tr>
</tbody>
</table>

6.3 Key recommendations

Access Economics makes the following recommendations:

- Recommendation 1: Option 1 – the wholly centralised system – is the preferred NAVR system design, based on the lower cost of implementation.

- Recommendation 2: The phased implementation approach, where the ANPR capability is introduced in NSW and the ACT, is desirable to allow an evaluation period, based on actual observed information. This approach may also reduce the risk involved in this major capital outlay.

- Recommendation 3: Alternative implementation options should be considered. Rather than a ubiquitous rollout of ANPR, it may be possible to achieve (say) 75% of the benefits at 25% of the cost by a selective and targeted rollout of equipment.
APPENDIX A

STAKEHOLDERS

CRIMTRAC
Responsive - Innovative - Accountable
Released by the CrimTrac Agency under the Freedom of Information Act 1992
<table>
<thead>
<tr>
<th>STAKEHOLDER GROUPING</th>
<th>STAKEHOLDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ministerial Level Forums</td>
<td>Australian Transport Council (ATC)</td>
</tr>
<tr>
<td></td>
<td>Ministerial Council on Police and Emergency Management – Police (MCPEMP)</td>
</tr>
<tr>
<td>National Level Forums</td>
<td>Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA)</td>
</tr>
<tr>
<td></td>
<td>MCPEMP – Senior Officer Group (SOG)</td>
</tr>
<tr>
<td></td>
<td>National Counter Terrorism Committee (NCTC)</td>
</tr>
<tr>
<td></td>
<td>Standing Committee on Transport (SCOT)</td>
</tr>
<tr>
<td>National Agencies</td>
<td>Australian Crime Commission (ACC)</td>
</tr>
<tr>
<td></td>
<td>Australian Customs Service (ACS)</td>
</tr>
<tr>
<td></td>
<td>Australian Federal Police (AFP)</td>
</tr>
<tr>
<td></td>
<td>Australian Institute of Criminology</td>
</tr>
<tr>
<td></td>
<td>Australian Security Intelligence Organisation (ASIO)</td>
</tr>
<tr>
<td></td>
<td>Austroads</td>
</tr>
<tr>
<td></td>
<td>Carsafe</td>
</tr>
<tr>
<td></td>
<td>National Motor Vehicle Theft Reduction Council (NMVTRC)</td>
</tr>
<tr>
<td></td>
<td>National Transport Commission (NTC)</td>
</tr>
<tr>
<td>Commonwealth Departments</td>
<td>Attorney General’s Department (AGD)</td>
</tr>
<tr>
<td></td>
<td>Department of Defence</td>
</tr>
<tr>
<td></td>
<td>Department of Infrastructure, Transport, Regional Development and Local Government</td>
</tr>
<tr>
<td></td>
<td>Department of Prime Minister &amp; Cabinet</td>
</tr>
<tr>
<td></td>
<td>Protective Security Coordination Centre (P5CC)</td>
</tr>
<tr>
<td>STAKEHOLDER GROUPING</td>
<td>STAKEHOLDER</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CrimTrac</td>
<td>ANPR Scoping Study Project Board</td>
</tr>
<tr>
<td></td>
<td>ANPR Sponsoring Group</td>
</tr>
<tr>
<td></td>
<td>Board of Management</td>
</tr>
<tr>
<td></td>
<td>CrimTrac Projects</td>
</tr>
<tr>
<td></td>
<td>Strategic Issues Group</td>
</tr>
<tr>
<td>Policing Jurisdictions</td>
<td>Australian Capital Territory Policing</td>
</tr>
<tr>
<td></td>
<td>New South Wales Police</td>
</tr>
<tr>
<td></td>
<td>Northern Territory Police</td>
</tr>
<tr>
<td></td>
<td>Queensland Police</td>
</tr>
<tr>
<td></td>
<td>South Australia Police</td>
</tr>
<tr>
<td></td>
<td>Tasmania Police</td>
</tr>
<tr>
<td></td>
<td>Victoria Police</td>
</tr>
<tr>
<td></td>
<td>Western Australia Police</td>
</tr>
<tr>
<td>Investigative &amp; Oversight Agencies</td>
<td>Australian Commission for Law Enforcement Integrity (ACLEI)</td>
</tr>
<tr>
<td></td>
<td>NSW Crime Commission</td>
</tr>
<tr>
<td></td>
<td>NSW Independent Commission Against Corruption (ICAC)</td>
</tr>
<tr>
<td></td>
<td>NSW Police Integrity Commission (PIC)</td>
</tr>
<tr>
<td></td>
<td>QLD - Crime and Misconduct Commission (CMC)</td>
</tr>
<tr>
<td></td>
<td>SA - Police Complaints Authority</td>
</tr>
<tr>
<td></td>
<td>VIC - Office of Police Integrity (OPI)</td>
</tr>
<tr>
<td></td>
<td>WA - Corruption and Crime Commission (CCC)</td>
</tr>
<tr>
<td>State &amp; Territory Government Departments</td>
<td>ACT - Department of Territory and Municipal Services</td>
</tr>
<tr>
<td></td>
<td>NSW - Ministry of Transport</td>
</tr>
<tr>
<td></td>
<td>NSW - Roads and Traffic Authority</td>
</tr>
<tr>
<td></td>
<td>NT - Department of Planning and Infrastructure</td>
</tr>
<tr>
<td></td>
<td>QLD - Department of Main Roads</td>
</tr>
<tr>
<td></td>
<td>QLD - Department of Transport</td>
</tr>
<tr>
<td></td>
<td>QLD - Parliamentary Travelsafe Committee</td>
</tr>
<tr>
<td>STAKEHOLDER GROUPING</td>
<td>STAKEHOLDER</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>State &amp; Territory Government Departments (cont'd)</td>
<td>SA - Department for Transport, Energy and Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Tasmania - Department of Infrastructure, Energy and Resources</td>
</tr>
<tr>
<td></td>
<td>VIC - Department of Infrastructure</td>
</tr>
<tr>
<td></td>
<td>VIC - Department of Justice</td>
</tr>
<tr>
<td></td>
<td>VIC - VicRoads</td>
</tr>
<tr>
<td></td>
<td>WA - Department of Main Roads</td>
</tr>
<tr>
<td></td>
<td>WA - Department of Planning and Infrastructure</td>
</tr>
<tr>
<td>Privacy Commissioner &amp; Ombudsman Offices</td>
<td>Office of the Privacy Commissioner</td>
</tr>
<tr>
<td></td>
<td>ACT Human Rights Commission</td>
</tr>
<tr>
<td></td>
<td>NSW Office of the Privacy Commissioner</td>
</tr>
<tr>
<td></td>
<td>NT Office of the Information Commissioner</td>
</tr>
<tr>
<td></td>
<td>VIC Office of the Privacy Commissioner</td>
</tr>
<tr>
<td></td>
<td>WA Office of the Information Commissioner</td>
</tr>
<tr>
<td></td>
<td>Commonwealth Ombudsman</td>
</tr>
<tr>
<td></td>
<td>NSW Ombudsman</td>
</tr>
<tr>
<td></td>
<td>ACT Ombudsman</td>
</tr>
<tr>
<td></td>
<td>NT Ombudsman</td>
</tr>
<tr>
<td></td>
<td>QLD Ombudsman</td>
</tr>
<tr>
<td></td>
<td>SA Ombudsman</td>
</tr>
<tr>
<td></td>
<td>Tasmanian Ombudsman</td>
</tr>
<tr>
<td></td>
<td>VIC Ombudsman</td>
</tr>
<tr>
<td></td>
<td>WA Ombudsman</td>
</tr>
<tr>
<td>Motoring Organisations</td>
<td>Insurance Council of Australia (member of NMVTRC)</td>
</tr>
<tr>
<td></td>
<td>Australian Automobile Association</td>
</tr>
<tr>
<td></td>
<td>Federal Chamber of Automotive Industries</td>
</tr>
<tr>
<td></td>
<td>Motor Trades Association of Australia</td>
</tr>
<tr>
<td></td>
<td>National Roads &amp; Motorists Association Limited (NRMA)</td>
</tr>
<tr>
<td></td>
<td>Royal Automobile Club of Victoria (RACV)</td>
</tr>
<tr>
<td>STAKEHOLDER GROUPING</td>
<td>STAKEHOLDER</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Motoring Organisations (cont'd)</td>
<td>Royal Automobile Club of Queensland (RACQ)</td>
</tr>
<tr>
<td></td>
<td>Royal Automobile Association of South Australia (RAA)</td>
</tr>
<tr>
<td></td>
<td>Royal Automobile Club of Western Australia (RAC)</td>
</tr>
<tr>
<td></td>
<td>Royal Automobile Club of Tasmania (RACT)</td>
</tr>
<tr>
<td>Special Interest Groups</td>
<td>ACT Victims of Crime Assistance League</td>
</tr>
<tr>
<td></td>
<td>Australian Council of Social Service</td>
</tr>
<tr>
<td></td>
<td>Australian Federal Police Association</td>
</tr>
<tr>
<td></td>
<td>Australian Privacy Foundation</td>
</tr>
<tr>
<td></td>
<td>Human Rights and Equal Opportunity Commission</td>
</tr>
<tr>
<td></td>
<td>Northern Territory Police Association</td>
</tr>
<tr>
<td></td>
<td>Police Association of NSW</td>
</tr>
<tr>
<td></td>
<td>Police Association of South Australia</td>
</tr>
<tr>
<td></td>
<td>Police Association of Tasmania</td>
</tr>
<tr>
<td></td>
<td>Police Federation of Australia</td>
</tr>
<tr>
<td></td>
<td>Public Interest Advocacy Centre</td>
</tr>
<tr>
<td></td>
<td>Queensland Police Union</td>
</tr>
<tr>
<td></td>
<td>The Police Association of Victoria</td>
</tr>
<tr>
<td></td>
<td>Victorian Council for Civil Liberties</td>
</tr>
<tr>
<td></td>
<td>Western Australian Police Union</td>
</tr>
</tbody>
</table>

Released by the CrimTrac Agency under the Freedom of Information Act 1982
CONTENTS

1 EXECUTIVE SUMMARY 308

2 INTRODUCTION 319
   2.1 CrimTrac and the ANPR Scoping Study 310
   2.2 About ANPR 310
   2.3 About the PIA 311
   2.4 Scope of the PIA 312

3 ISS RECOMMENDATIONS 313
   3.1 Recommendations 314

4 PROPOSALS 319
   4.1 CrimTrac Scoping Study and Proposals 319
   4.2 Overview of the National Automated Vehicle Recognition System 319
   4.3 NAVR System – model high-level approaches and assumptions 320

5 BENEFITS OF A NATIONAL ANPR SYSTEM 322

6 PRIVACY ISSUES IN THE ANPR CONTEXT 324
   6.1 General approach to privacy analysis 325
   6.2 Privacy issue analysis 326

7 APPENDIX I – PIA METHODOLOGY 343
   7.1 Information drawn upon 343
   7.2 Meetings and Consultations 344

8 APPENDIX II – AUSTRALIAN GOVERNMENT USE OF ANPR 345

9 APPENDIX III – USE OF ANPR 5 YEARS OUT 346

10 APPENDIX IV – AUSTRALIAN PRIVACY LAWS 348
Information Integrity Solutions Pty Ltd (IIS) has conducted a privacy impact assessment (PIA) of proposals for a national strategic approach to the use of Automated Number Plate Recognition (ANPR).

The PIA is one input to CrimTrac’s scoping study which is considering a national ANPR system that would overlay an existing and evolving system. Australian state and territory governments are already making use of ANPR and can be expected to expand this use in the future. The intention for a national ANPR system is to facilitate the collection and sharing of ANPR data across Australian states and territories to promote community safety, law enforcement, road safety and national security.

The decisions that will be made in relation to a national ANPR system will include where to draw the balance between the privacy impacts of the proposals and other considerations, including the extent of benefits to the community. The point of balance is going to be a matter of judgment for the decision makers in governments and, ultimately, Parliament.

If governments do proceed to consider and implement any national ANPR system, such an approach could have the possible advantages of setting high and consistent standards and protocols for ANPR technology and of ensuring that data exchanges between state agencies are properly authorised and governed.

However, IIS considers that a national ANPR system which includes an extensive network of ANPR cameras recording all vehicle movements would be a very significant new form of population level surveillance with potentially high-order privacy impacts and so should not be undertaken lightly.

IIS recommends that a national ANPR system should proceed only after alternative approaches to dealing with identified problems have been considered and if it can be clearly demonstrated that the benefits of a national ANPR system significantly outweigh the costs, including intangible costs such as the privacy impact.

The IIS recommendations aim to lay out a process that will allow privacy interests to be fully considered should governments decide to proceed with any further consideration or implementation of a national ANPR system. IIS also makes recommendations about matters it considers should be built into a national ANPR system to mitigate the potentially very significant and high-order privacy risks, most particularly in relation to cross-border governance and accountability measures.

The IIS findings following the PIA are set out in this report, which is structured as follows:

- **Section 1** is this executive summary.
- **Section 2** introduces ANPR and the CrimTrac scoping study and outlines the PIA process.
- **Section 3** sets out the recommendations IIS is making to CrimTrac.
- **Section 4** provides further information relevant to the PIA about the CrimTrac scoping study.
- **Section 5** outlines the possible benefits of a national ANPR strategy.
- **Section 6** identifies and provides a deeper analysis of privacy issues that may arise in the context of any national ANPR system.
- **Sections 7-10** are appendices and include the material ISS considered, and a list of participants in the PIA consultation process.
2 INTRODUCTION

2.1 CrimTrac and the ANPR Scoping Study

CrimTrac is conducting a whole-of-government Automated Number Plate Recognition (ANPR) scoping study to identify a national strategic approach to the use of ANPR technology across Australia, including the infrastructure needed and the possible costs and benefits.

The system would overlay state and territory government ANPR systems. The intention is to develop a whole-of-government combined state/territory and national ANPR system to be used by law enforcement, national security and road transport authorities for improvements in road safety and public safety and national security, and the prevention, detection and reduction of crime.

While these are important aims and may deliver significant benefits, CrimTrac has recognised that a national ANPR system could raise very significant privacy issues. In response, CrimTrac has engaged Information Integrity Solutions Pty Ltd (IIS) to undertake a privacy impact assessment as an input to the scoping study.

A national ANPR system could potentially collect substantial amounts of information about vehicle movements and have a wide range of uses and users. These could range from organisations with powers to operate covertly or coercively all the way through to civilian organisations where law enforcement is not the issue. Mistakes in or misuse of this data could result in serious practical harm to individuals. There are also less tangible risks relating to citizens’ interactions with the state and the community’s sense of privacy or individual liberty.

This PIA report identifies a range of matters that, if adopted, will address or mitigate some of the potential privacy risks. However, IIS considers that an extensive network of ANPR cameras recording all vehicle movements would be a very significant new form of population-level surveillance with potentially high-order privacy impact and so should not be undertaken lightly.

2.2 About ANPR

ANPR uses a camera and optical character recognition software to capture an image of a vehicle, locate the number plate within the image and then convert the number plate value to a text string. Users can then compare the text with databases containing vehicle number plate values, known as hotlists, for example, for road transport authorities (RTAs) to identify unregistered vehicles and issue infringement notices or for law enforcement agencies to generate alerts for stolen vehicles. State agencies have used variants in most Australian states since the 1980s. Private sector bodies also use ANPR, for example, in toll road charging, for site or precinct security, car park access or petrol station security.

ANPR system configurations are generally mixtures of design features that can include fixed or mobile cameras that may be single point or point-to-point and single direction or dual facing cameras; local or centralised systems; wired or wireless communications; intercept of vehicles or back-office issuing notifications; and store sightings and action or store sightings only. A useful

In Australia, governments have mainly used ANPR to manage heavy vehicle and other traffic issues, although law enforcement agencies also use, or have been exploring, the technology for law enforcement and national security purposes. A brief summary of current state and territory use of ANPR is at Appendix II. These initiatives generally involve the collection of ANPR data and then comparison with databases and hotlists within a state's boundaries. In many cases, law enforcement or regulatory agencies will have access to data held in other states. However, such arrangements tend to involve a range of organisations and processes rather than to provide direct access.

2.3 About the PIA

A PIA is a process which enables organisations to 'anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions.' It usually looks beyond mere compliance with privacy law to consider wider privacy challenges, including allocation of risks and individual trust.

IIIS sees a PIA as a dialogue rather than a simple 'audit'. A critical part of a PIA is consultation with people affected by or with an interest in the system or proposal under assessment. Consultation can draw in new information and perspectives about the impacts and implications of the proposal, allow assumptions, assertions and arguments to be tested, and develop options to avoid or ameliorate negative privacy impacts.

The steps in the PIA process are:

- information gathering
- analysis
- consultation, and
- development of recommendations and preparation of the PIA report.

IIIS held five consultation meetings, some with particular interest groups and one on 8 July 2008 to which all the previous participants were invited. This report has drawn on these discussions and aims to give an indication of the issues raised and views presented. However, the perspective and views expressed here are those of IIIS as the independent PIA consultants. They are not intended to represent the views of the people consulted and it is open to those people to express different views about any national ANPR system.

The PIA analysis presented in this report is based on the discussions noted above, documents provided by CrimTrac about the scoping study, and discussions with CrimTrac staff and with some of the potential user agencies. This material included a detailed privacy issues report prepared for CrimTrac by Xamax Consultancy Pty Ltd.

Details of the material considered and the people and groups consulted are set out in Appendix 1.

---

1 See www.ico.gov.uk/upload/documents/oha_handbook.html/htm/1-intro.html
2.4 Scope of the PIA

CrimTrac’s ANPR scoping study, of which this PIA is a part, commenced in April 2007 and is due to be finalised in November 2008. CrimTrac will present the scoping study report to the Ministerial Council for Police and Emergency Management – Police and the Australian Transport Council in late 2008.

The nature of the scoping study means that CrimTrac is putting forward high-level recommendations for consideration by governments; not detailed proposals for implementation. At the time this PIA was undertaken, CrimTrac was still in the process of finalising its recommendations and had not taken final decisions. CrimTrac sought the PIA process and the issues as input to its recommendations. Further consideration of privacy impacts, taking account of detailed implementation approaches, would be needed if CrimTrac’s recommendations to government are adopted.

The PIA focuses on the privacy impact, particularly arising from a national ANPR system. It focuses on impacts of any national system compared with how the use of ANPR might in any case develop in the Australian states and territories (in other words what is the impact of the national system) in the context of the general privacy impacts of wide use of ANPR.

Finally, for the purposes of this PIA, IIS assumes ANPR data is personal information. While ANPR data alone may not always be considered to be personal information as defined by privacy laws, it will routinely be matched and combined with information about individuals, for example, the name of the registered owner.
3 IIS RECOMMENDATIONS

The recommendations set out below follow IIS’s examination of the possible privacy impacts of a whole-of-government combined state/territory and national ANPR system that law enforcement, national security and road transport authorities would use for improvements in road safety and public safety and national security, and the prevention and detection of and reductions in crime.

The study is starting with the assumptions that such a system will:

- collect and retain sightings data for all vehicle movements past a camera point
- facilitate sharing of information about vehicle movements by road safety, law enforcement and national agencies, and
- enable this information to be leveraged, for example, by analysis for police investigations, or for road safety purposes using aggregated data.

IIS notes that the community, privacy and civil liberties advocates consulted as part of this PIA have expressed strong appreciation of CrimTrac’s transparency about the scoping study and its decision to consider privacy issues at this early stage in the process. However, the consultation process revealed strong reservations about the proposals.

The key concern is that a whole-of-government ANPR system implemented with the intention of recording all vehicle movements past an extensive network of ANPR cameras would be a very significant new form of population level surveillance with potentially high-order privacy impact. At the same time, there are potentially high-order benefits, some of which may be quantified by the cost/benefit process that is also part of this scoping study. This makes the decision making process very serious. Ultimately, it will be a decision for government as to where the balance is in this instance.

The PIA process has identified a range of other issues that IIS considers should be taken into account in considering if the proposals should proceed and, if so, in what form, and also issues that would need to be addressed in any implementation. These are set out in section 6.

Based on the issues identified, IIS has made a range of recommendations that it considers will mean decision makers can factor privacy into decisions about the proposals and will help mitigate privacy impact should a national ANPR system be implemented.

IIS appreciates that some of its recommendations address matters that are not directly within CrimTrac’s control, for example, the nature of the law applying to any national ANPR system, or the resources that state or territory agencies make available to complaint handling bodies responsible for investigating citizens’ issues about infringement notices or other matter arising from an ANPR sighting. However, it considers that they are all matters that are relevant for governments and other bodies considering the scoping study and making decisions about if or how to proceed with a national ANPR system.
3.1 Recommendations

RECOMMENDATIONS 5 - THRESHOLD DECISIONS ABOUT A NATIONAL ANPR SYSTEM

Recommendation 1 – Decision to proceed with ANPR requires strong justification

IIS recommends to CrimTrac that its report recommend that proposals for a national ANPR system that includes mass population-level surveillance and recording of innocent vehicle movements should proceed only after alternative approaches to dealing with identified problems have been considered and if a cost/benefit analysis undertaken on the principles laid out in section 6.2.5 shows a significant benefit cost ratio. IIS notes that this evidence may be available only after a controlled trial process such as laid out in Recommendation 6.

Recommendation 2 – National ANPR System to be limited to significant road safety, law enforcement and national security matters

IIS recommends that CrimTrac’s report recommend that should a national ANPR system proceed, it should be used only to address serious matters, not minor issues of road safety regulation or law enforcement. This requirement should apply to the purposes for which agencies may provide or access ANPR data held in the national system and to the matters that can be the subject of an agency hotlist. The objectives for the system, the legal framework and other mechanisms used to implement the system and the further development of the proposals should ensure that this intent is maintained.

Recommendation 3 – Image of vehicles and their occupants

IIS recommends that CrimTrac’s report should recommend that, if implemented, a national ANPR system proceed only on the basis that:

a. images of vehicles that may include images of vehicle occupants be collected only where necessary for the original collecting agencies’ functions; and

b. images of vehicles that may include images of vehicle occupants be retained only by the collecting agency or the national ANPR system where there is a justified need in the context of a match against a hotlist within a short period of the sighting.

Recommendation 4 – Data minimisation

IIS recommends that CrimTrac should consider if there are ways to modify its proposals consistent with a ‘data minimisation principle’, for example, by:

a. limiting the number of cameras overall, for example, by targeting their placement to critical sites, or

b. maximising the number of camera sites where data is collected into the NAVR only if an event matches ‘hotlist’ criteria, and minimising the number of camera sites from which sightings data is collected for all vehicle movement.

Recommendation 5 – Private sector involvement

IIS recommends that CrimTrac continue its intention to exclude all private sector bodies from accessing information held in a national ANPR system.
RECOMMENDATIONS – NATIONAL ANPR SYSTEM IMPLEMENTATION REQUIREMENTS

Recommendation 6 – Further development of proposals to include consultation, trials and evaluation

ILS recommends to CrimTrac that its scoping study report recommends that any further development or implementation of a national ANPR system proceeds on the basis of:

a. a trial of the system followed by a full, publicly reported evaluation of results, including claims about possible costs and benefits taking account of a full range of risks and costs to stakeholders, broadly defined and as set out in section 6.7.5

b. ongoing transparent consultation with the full range of stakeholders, including privacy and civil society groups and stakeholders, on all aspects of further development of the system, including

i. the establishment of clear objectives at a reasonably detailed and specific level for the system as a whole, including in relation to privacy (for example, collection of the minimum possible information to achieve specified objectives), and for each area of activity, that is, road safety, law enforcement and national security objectives;

ii. system architecture and security

iii. data retention and accuracy

iv. permitted users and uses and a system of graded and rigorously managed access to the system, and

v. legislation and governance and accountability mechanisms

c. further privacy impact assessments at critical stages of the process, including during detailed design phases and following evaluation of trials.

Recommendation 7 – Wide community consultation and awareness

ILS recommends to CrimTrac that its scoping study report recommends that a national ANPR system should be implemented only following wide community consultation based on a complete and detailed description of proposals.

Recommendation 8 – Data retention

ILS recommends to CrimTrac that its scoping study report recommends that any implementation of a national ANPR system be on the basis that information be stored in the NAVR for as short a period as possible, and in particular that:

a. decisions about data retention period are not arbitrary but are based on evidence of significant benefits in the Australian context, and

d. retention periods are determined in relation to the original purpose for which the information was collected rather than being set for the NAVR as a whole.

Recommendation 9 – Rigorous framework established in law

ILS recommends to CrimTrac that its scoping study report recommends that a national ANPR system, other than in the trials noted above, should not be introduced unless:
a. all major aspects of a national ANPR system are established in law (governing laws) either at state and territory or federal level (or both) so that the same rules and standards apply wherever ANPR information to be included in the system is collected, held or used

b. the governing laws for any national ANPR system
   i. include a clear statement of objectives and purposes for the system
   ii. specify the information that may be included in the system and how long it may be retained, whether in identified and de-identified form
   iii. ensure that agencies only collect, use or disclose information for any national ANPR system to the extent this is necessary for their legitimate functions
   iv. ensure law enforcement agencies are permitted to collect information for inclusion in any national ANPR system only if the information is collected, and would normally be retained, in the normal course of policing activities, for example, where there is a reasonable suspicion that an offence has been committed
   v. specify the agencies that are permitted to access information in the national ANPR system and the circumstances in which access is permitted, including the authorisation process needed
   vi. include data breach notification obligations equivalent to those recommended by the Australian Law Reform Commission unless or until this is made redundant by more broad-based obligations inserted into privacy or other law
   vii. provide a ‘one-stop’ approach so that citizens are easily able to exercise their freedom of information rights to gain access to information held about them, including for the purposes of ‘innocence testing’, regardless as to which agency or jurisdiction holds it, and
   viii. include explicit decision making procedures for changes in the extent of the national ANPR system, such as the nature or amount of information collected, the purposes for which the system is established, and the agencies that may access the system.

Recommendation 10 - Security and accuracy

IfS recommends to CrimTrac that its scoping study report recommends that the development of a national ANPR system proceeds on the basis that it will be designed and resourced with high standards of security and accuracy in mind, and that, in particular, the legal or administrative framework for the system include:

a. requirements for ongoing monitoring and testing of accuracy of the information contained in or relied on by the national ANPR system, including sightings data, agency hotlists and any external databases

b. consistent rigorous security standards based on identified risks applying to all information collected, used or stored in relation the national ANPR system and applying to all agencies participating in the system and from the first point of collection, in particular, in relation to information stored in ANPR cameras and processing units and information in transmission

c. limiting access to the national ANPR system to agencies that can demonstrate their data meets standards in relation to accuracy and currency of data items

d. other incentives to ensure agencies give priority to accuracy, including publishing audit reports, providing reports to parliaments and tying individual compensation for accuracy breaches to the action agencies have taken to remedy any accuracy issues, and
Recommendation 11 – Governance, accountability and transparency

IIIS recommends that CrimTrac’s report recommends that the national ANPR system and the NAVR include accountability and governance arrangements that reflect the following:

a. the highest standard of accountability and governance frameworks that apply within jurisdictions are maintained in the cross-jurisdictional model so that no citizen is exposed to increased risk of surveillance, inappropriate action or other error simply because either they or data about them moves between jurisdictions

b. in particular, the development of a set of governance principles that provide the same level of privacy protection wherever data is handled

c. recognising that the system will have multiple objectives, including relating to national security, the transparency and governance principles should reflect the highest level of transparency rather than that applying to national security wherever possible

d. the CrimTrac Board, where it has a role in relation to the NAVR, should be expanded to include representatives from the road transport authorities

e. accountability arrangements should permit monitoring of the scheme from a national perspective, including flows of information across jurisdictions

f. subject to the development of effective coordinating arrangements, each agency involved in the NAVR should continue to be fully responsible for and be fully accountable for information they provide to the NAVR, and

g. the system should ensure that oversight bodies can conduct audits or own motion investigations that cover cross-jurisdictional issues (where data leaves one participating jurisdiction and goes to another participating jurisdiction) as thoroughly and efficiently as if the incident occurred within only one jurisdiction, and

h. the allocation by government of sufficient resources to ensure the governance model can be implemented effectively.

Recommendation 12 – Safety net and complaint handling

IIIS recommends that CrimTrac’s report recommend that a condition of implementing a national ANPR system should be the provision of user-friendly and effective safety net arrangements for individuals, regardless as to where their information is collected, used or stored, as well as clear identification of which agency is responsible for data accuracy and individual access for each data element, and redress is low cost and swift, and including, for example:

a. adequately resourced and fair mechanisms to challenge road transport infringement notices

b. easy processes for individuals to access information about them, including a one-stop shop where information may be held in multiple jurisdictions

c. easily accessible and adequately resourced complaint handling mechanisms, and

d. the establishment of an agency as a nominal defendant where the responsible agency is not clear.
4. PROPOSALS

4.1 CrimTrac Scoping Study and Proposals

The overall aim of the CrimTrac scoping study is to explore the feasibility of a national ANPR system and to develop a national strategic approach and an implementation strategy, including proposed governance arrangements and a procurement strategy, taking account of the contestability of the market. The scoping study will consider the following areas:

- the possible outcomes for law enforcement, traffic management, road safety, and national security.
- the current uses and deployment of ANPR for road transport management and law enforcement in Australia.
- an agreed set of the system users' business needs for a national system.
- the system capability and design needed to meet business needs.
- the legal and privacy implications.
- a cost/benefit analysis, and
- high-level considerations of architecture options.

Apart from the factors noted above, the fact that the Australian states are at a relatively early stage in ANPR deployment also feeds into the business case. CrimTrac considers that there is value in developing common technical standards and procurement approaches. This would ensure that regardless of which agency was operating ANPR technology, there would be uniformity throughout Australia.

4.2 Overview of the National Automated Vehicle Recognition System

The scoping study is using the concept of a National Automated Vehicle Recognition System (NAVR) to focus its considerations and it is exploring the infrastructure and other issues that governments would need to address to implement such a system. If governments decide to proceed with a national system, its actual design will be influenced by factors such as the size of the system, for example, the number of ANPR cameras, whether they are fixed or mobile, where transactions are processed, what data is stored where, what technology is used, and how much infrastructure capacity is required where.

The intention is that the NAVR would be used by a range of state, territory and Australian law enforcement agencies and road transport and infrastructure planning authorities on a strictly controlled basis. There is no intention to allow participating agencies to obtain access to information that they would not otherwise be authorised to obtain. So, for example, law enforcement access would be limited to the enforcement of specific laws or the conduct of specific policing matters, and road transport bodies would not be able to access law enforcement hotlists or alerts.
In developing its proposals, CrimTrac spoke to a range of state, territory and Australian law enforcement agencies (including the Attorney-General’s Department, the Australian Customs Service and the Australian Crime Commission) and regulators (including road transport and infrastructure planning authorities [RTAs] and agencies) and gathered information about each agency’s ‘business requirements’. Following the IIS’s consultation process, CrimTrac has clarified that at this stage of the planning process, business requirements are desirable requirements rather than non-negotiable minima. The desirable elements identified included the nature of the information captured in relation to a sighting, requirements for camera operation and image functionality and hotlist and alert data, information sharing requirements, data storage and management. Following analysis and prioritisation of the data collated, CrimTrac identified three ‘core capabilities’ that potential users would expect for a national ANPR system. These are:

- national ability to capture [in real time] vehicle sightings and detect vehicles of interest (VOI)
- national ability to share information associated with VOI, including sightings, warnings, associated persons and vehicles and registration details, and
- ability to interrogate aggregate national data to aid investigation, intelligence gathering and road use analysis.

The CrimTrac material indicates that all types of agencies consulted support at least in principle the concept of a national ANPR system that would make available the combined ANPR data from a range of sources, facilitate information sharing between state/territory and Australian government agencies, and allow searching and analysis of the national set of ANPR data over time.

However, at the more detailed level there was both agreement and variation in the requirements identified by law enforcement agencies compared to regulatory agencies. The examples noted below give a flavour of the issues raised by potential users.

- All parties considered the system must have the ability to capture data for all passing vehicles through ANPR equipment, rather than just matches against a hotlist.
- All parties considered the system would need to be able to limit access to ANPR data by their staff based on roles and specified circumstances.
- Law enforcement agencies considered the system must provide a clear image of the whole of vehicle frontage to allow the identification of the driver and/or front passenger at the resolution that agencies can use in court evidence, while for RTAs this was highly desirable.
- Law enforcement agencies considered that it would be highly desirable for images to be at a resolution suitable for use with facial recognition applications, while this was a lower priority for RTAs.
- RTAs considered that a national ANPR system would need to be able to respond to legal data retention/data deletion requirements in state/territory laws, while law enforcement agencies expressed interest in keeping data for as long as possible.
4.3 NAVR System – model high-level approaches and assumptions

States and territories currently collect and use ANPR sightings data for their own functions as permitted by state law. As noted earlier, they are also considering extensions in the use of ANPR systems. If governments decide to implement a national ANPR system, they would also transfer some or all sightings data to the NAVR, or otherwise make it available under the NAVR system.

The ANPR process starts with a camera taking images. The images are processed in the camera, or in a processing unit near the camera, to produce sightings data. This data is likely to include a text string and images, including record identifier, front and rear registration, vehicle direction, lane, sighting time and date, location in text and GPS coordinates, camera identifier, and jurisdiction.

State and territory agencies would compare sightings to their own hotlists or to hotlists held in the NAVR to identify vehicles of interest (for example, heavy vehicles that have moved between points too quickly, unregistered vehicles). Technically, hotlists can be held and processing may take place either within the processing unit, at another location near a camera, within a state agency, or within the NAVR. Factors that will affect the decision here include cost, technology and security risk assessments, as well as privacy considerations. There may be a uniform approach (that is, all matching takes place within an agency or the NAVR) or a range of approaches depending on the business models and system architecture.

Following initial processing, some or all of the sightings data from each sighting would be transferred from the processing unit to the NAVR either directly, or first to a RTA or other state body and then to the NAVR. Factors affecting the decision here include relevant state law, for example, whether an RTA could legally collect data not needed for its functions, whether sightings data will include images of vehicle occupants, whether these images can be stored at state level and whether there is sufficient "pipe" capacity to transfer images, other technological matters and cost.

The intention is also that some sightings data will be held in the NAVR for future analysis, for example, by law enforcement agencies for post-incident analysis, by national security agencies to identify threats, or by road transport agencies to identify patterns of road use. The analysis may use identified or de-identified data, depending on the agency and the agreed law and protocols.

CrimTrac has also assumed, for the sake of its modelling, that the NAVR would hold ANPR data for five years. The nature of data stored and the length of storage is a critical issue affecting both the privacy impact of the national system and the cost and nature of infrastructure required.

Using the assumptions above, CrimTrac has explored other aspects of the NAVR, in particular, how the central facility will connect to the jurisdictions and the extent to which processing will take place centrally or within jurisdictions. In the former case, at one extreme, each agency within each state could connect directly to the NAVR and, at the other extreme, the NAVR could connect to umbrella agencies such as Austroads and the Australian Federal Police. The decisions here would affect the nature of communications channels and infrastructure needed. CrimTrac is also exploring various architecture models. The models under consideration at this point are:

- **Option 1 – Central broker** is based on brokering data between autonomous systems. Each agency would hold its own sightings and hotlists. This option will involve technical and ongoing management complexity in accessing and sharing data in multiple and independent repositories, and it requires distributed copies of data and functions.

- **Option 2 – Central system** supports national operation through a single central system that holds all data and directly supports all users, but relies on all agencies committing to the central system architecturally.

- **Option 3 – Central repository and services, distributed systems** also supports national operation but, unlike Option 2, supports users locally and allows local processing in locally preferred solutions. Some level of duplication is inevitable with this option, and it is likely to be more expensive and more difficult to implement, but it recognises that many (if not all) agencies will require autonomy to fulfill their obligations.
Option 4 - Hybrid central and distributed systems is a hybrid approach that combines the features of Options 2 and 3. The option recognises that a decision on the best overall architecture model may depend more on business preferences regarding the business models associated with each option, as well as the varied ability of agencies to provision system capability. The assessment of the scoping study is that, in practice, a mix of options will be required. Many agencies will require the flexibility to provide a local ANPR capability in the manner that best suits local conditions but also allows participation at a national level, while others will require a packaged and externally supplied solution. A hybrid approach supports both categories of agency by providing the central and distributed system models concurrently, and is therefore likely to best meet overall requirements.

Again, governments' decisions about how and where they will process ANPR data will affect the nature of the infrastructure required, the communication channels and the cost and efficiency of the system.

In summary, IIS understands that CrimTrac is proposing a national ANPR system characterised by:

- a whole-of-government approach, meaning data is collected by road safety, law enforcement and national security agencies for their own purposes and also with a presumption of shared use of data, subject to permitted purposes/uses for each agency
- large-scale deployment of ANPR cameras (increase from around 300 cameras to approximately 4000 cameras nationally) focusing on critical infrastructure, main roads and other sites
- capture of all vehicle movements at each camera point
- the possible capture of high resolution images of vehicles for all sightings which may show occupants. Camera orientations will be a mixture of forward and rear facing
- a NAVR that will facilitate data sharing, subject to legal or other authorisation and access arrangements, possibly including by providing a central data store of some or all of the data and a copy of same or all of the data may also be held and used locally within state agencies
- the ability for the NAVR to offer authorised users the facility to link sightings data to registration and drivers licence registers managed by Austroads
- the ability for alerts lists created by state agencies to be shared by the jurisdictions, for example, Victoria may permit NSW to match its hotlists with Victoria's sightings
- the principle that unless the state law provides otherwise, sightings data will be 'owned' by the agency that collected it, regardless as to whether it is held in a state agency or in the NAVR
- the intention for the NAVR to hold sightings data for a significant period, noting that sightings data collected and held by the state agencies may be held for brief or long periods depending on the agencies' functions and governing law
- the principle that NAVR may include sightings from private sector organisations (toll road, petrol stations) but will not provide data to the private sector
- the fact that the NAVR will be subject to the federal privacy and other relevant law
- the fact that state agencies' collection, use and disclosure of sightings data will be subject to the relevant state privacy and other law.

IIS understands that if governments accept its proposals, CrimTrac will be proposing a phased implementation including a trial in one or two states for a reasonable period. CrimTrac would then undertake a full evaluation and make recommendations about any full implementation after that.
5  BENEFITS OF A NATIONAL ANPR SYSTEM

The community and decision makers will need to test the privacy impact of a national ANPR system against the possible benefits of the system. CrimTrac expects that a national ANPR system will deliver very significant benefits to the community in the areas of road safety, law enforcement and community safety. In general, these benefits derive from the use of information that has been collected state by state to manage road safety and law enforcement responsibilities on a national basis. The diagram below illustrates the concept.

![ANPR national strategic approach](image)

CrimTrac expects the system will deliver efficiency benefits and cost savings and, more importantly, significant improvements in road safety and policing. It has identified a significant number of benefit areas and is proposing to track and quantify the realised benefits of 38 of these areas should the proposals proceed to implementation. These benefit areas include:

- greater ability to detect and remove unregistered vehicles and unlicensed drivers from the road and, given that these vehicles are significantly more likely to be involved in accidents, consequent reductions in accidents, impact on the health system, insurance premiums etc
• financial savings, for example, through reduced investigation times, national procurement

• community safety and national security, for example, through enhanced road safety, enhanced investigation and intelligence effectiveness, reduction in crime and increased compliance with road transport and criminal legislation

• information sharing, for example, leading to better decision making and improved practices and strategies, and

• optimum resource utilisation, for example, because of reduced duplication of effort and improved ability to allocate resources.

Part of the work of the scoping study is to explore the evidence to support and quantify the perceived benefits, including by conducting an independent cost/benefits analysis. IIS understands that CrimTrac is also exploring general criminology studies that point to likely benefits, including for example, deterrence effects and the impact of increasing enforcement activity in relation to minor crimes on the frequency of more serious matters.

---

2 The cost/benefit study was under way at the time of this PIA and was not available as an input to the PIA. IIS understands that CrimTrac will publish the cost/benefit report as part of the scoping study report in late 2008.
Privacy is an important value for Australians, reflecting the country's history and culture. Discussion about privacy has been a regular part of Australia's discourse and there have been passionate debates and action on the issue. Australian governments have acted on the issue, reflecting Australia's commitment to international approaches on human rights and to increasing global movements of personal information. Australia's legal system includes an extensive framework of privacy and related law.\(^3\)

While privacy is clearly valued, Australians generally recognise that it is not an absolute right and that there will be times when other interests prevail. This feature of privacy, that is, the need to balance privacy and other interests, is illustrated, for example, in the Privacy Act 1988 (Cth). The Act requires the Privacy Commissioner to 'have due regard for...social interests that compete with privacy...and the recognition of the right of government...to achieve their objectives in an efficient way'.\(^4\)

Surveys of Australians' attitudes to privacy confirm their interest in privacy and show that they recognise that privacy rights may need to defer to other interests in some circumstances.\(^5\)

The current Australian Law Reform Commission Inquiry reviewing Australian privacy law includes detailed discussion of the concept of privacy.\(^6\) It divides privacy into a number of separate but related concepts:

- **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection'.
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches.
- **Privacy of communications**, which covers the security and privacy of mail, telephones, email and other forms of communication.
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.\(^7\)

While privacy law in Australia tends to focus on information privacy or 'data protection', the impact of a national ANPR system will clearly be broader. ANPR by its nature involves 'observing' vehicles and, in this case, creating records of those observations which can include information about

\(^3\) For example, see www.privacy.gov.au/privacy_rights/index.html\(^8\)

\(^4\) Section 29 Privacy Act 1988 available at www.privacy.gov.au

\(^5\) See www.privacy.gov.au/business/research/index.html\(^8\)

\(^6\) Information about the inquiry and copies of its issues papers and discussion papers are available at www.alrc.gov.au

particular individuals associated with the vehicle. These characteristics mean it can affect at least both territorial and information privacy.

6.1 General approach to privacy analysis

The focus of this PIA process has been on the privacy impact specifically in relation to a national ANPR system. The PIA does not provide a detailed analysis of the privacy impacts of ANPR generally, but does take account of such issues.

CrimTrac’s national ANPR system proposals are still under development and decisions are still being taken in relation to what it will recommend on a range of dimensions, including the extent of ANPR camera deployments, and whether some or all of the information will be stored centrally or in agencies in the jurisdictions. As a result, IIS’s discussion of the issues and the recommendations it makes are general and high level.

In assessing possible privacy impacts, the PIA is taking a broad view of privacy; this means that the assessment is not limited to the information privacy matters that are currently protected by Australian and state and territory privacy laws.

As is the practice for PIAs generally, this PIA aims to take account of the possible benefits of the proposals as well as their possible privacy impact. While these benefits could be very significant, at this stage in the process the benefits are articulated at a high level. CrimTrac’s cost/benefit analysis, which will be presented with its report, will provide further insights in this area.

As noted earlier, state and territory agencies are using ANPR primarily for road transport and road safety management, but also for some policing activities. A brief overview of activity in each state is at Appendix II.

In considering the privacy implications of the proposed national ANPR system, in the form of the NAWR, IIS has recognised that in the absence of such a system the states and territories are likely to continue to develop and deploy ANPR. They have, for example, participated in the CrimTrac scoping study and have indicated interest in reporting in the business requirements in possible areas of future activity. For the purposes of its discussion, IIS considered the possible situation 5 years out. Its observations are set out at Appendix III.

The proposals described so far in this report potentially raise a range of very significant privacy issues. The key issues are set out below. They are very serious and of a high-order privacy impact. Based on the issues identified, IIS has made a range of recommendations that it considers will mean decision makers can factor privacy into decisions about the proposals and to help mitigate privacy impact should a national ANPR system be implemented.

IIS will be recommending to CrimTrac that proposals for a national ANPR system that includes mass population level surveillance and recording of innocent vehicle movements should proceed only if strongly supported by the quantification of benefits and costs widely cost and reasonable consideration of alternatives.

CrimTrac
Responsive - Innovative - Accountable
Released by the CrimTrac Agency under the Freedom of Information Act 1982
6.2 Privacy issue analysis

6.2.1 SURVEILLANCE ASPECTS OF ANPR

Surveillance conducted by Australian governments will be for legitimate public purposes and its use will be subject to a range of checks and balances, in this instance, the intention is to promote road safety and community safety and effective law enforcement.

ANPR can be used in a targeted manner, where all sighting at a camera point are matched against 'hotlists' and information about matches is retained and all other information is discarded, or for mass surveillance, where information about all vehicle movement past a particular point is recorded or for points in between.

While CrimTrac's final proposals are not settled, it is considering the option of mass surveillance and recording of vehicle movements. The question as to whether an equivalent level of vehicle surveillance would develop in the absence of a national ANPR system is an open one. It appears very likely that the states and territories will expand on their current use of ANPR as they have contributed such views to the ANPR scoping process. However, it is difficult to say at this stage what the actual outcome would be. What is clear is that a move to mass surveillance of vehicle movements, whether driven nationally or at a state or territory level, would be a very significant change in the Australian environment.

The use of ANPR to collect information about vehicle movements is generally considered to be a form of surveillance, for example, by participants in this consultation process, and in reports on surveillance by the United Kingdom Information Commissioner, and the United Kingdom Home Affairs committee.9

Surveillance by its nature can have an impact on privacy, for example, the Home Affairs Committee Report took the view that:

*Engaging in more surveillance...erodes trust between citizen and state. In turn such an erosion of trust—with the citizen living under the assumption that he or she is not trusted by the state to behave within the law—may lead to a change in the reaction of the citizen and in his or her behaviour in interactions with other citizens and the Government.*

Other surveillance privacy impacts, of surveillance in general and in the context of these proposals, include that:

- it will result in records of information that may have the capacity when linked with other information to reveal people's movements, where they were and when and who they were with
- there is potential for incorrect inferences about individuals to be drawn from the information, at best meaning they have to take steps to sort out an issue and at worst resulting in a wrongful conviction
- it may intrude on people's sense of autonomy and space, and
- it may affect people's trust in and relationship with their governments.

The extent to which privacy risks will eventuate will depend on the nature of the final proposals and if and how they are implemented. It is extremely difficult to quantify the impact of surveillance. This is in part because privacy is an intangible concept. Moreover, the Australian community is likely to have a range of views about the use of ANPR to observe and record vehicle movements, whether by

---


9 See note 1 above.
the state and territories or linked in a national system. Some will welcome the initiative, others will consider it intrusive and abhorrent and there will be views in between.

In discussions during the PIA consultation phase, victims support groups in particular saw the possible benefits from the use of a national ANPR system in some policing contexts, for example, in remote locations such as forests where there had been prior incidents, or in monitoring vehicles near schools or pursuing kidnappers.

However, participants also identified a number of features of the proposals under consideration that they considered raised serious issues from a privacy perspective. Observations and comments included that:

- generally there will be no prior suspicion of any wrongdoing, rather the surveillance would be a ‘fishing expedition’
- if a mass surveillance approach is adopted, the vast majority of the information collected will be about ‘innocent’ vehicle movements
- the routine inclusion of images of vehicle occupants in the information retained in relation to ‘innocent’ vehicle movements would take the proposals to a new and serious level of intrusion
- extensive data collection such as this tends to facilitate government thinking the worst of its citizens, and equally citizens to lose trust in their government
- an extensive data collection such as this inevitably will result in information misuse
- the potential for a mass surveillance to affect people’s behaviour, including a so called ‘chilling’ effect
- there may be effects such as reduced citizen self-enforcement if community attitudes reduce to you can get away with it, do so ‘in response to a sense of living in a surveillance society, community abrogates its responsibility back to government, and
- a strong sense that there was insufficient information at this point, for example, in relation to the specific objectives for the system, the nature of problems to be addressed, or assessment of cost and benefits, to decide if the proposals were a proportionate response to identified problems and therefore justified despite the possible impact on privacy.

The proposals may also have other impacts on the relationship between the individual and the state, including expanding on the circumstances where the onus of proof is reversed to guilty until proven innocent, an approach already taken with red-light cameras and some speeding ticketing. A question to consider is whether this is appropriate for a less targeted system or mass surveillance system.

A factor to consider is that Australian agencies already undertake a range of surveillance activities. These include:

- public and private sector video surveillance
- as already noted, some use of ANPR for toll roads payments and for heavy vehicle monitoring etc, and
- financial reporting under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 which requires a range of institutions to routinely report large financial transactions as well as ‘suspicious’ transactions to AUSTRAC.15

These initiatives have not been uncontroversial or uniformly accepted. However, in some circumstances, Australians have been moderately accepting of some forms of surveillance.

15 For information about the anti-money laundering and counter-terrorism financing scheme see www.austrac.gov.au/
For example, a survey on community attitudes to privacy conducted by the Office of the Privacy Commissioner in 2007 found that amongst those aware of CCTV cameras, 79% are not concerned about their use in public places.\textsuperscript{11} However, only about 20% of the survey respondents were comfortable with organisations or agencies other than the police viewing the CCTV footage.

The current proposals also need to be considered in terms of Australia’s obligations as a party to the international instruments on human rights, for example, the International Covenant on Civil and Political Rights (ICCPR). Relevant provisions of the ICCPR include:

- article 17, which provides that no one shall be subjected to arbitrary or unlawful interference with his privacy
- article 12, which provides for freedom of movement
- article 22, which provides for freedom of association.\textsuperscript{12}

The Privacy Act 1988, state privacy laws, and the ACT Human Rights Act 2004 and the Victorian Charter of Human Rights and Responsibilities Act 2006 respond in part or reflect these obligations. They will require consideration both in terms of whether any proposed ANPR law is consistent with the state laws and whether ANPR activities can be conducted consistently with the law.

A factor that may come into play in considering the human rights implications of ANPR proposals is people’s reasonable expectation of privacy in public places. Some argue that people should not expect any level of privacy in places. However, community expressions of concern, for example, about the use of mobile phones to take photos on beaches or other public places, and government action to set rules about the use of video surveillance, suggest that Australians continue to expect a level of privacy in public spaces.

IIS considers that all of the issues raised so far point to the view that mass population level surveillance and recording of vehicle movements, and particularly the routine capture of images of vehicle occupants, raise very serious privacy issues with the potential to have a high-order privacy impact.

IIS has made a range of recommendations to CrimTrac, including that proposals for a national ANPR system that include mass population level surveillance and recording of innocent vehicle movements should proceed only if strongly supported by the quantification of benefits and costs widely cost and reasonable consideration of alternatives.

If a national ANPR system is to proceed, IIS has also made recommendations that aim to allow for a measured decision making process and to minimise the impact on citizens and on the relationship between citizens and their governments. The recommendations that address the specific issues raised in this discussion are:

- **RECOMMENDATION 1 – DECISION TO PROCEED WITH ANPR REQUIRES STRONG JUSTIFICATION**
- **RECOMMENDATION 2 – NATIONAL ANPR SYSTEM TO BE LIMITED TO SIGNIFICANT ROAD SAFETY, LAW ENFORCEMENT AND NATIONAL SECURITY MATTERS**
- **RECOMMENDATION 3 – IMAGE OF VEHICLES AND THEIR OCCUPANTS**
- **RECOMMENDATION 4 – DATA MINIMISATION**
- **RECOMMENDATION 6 – FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION**

\textsuperscript{11} Waitis Consulting Group Pty Ltd, Office of the Privacy Commissioner, Australia Community Attitudes to Privacy, 2007, page 74 www.privacy.gov.au/business/research/index.html#b

\textsuperscript{12} http://www2.shcr.org/english/law/ccpr.htm
6.2.2 COLLECTING IMAGES OF VEHICLES INCLUDING OCCUPANTS

In its first briefings, CrimTrac advised IIS that it was considering routine collection of vehicle images that may include images of front or back seat passengers, depending on which way the ANPR camera is facing. CrimTrac indicated that some user agencies had advised, for example, that it would be highly desirable for sightings data to include ‘a clear image of the whole vehicle frontage to allow the identification of the driver and/or front passengers which is at a resolution that can be used as court evidence’.

In discussions with community, civil society and regulator representatives, this aspect of the proposals evoked strong views; the groups considered the routine inclusion of images of people was intrinsically more intrusive, revealing associations, movements and possibly impinging further on society’s sense of privacy. The groups noted the possible benefits to individuals, for example, in proving that they were not responsible for an infringement notice. However, the groups felt that these benefits alone were unlikely to make the case for routine collection of vehicle images that may include images of innocent Australians. There was also considerable discussion about the extent to which states and territories were currently collecting, or were likely in the future to collect, vehicle images that may include occupants. While noting some RTAs had expressed interest in images of vehicle occupants, the groups felt that there would need to be more examination of the circumstances and extent to which such images would be necessary for current road safety functions.

IIS also considered that this threshold is very significant and recommends that the collection of images of vehicles, including occupants, needs explicit consideration and justification. CrimTrac has now advised that its proposals are likely to recommend only limited inclusion of vehicle images in the NAVR. Its approach will be influenced by a range of factors, including technological capacity to transmit images, cost of data storage and privacy concerns. Its proposals are now likely to take the following approach:

- for each sighting, some data that is the text string and plate patch to be transferred and held in the NAVR
- for each sighting, an image of the vehicle, possibly including vehicle occupants, would be taken and held locally
- sightings data would be evaluated centrally or locally and, where the evaluation resulted in an alert, the text string, plate patch and image of vehicle would be transferred to the NAVR
- non-matched images would be held locally for a short period, possibly 7 days and if, following that period, there were no further alert that would trigger a request from NAVR for the vehicle image, then the images would be destroyed, and
- vehicle images would be transferred to the NAVR in high resolution format for a period, possibly 30 days, and then, unless needed at high resolution, would be converted to low resolution for storage.

IIS considers this approach will have a less although still significant impact on privacy. It considers this aspect of the proposal still needs to be subject to further consultation to establish community views and expectations and privacy impact testing in the context of more fully developed proposals. IIS has made the following recommendations to CrimTrac to assist in further development work:
6.2.3 UNIVERSAL COLLECTION VERSUS TARGETED COLLECTION

As noted earlier, the scoping study is likely to propose mass surveillance of vehicle movements with universal collection of information relating to vehicle sightings. This represents a change from the current general approach in the states and territories that largely focuses on matching sightings against hotlists to identify particular vehicles and discarding unmatched information. CrimTrac explains that this change in approach results from the general concept of the national ANPR system, which it has predicated on data sharing and leveraging, and the range of 'business requirements' identified by state and territory road transport and law enforcement agencies consulted in the scoping study process.

This aspect of the proposals was of significant concern to community, civil society and regulator representatives; they saw a distinction between passive collection of all sightings past a camera point and active collection based on a match against a hotlist. The groups' concerns centred on:

- the lack of a quantified benefits supporting the approach
- the nature of the 'business requirements' – were they in fact requirements or more desirable elements that would need further assessment against cost, law, privacy impact, etc
- the fact that objectives for road safety, law enforcement and national security were 'bundled' together, meaning that the information needs for the system would be set by the area with the greatest need for information.

The groups' perception was that interest in 'ability to interrogate aggregate national data to aid investigation, intelligence gathering and road use analysis' seemed most dependent on universal collection of ANPR data. It would be looking for clearer objectives and justification, particularly in relation to this capability.

Some of the people consulted considered that the most privacy sensitive approach would be to hold hotlists at or near the ANPR camera that took the sightings and discarding at this point all sightings that the processing unit did not immediately match.

As noted earlier, IIS considers that the passive universal collection of ANPR information is likely to be significantly more privacy intrusive than a targeted approach, raising high-level privacy concerns. It considers that this aspect of the proposal should be subject to further consultation and privacy impact testing in the context of more fully developed proposals. IIS has made the following recommendations to CrimTrac on the issues here:

- **RECOMMENDATION 1** – DECISION TO PROCEED WITH ANPR REQUIRES STRONG JUSTIFICATION
- **RECOMMENDATION 2** – NATIONAL ANPR SYSTEM TO BE LIMITED TO SIGNIFICANT ROAD SAFETY, LAW ENFORCEMENT AND NATIONAL SECURITY MATTERS
- **RECOMMENDATION 4** – DATA MINIMISATION
- **RECOMMENDATION 6** – FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION
6.2.4 OBJECTIVES, PURPOSES, PROPORTIONALITY

CrimTrac's scoping study is an exploratory one intended to serve legitimate community goals. It is testing the proposition that there could be significant benefits from a whole-of-government approach to ANPR in the areas of road safety, law enforcement and national security. The national approach to ANPR is expected to assist agencies in meeting their strategic objectives, which include addressing problems such as reducing serious and fatal crashes; reducing non-compliance with road rules; reducing the number of stolen vehicles; and reducing and preventing crime.

In effect, the scoping study is building a case from the bottom up; identifying possible uses, benefits and costs as well as possible system architectures and ANPR technologies. This approach clearly has the potential to mean that the Australian community reaps benefits that may not otherwise have emerged. However, there is also the risk that because the scoping study in effect starts with the notion of a national ANPR system and with high-level, unquantified objectives, there is not a clear benchmark against which to assess impacts. It is also possible that there may have been other ways to address the problems that may be cost-effective and less privacy intrusive.

In consultation discussions, the groups felt that the objectives were very broad and high level and they saw this as a key issue from a privacy perspective. The groups recognised that the proposals were at an early stage. However, they also observed that this made it difficult to consider questions such as:

- What is the overwhelming need?
- What alternatives have been considered?
- How can it be best achieved to be compatible with human rights?
- What are the checks and balances?

In addition, under the proposals agencies with responsibilities in a specific area will be collecting ANPR data for their own purposes and then providing it to support combined road safety, community safety and law enforcement goals and purposes. The problem here from a privacy perspective is that at the point of collection there may not be a clear link between the information collected (for example, for managing a bus lane regulation) and the way diverse user agencies later use it (for example, for research road use behaviour or for criminal investigations). Unless governments and agencies implementing proposals pay particular attention to public education and information, the community may not expect or accept the additional uses. This is particularly significant given that individuals will have no choice about whether ANPR information is collected.

The groups consulted considered it significant that, up to the point of this PIA, CrimTrac has developed its proposals from the perspective of only one set of stakeholders, that is, government agencies that may provide and/or use ANPR information. The groups considered that a wider concept of stakeholders is likely to produce a wider range of issues and different considerations in testing whether desired collection of ANPR data is justified given the impact on individual privacy.

IIIS considers that a clearer set of objectives will mean that the proposals can be focused and targeted; it also considers that a clear set of objectives is necessary to a full consideration of the privacy impacts of a national ANPR system. IIIS has made the following recommendations to CrimTrac to assist if the proposals proceed to further development work:

- **RECOMMENDATION 1** – DECISION TO PROCEED WITH ANPR REQUIRES STRONG JUSTIFICATION
- **RECOMMENDATION 2** – NATIONAL ANPR SYSTEM TO BE LIMITED TO SIGNIFICANT ROAD SAFETY, LAW ENFORCEMENT AND NATIONAL SECURITY MATTERS
- **RECOMMENDATION 4** – DATA MINIMISATION
6.2.5 ANPR BENEFITS

As noted earlier, CrimTrac expects that a national ANPR system will deliver very significant benefits to the Australian community in the form of financial savings, improvements in community safety and national security, better decision making and improved practices and strategies. In discussions, CrimTrac also noted specific instances where information sharing between states would enhance investigations or promote safety for police, or where targeted mass surveillance provided clear benefits.

In the PIA consultation discussions, groups saw the question of the possible benefits of a national ANPR system as being a critical factor in their ability to make informed comment about a national ANPR system. The groups noted that a cost/benefit analysis is being undertaken and welcomed this step. However, they considered that benefits cannot be properly addressed in the absence of clear objectives and that an assessment of costs and benefits will be meaningful only if the costs and benefits are cast as widely as possible. The groups considered, for example, that an appropriate cost/benefit analysis would include:

- the cost of privacy impacts on individuals, for example, the possible increase in number of people who may need to take action, including court action, to prove they were not the driver of a particular vehicle and the overall impact on social trust and cohesion
- impact on resources available for current road safety initiatives at state and territory levels and law enforcement initiatives
- hidden costs to agencies, for example, administrative costs, data security cost, additional responsibilities or duties of care that arise for agencies as they hold or have available more and richer information about citizens
- cost of regulation, including increased resources needed by regulators and by those regulated in order to attain compliance such as audit functions, complaints investigation and resolution etc, and
- cost of ensuring that responsible and transparent decisions are made about proposed further uses of the information held in the ANPR system.

IIS agrees that such a cost/benefit analysis is an important step. However, developing an empirically based realistic picture of the overall benefits of a national ANPR system will not be an easy task. In part, this is because there is limited empirical data relevant to Australian proposals on the broad impacts of ANPR.

Law enforcement agencies in the United Kingdom make extensive use of ANPR and there have been assessments of its effectiveness in that context. For example, the evaluations assert that ANPR increases police efficiency on particular operations two to three times. While these results are positive, they are not directly applicable to the Australian context. In addition, it is not clear that the same benefits would accrue in the road safety area. Watson and Walsh in their submission to the Queensland Travelsafe Committee Inquiry into ANPR did not give unqualified support for the introduction of ANPR in the road safety context, raising issues including:

- resources needed to process the ANPR results


- the impact on resourcing of other effective road safety programs
- the nature of ANPR deployment (whether targeted, overt etc) on its deterrence effects, and
- the potential impact of practices such as vehicle cloning (where the number plate of a law-abiding person's vehicle, that is similar to the criminal's, is either illegally purchased or copied and attached to the criminal's vehicle).13

This very brief review suggests that decision makers need to approach consideration of the possible benefits of a national ANPR system with caution.

IIS notes that CrimTrac is committing to track 38 benefit areas should the proposal proceed to implementation. It is also proposing a phased implementation process with detailed evaluations at each stage.

In general, IIS supports this approach. Its recommendations to CrimTrac include:

- **RECOMMENDATION 1 – DECISION TO PROCEED WITH ANPR REQUIRES STRONG JUSTIFICATION**
- **RECOMMENDATION 6 – FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION**

### 6.2.6 WHOLE-OF-GOVERNMENT AND NATIONAL APPROACH

A whole-of-government approach has much to commend it, especially when it can bring together the disparate needs and perspectives of the various levels of government in Australia. Some of the groups involved in the PIA consultation process saw potential value in a centralised, strongly regulated system as opposed to ANPR use developing on an ad-hoc state-by-state basis.

In terms of privacy impact, in this instance there are risks that also need to be considered transparently and, if they are not to have a negative impact on privacy, to be managed. These risks include:

- a whole-of-government approach that may lead to more collection of more information and longer data retention than would be the case if each agency in each state deployed ANPR for its specific functions and purposes
- the impact on individual agencies of collecting more data than they need for their own purposes, including the impact on trust, perceptions of how they carry out their functions, the possibility of misuse and reduced individual control
- the risks to citizens arising from extensive information sharing across jurisdictions, potentially including lack of clear responsibilities and accountabilities for data accuracy, audit and redress of error
- the possibility that the approach will lead to a lowest common denominator result across the proposed ANPR system, for example, if transparency requirements are reduced to those appropriate for national security even when the data is used for traffic or other minor infringements, and
- the possible impact on the scoping study and ANPR implementation processes of the fact that CrimTrac is a central executive agency with a law enforcement focus and no direct role with the community its decisions affect.

---

IIS has made the following recommendations to CrimTrac which focus on decisions about whether to proceed with a national ANPR system, what information is included in the system and how it might be used.

- **RECOMMENDATION 1** - DECISION TO PROCEED WITH ANPR REQUIRES STRONG JUSTIFICATION
- **RECOMMENDATION 6** - FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION
- **RECOMMENDATION 9** - RIGOROUS FRAMEWORK ESTABLISHED IN LAW
- **RECOMMENDATION 11** - GOVERNANCE, ACCOUNTABILITY AND TRANSPARENCY

### 6.2.7 EXPANDEDUSES (FUNCTION CREEP)

A key privacy risk associated with initiatives involving personal information, particularly where collecting information about individuals into large data holdings, is the risk of what commentators commonly call 'function creep'. This is often characterised as any kind of change in the use of personal information that the collecting agencies, and the community, did not envisage at the time they introduced the initiative. The likelihood of function creep increases with the 'attraction' of the information, including, for example, how much information is collected and how easy it is to link to other information.

IIS takes the view that not all changes in uses of information will necessarily be bad, and so not all changes deserve the negative connotations associated with the term 'function creep'. Whether or not changes or expansions of use of personal information will be welcomed by the wider community or considered to be unwelcome 'function creep' will depend on the kind of changes in use, and how those changes are made. At times, perceptions of function creep may result from lack of attention to more fundamental governance mechanisms relating to transparency and accountability. In these cases, the community may require more concrete measures to ensure abuse and unintended consequences do not occur before they are willing to accept changes. In other instances, the change is simply insidious and deserves no other label than 'function creep'.

There is evidence that the possibility of expansion in use of ANPR is a real risk. For example, Australia has experienced expansions in the use of tax file numbers and in the financial information held by the Australian Transaction Reports and Analysis Centre.

A national ANPR system could create significant new information holdings about individuals and there may be increasing impetus for governments and others to make wider use of this rich set of data. The discussion in the consultation process identified this as a very significant privacy risk in view of the following factors:

- individuals have no choice about the collection of information about their vehicle movements and the information may be used for purposes outside the context in which the information was collected
- the sheer amount of information to be collected and held for quite lengthy periods
- the presumption of data sharing, and
- a drift towards a society where the presumption of innocence is eroded, as a particular manifestation of function creep.
IIS, and the groups it consulted, consider the routine inclusion in the NAVR of high-resolution images of vehicles with images of vehicle occupants for all sightings would significantly increase the privacy risk.

The consultation discussion focused on avoiding function creep by avoiding the collection in the first place, in particular by adopting an active targeted, rather than a passive, universal collection approach or by limiting the information held in a central database. Other approaches discussed included having well-defined objectives and purposes for ANPR systems, and having strong governance and accountability measures, including a clear process to govern change in use over time.

IIS agrees that these approaches are helpful and has made the following recommendations to CrimTrac, suggesting a series of measures starting with a careful process to take decisions to proceed with a national ANPR system:

- **RECOMMENDATION 1** – DECISION TO PROCEED WITH ANPR REQUIRES STRONG JUSTIFICATION
- **RECOMMENDATION 2** – NATIONAL ANPR SYSTEM TO BE LIMITED TO SIGNIFICANT ROAD SAFETY, LAW ENFORCEMENT AND NATIONAL SECURITY MATTERS
- **RECOMMENDATION 3** – IMAGE OF VEHICLES AND THEIR OCCUPANTS
- **RECOMMENDATION 6** – FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION
- **RECOMMENDATION 9** – RIGOROUS FRAMEWORK ESTABLISHED IN LAW
- **RECOMMENDATION 11** – GOVERNANCE, ACCOUNTABILITY AND TRANSPARENCY

### 6.2.8 PRIVACY LAW AND OTHER PRIVACY PROTECTION

Part of a PIA will be the extent to which legal or other privacy protections can offset the impact of an initiative.

There are currently significant variations in the approach to privacy protection applying to personal information held by agencies of the Australian Government and the states and territories [see, for example, the brief comparison in the table in Appendix IV]. In particular, there are variations with respect to whether:

- there is a privacy scheme of any sort
- the privacy scheme is implemented in law or administratively
- there is a privacy regulator with oversight of the scheme
- there is a process for individuals to pursue complaints, and
- whether the scheme applies in full or in part to law enforcement agencies.

These variations in approach are significant in the context of a national ANPR scheme in that it is possible that information collected in one jurisdiction could be used in a jurisdiction with a lower standard of privacy protection, which could expose individuals to more risk or less opportunity to raise issues of concern. In consultation discussions, people saw this as an issue, in particular because of the absence of a privacy regulator in a number of jurisdictions.

The current privacy law and arrangements do set important expectations for the handling of personal information and reflect the value Australians place on privacy. However, it is also
important to note that where privacy principles are in place, whether or not law and formal redress mechanisms back them, there are general and minimum standards. The principles leave judgements about, for example, what might be reasonable steps to ensure that... the individual concerned is generally aware of... the purpose for which the information is collected or 'protect the personal information... from misuse and loss and from unauthorised access, modification or disclosure' to the responsible agency. This means that privacy principles and laws by themselves, even where they are in place, will not necessarily provide the full answer to privacy issues in the national ANPR context.

On the other hand, a national ANPR system may put pressure on the protection structure offered by privacy principles. For example, privacy principles generally aim to limit collection, use and disclosure of personal information, particularly where the individual does not have direct control. The mechanisms include testing as to whether the collection of information is likely to be considered 'necessary' for an agency's functions or activities, and limiting use of information to the purpose for which it was collected or related purposes, unless there are exceptions, including authorisation by law.

To the extent that the ANPR proposals seek to encourage state agencies to collect information that they do not need directly for their function, the proposals would be contrary to privacy principles. While technically such collection could be authorised by changes in agencies' governing law or privacy law, it would be a significant contributor to risks to privacy.

IIIS considers that, in the light of these considerations, if governments proceed with a national ANPR system they should establish a legal framework containing the principle that agencies should collect information about vehicle movements only where this is strictly necessary for their functions. It has made the following recommendations to CrimTrac.

- **Recommendation 1 - Decision to Proceed with ANPR Requires Strong Justification**
- **Recommendation 9 - Rigorous Framework Established in Law**

### 6.2.9 Data Retention

The length of time that personal ANPR information is stored by state agencies and in the national ANPR system will be another critical factor in the privacy impact of the system. In this regard, it is important to note that the states and territories are generally discarding ANPR data at the point of collection unless it relates to a particular incident. A national ANPR system potentially significantly increases the long-term storage of ANPR data.

In consultation discussions, people observed that the longer information is held the greater the security risks, the more potential for function creep and the greater the risk that incorrect or inappropriate inferences will be made on the basis of the data. People queried the proposed 5-year retention period, noting that it seemed to be arbitrary rather than based on evidence or research. They also thought that the third capability proposed for the CrimTrac system, which is the ability to interrogate aggregate national data to aid investigation, intelligence and road use analysis, appeared to require a big jump in the retention period for data.

IIIS has made the following recommendations to CrimTrac, which aim to have decisions made on the basis of clear objectives, are evidence-based and which are consistent with the first purpose for which information is collected.

---

15 CrimTrac PIA workshop presentation.
6.2.10 DATA SECURITY RISKS

Should the national ANPR system proceed, security is again a critical element in mitigating privacy impact and risk. The national ANPR system is likely to introduce new and increased security risks. Factors affecting security risks include:

- the fact that the more data held increases the potential for misuse
- the greater range of sites from which data will be collected, processed and transmitted
- that new holdings of alerts and possibly hotlists in the NAVR raise new risks in the course of transmission and storage
- the increased emphasis on data sharing leading to greater amounts of information being transmitted between the states and territories, as well as to the NAVR.

On the other hand, if implemented, with a focus on consistent national standards based on a thorough risk assessment and with adequate resources, the national ANPR approach may also have the potential to improve the overall security for holdings of ANPR data. The scoping study work on benchmarking ANPR systems and considering system standards is an important aspect of the study and should be an important safeguard. Further work on security standards is likely to be needed in relation to hotlists and storage of ANPR data in the jurisdictions and in relation to transmission security.

Security of ANPR data was an area of strong concern in the consultation discussions, in particular the potential for misuse of the information. It was noted that it is probably not possible to guarantee that the NAVR will be free of security breaches, including misuse by staff members, or incidents arising through human error or technological failure, or external threat. A number of recent high-profile cases of police corruption or misadventure were mentioned, including the Office of the Victorian Privacy Commissioner investigation reported as Jenny’s case.16 It was also noted that the collection and retention of images of vehicle occupants possibly adds to the risk of security breaches or misuse.

IIS notes that the strategy of making individuals aware of security breaches so that they can take any steps necessary to protect themselves and their reputation is increasingly being adopted by international governments and is also being considered in the current Australian Law Reform inquiry into the Privacy Act.17 The Office of the Privacy Commissioner has also recently released a draft Voluntary Information Security Breach Notification Guide for comment.18

IIS has made the following recommendations on data security, including on data breach notification, to CrimTrac:

- RECOMMENDATION 10 - SECURITY AND ACCURACY

6.2.11 DATA ACCURACY RISKS

The attention paid to accuracy issues at all stages in the ANPR process is one of the key factors in assessing and managing the privacy risks from the process.

Accuracy issues start at the point where the camera captures an image of a vehicle and optical character recognition software is used to locate the number plate within the image and then convert the number plate value to a text string. While the image will be a factual record of the event, there are factors at this point that may affect the accuracy of the conclusions drawn from the image, including whether the number plate itself is obscured or damaged, or other factors such as light or weather affect the quality of the image of the vehicle and/or the occupants, whether it relates to a 'cloned' vehicle number plate, and whether the number plate data extracted are the same as a plate allocated by another jurisdiction. Accuracy continues to be a potential risk in the process of matching sightings to hotlists, for example, a list of registered vehicles, to generate infringement notices or alerts, or where sightings data is used, for example, in the course of police investigations.

IIIS understands that the ANPR data matching process will involve adjudication of sightings by a person if there are questions about the validity of the match. It also appreciates that accuracy issues are being considered as part of the scope study and that CrimTrac's report is likely to include recommendations in relation to accuracy, including, for example:

- technical equipment benchmarks, standards and procurement processes, and
- providing resources to Austroads to improve the accuracy and timeliness of updates of the National Exchange of Vehicle and Driver Information System (NEVDIS) database.

The consultation discussions identified information accuracy as a potential critical issue for the NAVR system. There was a fair degree of concern that, unless accuracy standards were given priority and there were appropriate resources to deal with accuracy issues, there were real risks for many citizens. The discussion noted, for example, that ANPR literature suggests that technology is estimated to be between 60%–93% effective at correctly identifying every vehicle in a stream of traffic following processing that is taking an image, data matching and visual adjudication by an operator. The discussions also drew on the experience of the participants, for example, reviews undertaken by the Victorian Ombudsman of the Victorian drivers' licence and vehicle registration systems which identified a range of problems, including out-of-date, incomplete or fraudulent registration records.19

A compounding factor is that, if the system proceeds on the basis of universal surveillance and universal recording of sightings, the majority of the information collected will be about innocent vehicle movements. In addition, the massive increase in the amount of data collected has real potential to mean that there will also be a massive increase in the number of inaccurate matches, which may lead to people being pulled over or sent infringements for crimes or matters for which they are not responsible and where they are considered 'guilty' unless they can take steps, including court action, to sort things out.

While acknowledging that the current proposal does not include facial recognition, the consultation discussions did note the call for images of vehicle occupants to be a sufficient resolution to allow facial recognition technology to be used at some point in the future. This also raises accuracy issues, including the risk of false positives.

The consultation discussions suggested that the system should be designed and resourced with high standards of accuracy in mind. Approaches should include legal requirements, including limiting access to data to agencies that can demonstrate their data is accurate, and standards in relation to accuracy and currency of items on hotlists. Consideration should be given to building in

incentives for agencies to focus on accuracy, including published accuracy audits, the presumption that infringements will be waived where agencies fail to meet specified standards of accuracy, and public reports.

ILS has included these elements in its following recommendation to CrimTrac.

- **RECOMMENDATION 1 - DECISION TO PROCEED WITH ANPR REQUIRES STRONG JUSTIFICATION**
- **RECOMMENDATION 2 - NATIONAL ANPR SYSTEM TO BE LIMITED TO SIGNIFICANT ROAD SAFETY, LAW ENFORCEMENT AND NATIONAL SECURITY MATTERS**
- **RECOMMENDATION 4 - DATA MINIMISATION**
- **RECOMMENDATION 6 - FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION**
- **RECOMMENDATION 8 - DATA RETENTION**
- **RECOMMENDATION 9 - RIGOROUS FRAMEWORK ESTABLISHED IN LAW**
- **RECOMMENDATION 10 - SECURITY AND ACCURACY**
- **RECOMMENDATION 11 - GOVERNANCE, ACCOUNTABILITY AND TRANSPARENCY**
- **RECOMMENDATION 12 - SAFETY NET AND COMPLAINT HANDLING**

### 6.2.12 SYSTEM ARCHITECTURE

Decisions about the system architecture can have an impact on privacy in that they may influence where ANPR data is processed and stored, and how much information is collected and retained. As noted earlier in this document, CrimTrac is exploring four system architectures for the purposes of this scoping study. These are:

- **Option 1 - Central broker** is based on brokering data between autonomous systems. Each agency would hold its own sightings and hotlists. This option will involve technical and ongoing management complexity in accessing and sharing data in multiple and independent repositories, and it requires distributed copies of data and functions.

- **Option 2 - Central system** supports national operation through a single central system that holds all data and directly supports all users, but relies on all agencies committing to the central system architecturally.

- **Option 3 - Central repository and services**. Distributed systems also support national operation but, unlike Option 2, supports users locally and allows local processing in locally preferred solutions. Some level of duplication is inevitable with this option, and it is likely to be more expensive and more difficult to implement, but it recognises that many (if not all) agencies will require autonomy to fulfil their obligations.

- **Option 4 - Hybrid central and distributed systems** is a hybrid approach that combines the features of Options 2 and 3. The option recognises that a decision on the best overall architecture model may depend more on business preferences regarding the business models associated with each option, as well as the varied abilities of agencies to provision system capability. The assessment of the scoping study is that, in practice, a mix of options will be required. Many agencies will require the flexibility to provide a local ANPR capability in the manner that best suits local conditions but also allows participation at a national level,
while others will require a packaged and externally supplied solution. A hybrid approach supports both categories of agency by providing the central and distributed system models concurrently, and is therefore likely to best meet overall requirements.

A possible issue to consider in the privacy context is whether data is distributed or held in a central database. Some participants in the consultation process considered that a central database is more likely to be a 'honey pot' attracting interest in new or expanded uses of the data. IIIS considers that the increasing power for IT systems to combine and process data in different systems is making less of an issue. However, it does consider the issue needs further consideration if the proposals proceed. As noted earlier, there were also strong views about the location of ANPR processing, with the suggestion that local processing, with non-matched results discarded, was likely to lead to the least privacy impact. This view was also reflected in the Xmax report.

IIIS has made the following recommendation to CrimTrac in relation to these issues:

- **RECOMMENDATION 6 - FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION**

### 6.2.13 BUSINESS MODEL

Using the assumptions above, CrimTrac is now exploring other aspects of the NAVR, in particular how the central facility will connect to the jurisdictions and the extent to which processing will take place centrally or within jurisdictions. In the former case, at one extreme each agency within each state could connect directly to the NAVR and at the other extreme the NAVR could connect to umbrella agencies, for example, Austroads and the Australian Federal Police. The decisions here would impact on the nature of communications channels and infrastructure needed. IIIS considers that in making decisions about the approach CrimTrac should undertake a full security risk assessment of the options. It has made the following recommendations to CrimTrac.

- **RECOMMENDATION 6 - FURTHER DEVELOPMENT OF PROPOSALS TO INCLUDE CONSULTATION, TRIALS AND EVALUATION**

- **RECOMMENDATION 10 - SECURITY AND ACCURACY**

### 6.2.14 GOVERNANCE AND ACCOUNTABILITY

As has been noted earlier, the risk of misuse of data or security breaches in relation to large databases of sensitive information (as the NAVR will be) is quite high, based on recent experience. The extent to which assurances about future uses of ANPR data, access and security arrangements are delivered is likely to be an important factor in the community trust in and acceptance of a national ANPR system.

Good governance and accountability arrangements will be a vital part of ensuring that promises can be delivered. Such arrangements include the operation of law, oversight by independent external regulatory bodies, internal management structures, policies and procedures and technology.

There are a number of fundamental accountability and governance issues for a national ANPR system. These are that:

- the accountability for multi-jurisdictional activities can be significantly weaker than the governance and accountability arrangements within jurisdictions. This has been recognised, for example, in a report on review of Part 1D of the Crimes Act by the Standing Committee of Attorneys-General in the context of the national DNA database;\(^2\)

---

tt1914-Forensicprocedures-March2003
• in a multi-purpose system including national security, there may be a tendency to design
governance and accountability systems for the most sensitive element, with a resulting
reduction in transparency and redress

• unless limited in accordance with the recommendations of this PIA, the very significant
increase in the size of the data collections compared with current systems will result in a
correspondingly significant increase in the number of errors occurring annually, even if error
rates are reduced from the current sometimes unsatisfactory rates to world best practice

• unless limited in accordance with the recommendations of this PIA, the vast bulk of the data
will relate to innocent movements by innocent citizens going about their daily lives

• as a consequence of these factors, the bulk of the errors in the system will also relate to
innocent citizens.

Other factors that need to be considered include:

• the need for governance and accountability mechanisms to provide for a well-resourced
regulator with ability to audit the collection and handling of ANPR data

• the need to ensure that regulators are able to share information and resources so that
oversight and investigation powers are equal to the data sharing arrangements of the system
across agencies and across jurisdictions and match within-jurisdiction capabilities.

IIIS has made the following recommendations to CrimTrac.

• RECOMMENDATION 4 – DATA MINIMISATION
• RECOMMENDATION 11 – GOVERNANCE, ACCOUNTABILITY AND TRANSPARENCY

6.2.15 SAFETY NET AND COMPLAINT HANDLING

Most significantly, if the proposal proceeds as a universal surveillance model, the majority of the
information in the NAVR will relate to innocent vehicle movements. If this issue is not factored into
the proposals in all of the ways suggested in the recommendations, but most particularly in relation
to safety net and complaint handling arrangements, the risks of the process will, by default, fall on
individuals.

Consultation discussions revealed that the elements needed to ensure an effective safety net
arrangement include that individuals can access ANPR data relevant to them and that there should
be mirror arrangements for individuals and agencies; to the extent that the system facilitates
access and data sharing for agencies the same level of ease should be available for individuals. The
aim is for user-friendly complaint handling, where the agency responsible is clear and accessible
and redress is law cost and swift. Where the responsible agency is not clear, it was suggested that
CrimTrac might act as a nominal defendant.

IIIS has made the following particular recommendations to CrimTrac to ensure that there are
effective safety net arrangements for a national ANPR system.

• RECOMMENDATION 9 – RIGOROUS FRAMEWORK ESTABLISHED IN LAW
• RECOMMENDATION 12 – SAFETY NET AND COMPLAINT HANDLING
6.2.16 POSSIBLE PRIVATE SECTOR INVOLVEMENT

As has been noted earlier, the scoping study is likely to include recommendations that private sectors organisations should not be permitted to access the NVIR system, although information collected by private sector organisations or using cameras located on private sector sites is still a possibility.

Consultation discussions did indicate this was a strong area of concern with the conclusion that the community should be made aware of the possibility of any inclusion of ANPR data collected by private sector organisations. Any decisions to permit ANPR data to be used for private sector purposes should be subject to extensive public consultation and authorised by law.

IIIS has made the following recommendation to CrimTrac:

- **RECOMMENDATION 5 – PRIVATE SECTOR INVOLVEMENT**
7 APPENDIX I - PIA METHODOLOGY

7.1 Information drawn upon

In gathering information for this PIA, IIS referred to the following documents:

<table>
<thead>
<tr>
<th>DOCUMENT NAME</th>
<th>AUTHOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANPR Environment Scan - 1 - Strategic Scan v0.2 Matt</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>ANPR Project Business Requirements V1.0</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>ANPR Project Charter</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>ANPR SC #4 Architecture Options V02</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>ANPR Scoping Study Stakeholder Engagement Strategy</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>Programme Mandate Automated Number Plate Recognition Programme</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>ANPR Benefits Map</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>Review and Sign off process - business requirements</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>ANPR Project Business Requirements V1.0 - Appendix 3 Priority Matrix V1.0</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>ANPR Project Business Requirements V1.0 - Appendix 4 Risk Register V1.0</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>RFT - Request for Proposal Cost &amp; Benefit Analysis</td>
<td>CrimTrac</td>
</tr>
<tr>
<td>Business requirements - review sheet</td>
<td>CrimTrac and stakeholders</td>
</tr>
<tr>
<td>License Plate Recognition - A Tutorial</td>
<td>Hi-Tech Solutions, Yoram Hofman</td>
</tr>
<tr>
<td>British Columbia Ministry of Environment, Lands &amp; Parks: Government and police launch new crime-fighting tool</td>
<td>Media</td>
</tr>
<tr>
<td>Denver's E-470 Toll Road to Enhance Revenue Collection With Latest in Toll Violation Processing Technology</td>
<td>Media</td>
</tr>
<tr>
<td>Faster action on stolen trucks</td>
<td>Media</td>
</tr>
</tbody>
</table>
### 7.2 Meetings and Consultations

CrimTrac contacted a range of community, civil society and privacy organisations to participate in the PIA consultation process. The following organisations accepted invitations and participated in the PIA consultation process.

<table>
<thead>
<tr>
<th>SECTOR</th>
<th>ORGANISATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and community organisations</td>
<td>Australian Privacy Foundation</td>
</tr>
<tr>
<td></td>
<td>Victorian Council for Civil Liberties</td>
</tr>
<tr>
<td></td>
<td>Public Interest Advocacy Centre</td>
</tr>
<tr>
<td>Road Users Organisations</td>
<td>RACV</td>
</tr>
<tr>
<td>Victims of Crime</td>
<td>Victims of Crime Assistance League ACT</td>
</tr>
<tr>
<td>Regulators</td>
<td>Office of the Privacy Commissioner</td>
</tr>
<tr>
<td></td>
<td>Office of the NSW Privacy Commissioner</td>
</tr>
<tr>
<td></td>
<td>Victorian Privacy Commissioner</td>
</tr>
<tr>
<td></td>
<td>Commonwealth Ombudsman</td>
</tr>
<tr>
<td></td>
<td>Victorian Ombudsman</td>
</tr>
<tr>
<td>Other</td>
<td>The Australian Institute of Criminology</td>
</tr>
</tbody>
</table>
## AUSTRALIAN GOVERNMENT USE OF ANPR

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>All Australian toll roads use ANPR to identify vehicles that have not used an eTag or manual payment to pay the toll. The owners of these vehicles are then invoiced either by the toll company or by RTAs on their behalf. All portable ANPR units owned by police are able to be used in general crime investigations as well as for traffic management.</td>
</tr>
<tr>
<td>NSW 210 cameras</td>
<td>There is extensive use of ANPR by the Roads and Traffic Authority (RTA) for heavy vehicle monitoring (Safe-T-Cam), bus and transit lane management and for specialised uses such as vehicle noise and pollution monitoring. Infringements are issued through the post by a back office facility. Police have a number of portable roadside units which are generally used in conjunction with intercept teams. Infringements are issued on the spot.</td>
</tr>
<tr>
<td>ACT 3 cameras</td>
<td>ACT Policing have portable roadside units which are used in conjunction with intercept teams. These teams often include ACT RTA staff that check vehicle safety. These units are available to the AFP generally.</td>
</tr>
<tr>
<td>Victoria 6 cameras</td>
<td>Victoria police have several portable roadside ANPR units used in conjunction with intercept teams. Victoria's Department of Justice has a network of heavy vehicle monitoring stations that use ANPR and VicRoads uses ANPR to measure travel times on busy roads and advise motorists and set variable speed limits. A point-to-point speed monitoring network has been set up on the Hume Highway to regulate speed over distance for all vehicles. The Victorian Environmental Protection Authority and the Department of Fisheries use ANPR to investigate incidents and help regulate licensees.</td>
</tr>
<tr>
<td>Tasmania 11 cameras</td>
<td>The Tasmanian Department of Infrastructure, Environment and Resources uses ANPR to monitor heavy vehicles and unregistered or uninsured vehicles. Tasmanian Police are not currently using ANPR.</td>
</tr>
<tr>
<td>South Australia 25 cameras</td>
<td>South Australia uses ANPR for policing broadband and in vehicle units, heavy vehicle monitoring (Truckscan) in conjunction with the NSW RTA, traffic flow monitoring and general roads regulation.</td>
</tr>
<tr>
<td>Queensland 28 cameras</td>
<td>Police trials, DMR, BUC, Toll Road, Travel safe</td>
</tr>
<tr>
<td>Western Australia 10 cameras</td>
<td>Western Australia Main Roads and Western Australian Police use portable ANPR throughout the state. A number of fixed sites are used for monitoring busy roads and some key highways.</td>
</tr>
<tr>
<td>Northern Territory 0 cameras</td>
<td>Northern Territory Police and roads authorities do not currently use ANPR.</td>
</tr>
</tbody>
</table>
9 APPENDIX II – USE OF ANPR 5 YEARS OUT

The table below provides a simple comparison of the current situation and a non-national and national ANPR system. IIS developed the table based on the information IIS has considered to date for this PIA, its understanding of the assumptions CrimTrac is using and the general regulatory environment. In particular, IIS has assumed that ANPR use will develop in the states and territories to a significant degree, whether or not governments implement a national ANPR system.

<table>
<thead>
<tr>
<th></th>
<th>CURRENT STATE</th>
<th>5 YEARS OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DIMENSION</strong></td>
<td></td>
<td><strong>NON-NATIONAL SYSTEM</strong></td>
</tr>
<tr>
<td>Amount and nature of information ANPR data captured</td>
<td>Varies, particularly in relation to whether image of driver and passengers included</td>
<td>Likely to continue to vary between states</td>
</tr>
<tr>
<td>No. of cameras</td>
<td>Australia wide 292 fixed and 100 mobile cameras</td>
<td>Assumed to be likely to be approaching the national level</td>
</tr>
<tr>
<td>System functionality</td>
<td>Ability to capture sightings, match sightings to hotlists and generate and action alerts, and where data are held long term, provide data for analysis</td>
<td>Ability to capture sightings, match sightings to hotlists and generate and action alerts, and where data are held long term, provide data for analysis</td>
</tr>
<tr>
<td>System standards, costs and efficiency</td>
<td>Varies according to the state approach</td>
<td>Will continue to vary according to state approach</td>
</tr>
<tr>
<td>DIMENSION</td>
<td>CURRENT STATE</td>
<td>5 YEARS OUT</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NON-NATIONAL SYSTEM</td>
</tr>
<tr>
<td>Data sharing between state RTAs and between RTAs and law enforcement agencies</td>
<td>Data sharing does occur but arrangements vary between states and may be slow and complex at times</td>
<td>Data sharing levels likely to increase, arrangements may continue to be variable</td>
</tr>
<tr>
<td>Data retention</td>
<td>Varies considerably, also at present no jurisdiction in Australia bulk stores ANPR sightings and most do not store them at all</td>
<td>Likely to continue to vary between the states</td>
</tr>
<tr>
<td>Legal framework</td>
<td>Privacy and other law applying to ANPR varies considerably between the states and in its application to ANPR</td>
<td>Likely to continue to vary between the states</td>
</tr>
<tr>
<td>Governance arrangements</td>
<td>State oversight by law, accountability arrangements, including audit and parliamentary scrutiny</td>
<td>State oversight by law, accountability arrangements, including audit and parliamentary scrutiny</td>
</tr>
</tbody>
</table>
### 10 APPENDIX IV - AUSTRALIAN PRIVACY LAWS

<table>
<thead>
<tr>
<th>JURISDICTION</th>
<th>PRIVACY LAW OR OTHER PRIVACY PROTECTION MECHANISM</th>
<th>REGULATOR</th>
<th>APPLICATION TO LAW ENFORCEMENT AND NATIONAL SECURITY ACTIVITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Privacy Act 1988</td>
<td>Office of the Privacy Commissioner</td>
<td>Most federal law enforcement agencies are subject to the Privacy Act, national security agencies are exempt</td>
</tr>
<tr>
<td>New South Wales</td>
<td>Privacy and Personal Information Protection Act 1998</td>
<td>NSW Privacy Commissioner</td>
<td>Significant exemptions for law enforcement agencies for policing activities</td>
</tr>
<tr>
<td>Victoria</td>
<td>Information Privacy Act 2000</td>
<td>Office of the Victorian Privacy Commissioner</td>
<td>Applies to law enforcement agencies, except where the agency believes compliance is inconsistent with its law enforcement functions</td>
</tr>
<tr>
<td>Australian Capital Territory</td>
<td>Privacy Act 1988</td>
<td>Office of the Privacy Commissioner</td>
<td>Applies to law enforcement activities</td>
</tr>
<tr>
<td>Northern Territory</td>
<td>Information Act 2002</td>
<td>The Office of the Information Commissioner</td>
<td>Applies to law enforcement agencies, except where the agency believes compliance is inconsistent with its law enforcement functions</td>
</tr>
<tr>
<td>Queensland</td>
<td>Government adopted privacy principles on an interim non-statutory basis.</td>
<td>None</td>
<td>The arrangements apply to law enforcement agencies with certain exemptions, for example, principles in relation to providing notice and use and disclosure</td>
</tr>
<tr>
<td>Tasmania</td>
<td>Personal Information Protection Act 2004</td>
<td>Tasmanian Ombudsman</td>
<td>The arrangements apply to law enforcement agencies with certain exemptions, for example, principles in relation to providing notice and use and disclosure</td>
</tr>
<tr>
<td>South Australia</td>
<td>Administrative scheme based on privacy principles</td>
<td>None</td>
<td>Some exemptions for specific activities</td>
</tr>
<tr>
<td>Western Australia</td>
<td>No current scheme</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>


APPENDIX C

DETAILED LEGISLATIVE REVIEW

CrimTrac
Responsive · Innovative · Accountable

Released by the CrimTrac Agency under the Freedom of Information Act 1982
This detailed report has been provided by the Australian Government Solicitor.
# CONTENTS

## INTRODUCTION
- Brief description of ANPR technology and its use 352
- Legislative review 353
- Preliminary matters 353

## PRIVACY LAWS
- Privacy Act 1988 [Cth] 355
- NSW Privacy Law - the Privacy and Personal Information Protection Act 1998 (NSW) 377
- Victoria - Information Privacy Act 2000 [Vic] 383
- Queensland privacy - Information Standard No 42 390
- South Australian privacy - Information Privacy Principles Instrucion 391
- Tasmanian privacy law - the Personal Information Protection Act 2004 (Tas) 392
- Western Australia - Information Privacy Bill 2008 (WA) 398
- Northern Territory - Information Act (NT) 403

## STATE AND TERRITORY ROAD TRAFFIC LEGISLATION
- New South Wales 409
- Victoria 416
- Queensland 422
- Northern Territory 430
- Australian Capital Territory 435
- Western Australia 438
- Tasmania 445
- South Australia 450

## OTHER RELEVANT STATE AND TERRITORY LEGISLATION
- Freedom of Information Legislation 459
- Surveillance Devices legislation 460
- Archives legislation 461
INTRODUCTION

1. The following paragraphs set out our detailed report in relation to the collection of relevant ANPR information by the relevant Commonwealth, State and Territory authorities, and the disclosure of that information to CrimTrac.

Brief description of ANPR technology and its use

2. ANPR uses camera and optical character recognition technology to recognise and capture vehicle number plates. Various States and Territories in Australia are already using this technology. However, there is currently no national scheme for its use or future implementation.

3. CrimTrac is currently undertaking a scoping study into the national use of ANPR technology for three purposes in Australia – road safety, criminal investigations and national security initiatives.

4. To meet these purposes, cameras fitted with ANPR technology would collect an overview image of the vehicle, and data generally consisting of the text string of the vehicle number plate, date, time, location of the camera (including GPS coordinates and street name).

5. The data collected would be of all vehicles passing a particular point during a particular period or on a continuous, ongoing basis. The cameras would not be triggered only by a particular vehicle (or class of vehicle) or by a vehicle that was driving at a particular speed or in a particular manner. The cameras would record information about all vehicles regardless of the circumstances relating to the vehicle or its driver, that is, whether or not vehicles were being driven unlawfully or dangerously or by persons of interest to the police. This is an essential element of the scheme.

6. The collected data would then be matched against ‘hotlists’ compiled, for example, in relation to number plates for stolen vehicles or vehicles wanted in relation to certain offences. The program would involve the installation of a large number of ANPR-enabled cameras across Australia.

7. If a national scheme were to be implemented and ANPR technology used for the three purposes outlined above, there are numerous agencies that may require access to the data. These include all Australian police agencies; Commonwealth law enforcement agencies; all Australian road transport agencies; national security agencies (Australian Security Intelligence Organisation) and other law enforcement bodies in Australia (for example, the New South Wales Independent Commission Against Corruption and the Australian Commission for Law Enforcement Integrity). CrimTrac would act as the central broker of ANPR information to these law enforcement and regulatory agencies and would administer the national ANPR system.
Legislative review

8. CrimTrac requested AGS to undertake a legislative review and prepare a report in relation to the implementation of the policy objective outlined above. We have examined a large range of existing Commonwealth, State and Territory legislation which is potentially relevant to the policy objective. This has been a large exercise due to the number of jurisdictions, the large number of agencies that may be involved in the collection and disclosure of ANPR data and the broad purposes for which the data would be collected and used. In our review we have identified a number of statutory provisions dealing with the collection, storage and disclosure of information that would be applicable to ANPR data. The legislation we have reviewed includes road transport legislation, police legislation, general criminal laws, national security legislation, human rights laws, privacy legislation, surveillance legislation and archives legislation.

9. In our detailed report we have identified and listed relevant sections of Commonwealth, State and Territory legislation that would prevent or limit aspects of the ANPR program and have suggested possible legislative amendments and, where possible, non-legislative solutions.

Preliminary matters

10. For the purposes of this report, we have used three key terms that need to be defined and understood.

ANPR PROGRAM

11. We have used the term ‘ANPR program’ to describe all aspects of the policy objective outlined above including, in particular, the actual deployment of ANPR-enabled cameras, the collection of ANPR data by those cameras, the provision of the data to CrimTrac and the subsequent access by relevant agencies to the data. A central aim of the policy objective is to allow and facilitate the exchange of data between relevant agencies and different jurisdictions.

PURPOSES OF THE ANPR PROGRAM

12. We have used the phrase ‘purposes of the ANPR program’ or ‘broad purposes of the ANPR program’ to collectively describe the three purposes for which the ANPR technology would be used: road safety, criminal investigation and national security. It is necessary to say a few things about these three particular purposes.

- First, they overlap to a considerable extent. For example, driving a vehicle in excess of the local speed is a criminal offence and also affects the safety of drivers and pedestrians. Another simple example can be given: planning to explode a bomb in a public place is a terrorist offence and also affects national security.

- Secondly, the three purposes are also distinct. For example, driving a vehicle under the local speed limit is not an offence but it may affect road safety if the vehicle is driven near a school. Another simple example can be given: a person suspected of having links with known or suspected terrorists would not necessarily be committing an offence but information about his whereabouts may be of importance for national security.

- Thirdly, each of the three purposes is clearly broad. In particular, in this summary and our detailed report we assume that the term ‘criminal investigation’ in the above description of the purposes for which ANPR technology would be used is intended also...
to include measures for the prevention and detection of crime. Criminal investigation is a major aspect of law enforcement more generally. Furthermore, we understand that the term 'road safety' in the description of the purposes for which ANPR technology would be used is intended to also cover related regulatory purposes such as road use planning and road usage.

13. Accordingly, where in this summary or in the detailed report we conclude, for example, that ANPR data is unable to be collected for the purposes of the ANPR program, we mean that the data is unable to be collected for each of the three purposes (i.e., criminal investigation, road safety and national security). Only if the data could be collected for each of the three purposes would we conclude that the ANPR data is able to be collected for the purpose of the ANPR program.

RELEVANT ANPR INFORMATION

14. We have used the term 'relevant ANPR information' to describe the following image and data obtained by the use of cameras fitted with ANPR technology:

- an overview image of the vehicle;
- the text string of the vehicle number plate;
- date, time and location of the camera (including GPS coordinates and street name).
Privacy Act 1988 (Cth)

15. The Privacy Act 1988 (Cth) [the Commonwealth Privacy Act] regulates the collection, storage, use and disclosure of personal information by Commonwealth agencies, ACT agencies and certain private sector organisations.

SCOPE AND GENERAL OPERATION OF THE PRIVACY ACT

16. The Privacy Act states that 'an agency shall not do an act or engage in a practice that breaches an Information Privacy Principle' [IPP] (s 16). The IPPs are contained in s 14 of the Commonwealth Privacy Act, and deal with the collection, storage, use and disclosure of personal information. It is an interference with the privacy of an individual if an act or practice of an agency breaches an IPP in relation to personal information that relates to the individual (s 13(c)).

17. The term 'agency' is defined to include a wide range of Commonwealth departments, agencies and bodies. CrimTrac is an Executive Agency established under s 65 of the Public Service Act. It is clearly an 'agency' for the purposes of the Commonwealth Privacy Act [see para (b) of the definition of the term 'agency' and the definition of the term 'Department' in s 6 of the Commonwealth Privacy Act, read with the definition of the term 'Agency' in the Public Service Act].

18. The term 'agency' is defined also to include 'an ACT agency' [ie, ACT government departments and agencies] (see s 23 of the Australian Capital Territory Government Service (Consequential Provisions) Act 1994, read with Schedule 3 to that Act).

19. The term 'agency' also includes the Australian Federal Police [AFP] [see para (h) of the definition of the term 'agency' in s 6 of the Commonwealth Privacy Act].

20. Accordingly, CrimTrac, the AFP and ACT agencies are each covered by the Commonwealth Privacy Act. The Australian Customs Service and the Australian Crime Commission are also 'agencies' for the purpose of the Commonwealth Privacy Act.

21. An individual may complain to the Federal Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual (s 36). The Federal Privacy Commissioner is empowered to conduct investigations and inquiries in relation to complaints (see, eg, s 40). Following an investigation, the Federal Privacy Commissioner is empowered to make a range of determinations including, for example, a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (s 52(1)(b)(iii)).
DEFINITION OF 'PERSONAL INFORMATION' – IS RELEVANT ANPR INFORMATION 'PERSONAL INFORMATION'?

22. The definition of the term 'personal information' is critical to the scope and operation of the Commonwealth Privacy Act. The term is relevantly defined in s 6(1) of the Commonwealth Privacy Act as follows:

**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.

23. In our view, in most cases an individual’s identity would not be apparent, or could not reasonably be ascertained, from an overview image of a vehicle or the text of a vehicle number plate. We assume, for the purposes of this report, that the ANPR technology would not enable a clear photograph of the driver or passengers in the vehicle to be made, or produce such a photograph.

24. However, if the image or text were of a unique vehicle or special number plate (such as a rare or custom-designed vehicle or a personalised number plate), the identity of the owner or driver of the vehicle may be apparent, or could reasonably be ascertained, from the image or text. This is a major issue because there are many unique or distinctive vehicles used on Australian roads and personalised vehicle number plates are becoming increasingly common. The question to be asked, in our view, is whether a moderately informed member of the Australian community (or of a significant section thereof) could, by looking at the image or text, correctly physically identify the individual who owned or was likely to be driving the vehicle. The moderately informed member of the public would have access to other readily available information to assist in the identification (cf Freedom of Information Memorandum 98, issued by the Attorney-General’s Department (FOI Memo 98)). What will amount to readily available information will depend on the circumstances of the case.

25. We understand that information enabling people generally to identify the owners or drivers of vehicles by reference to the number plate of the vehicle is not readily available. Indeed, we understand that such information is protected from general disclosure under State and Territory law and is thus not available to members of the public.

26. However, for the purposes of the definition of the term 'personal information', identification of an individual is not enough on its own. The definition of 'personal information' states that the information must be 'about an individual'. This means that, in order to be 'personal information', the image of the vehicle or the text of the number plate must be linked to other information about the individual that says something about the individual (see FOI Memo 98 and Kristie Foldvær Department of Employment, Workplace Relations and Small Business (2002) FCA 55). An image of a rare or unusual vehicle or the text of a personalised or well-known number plate that was linked to a particular date, time and physical location would be likely, in our view, to constitute 'personal information' for the purposes of the Commonwealth Privacy Act.

27. We assume that the overview image of the vehicle would contain an image only of the vehicle itself, the image would not also contain informative contextual elements such as street or suburb signs, or prominent buildings or landmarks. Therefore, the image would not of itself say anything more than that, at some unknown place, date and time, the owner or someone else (with or without the owner’s permission) was driving the vehicle. In practice it is difficult to imagine that a complaint would be made or upheld under the Commonwealth Privacy Act in relation to the collection, use or disclosure of a mere image of an identified person’s vehicle in use.
28. On the other hand, an image of a common type or model of vehicle or the text of a standard number plate that was linked to a particular date, time and location would not be likely, in our view, to constitute 'personal information' for the purposes of the Commonwealth Privacy Act.

29. Clearly, where the image or text is linked with information such as the name or address of the owner or driver of the vehicle, this will constitute 'personal information'. We mention this only because it is possible that other data held by CrimTrac, the AFP and relevant ACT agencies for the purposes of the ANPR program more generally may include details of identity of this kind.

30. It follows that the large majority of data collected by the ANPR-enabled cameras will not itself constitute 'personal information' for the purposes of the Commonwealth Privacy Act, and will therefore not need to be dealt with in accordance with the IPPs. However, a small but significant amount of data collected by the cameras would, when combined with date, time and location information, constitute 'personal information' and would therefore need to be dealt with in accordance with the IPPs and the Commonwealth Privacy Act. For this reason, assuming it is not technically possible in collecting or storing the data to distinguish between images of common and rare or unusual vehicles, or between standard and personalised number plates, it would be advisable to take a cautious approach to the operation of the Commonwealth Privacy Act and treat all data collected by the ANPR-enabled cameras as 'personal information' and deal with it in accordance with the IPPs.

31. We emphasise that, if the information collected or disclosed for the purposes of the ANPR program does not identify an individual, or enable an individual's identity to be reasonably ascertained, or if the information is not about an identified individual, it will not be personal information for the purposes of the IPPs. For example, the IPPs would not apply to the collection or disclosure by CrimTrac of information that, during a particular period, a particular number of vehicles were driven on a particular section of a public road. Information of this 'de-personalised' type could be relevant especially for national or State/Territory road use or road planning purposes.

Possible changes to the definition of 'personal information'

32. We note that the Australian Law Reform Commission (the ALRC) has recently examined the definition of 'personal information' in the Commonwealth Privacy Act and proposed that it be changed (see ALRC Discussion Paper 72 Review of Australian Privacy Law, paras 3.94 - 3.142). In particular, the ALRC has proposed that the Commonwealth Privacy Act should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual' (emphasis added). The ALRC stated:

3.131 The ALRC's view is that this element of the definition should be amended to bring it more into line with other jurisdictions and international instruments. The ALRC proposes that 'personal information' should be defined as information about an identified or reasonably identifiable individual. The ALRC notes the distinction drawn by the former Privacy Commissioner between 'identity' and 'identification' and is of the view that the Privacy Act should apply to information about an individual who is 'identified or reasonably identifiable' rather than information about an individual whose identity is apparent or can reasonably be ascertained.

3.132 The ALRC notes the difficulties that stakeholders have with the existing definition and is of the view that using terminology that is more consistent with that used in relevant international instruments may assist. International jurisprudence and explanatory material based on the terms 'identified' and 'identifiable' will be more directly relevant. The APEC Privacy Framework, the OECD Guidelines, the Council of Europe Convention and the EU Directive use the terms 'identified' and 'identifiable'.

3.133 In the ALRC’s view, the definition should include an element of reasonableness. Whether an individual can be identified or is identifiable depends on context and circumstances. While it may be technically possible for an agency or organisation to identify individuals from information it holds by, for example, linking the information with information held by another agency or organization, it may be that it is not practically possible because, for example, of logistics or legislation. In these circumstances, the ALRC is of the view that individuals are not ‘reasonably identifiable’.

3.134 If, however, the agency or organisation does have access to other information and is able to link that information with information it holds in such a way that individuals can be identified, the ALRC is of the view that those individuals are ‘reasonably identifiable’ and that the information is ‘personal information’ for the purposes of the Privacy Act. For this reason, the definition of ‘personal information’ should not be limited, as it currently is, to information about an individual who can be identified ‘from the information’. The ALRC proposes that the Explanatory Memorandum to the amended Act make clear that an individual is ‘reasonably identifiable’ when the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access.

33. We understand the ALRC has submitted its final report to the Government, although the report has not yet been publicly released. It is possible that the ALRC may recommend that the definition of ‘personal information’ be changed as outlined above, and it is possible that the Government may agree to this recommendation. If this were to occur, as we understand the situation we think most (but not all) of the data collected by the ANPR-enabled cameras would not be ‘personal information’ for the purposes of the new definition. However, for the reasons discussed above, we think that some data would be likely to be ‘personal information’ and would therefore need to be dealt with in accordance with the IPPs.

34. It is, however, possible that the ALRC may make a different recommendation about the definition of the term ‘personal information’ or that the Government may not accept any recommendation in this regard.

IPP 1 – MANNER AND PURPOSE OF COLLECTION OF PERSONAL INFORMATION – APPLICATION TO CRIMTRAC

35. The application of the Commonwealth Privacy Act to CrimTrac will not be confined to personal information generated only from Commonwealth sources. It will therefore not matter that the ANPR-enabled cameras are not owned or controlled by CrimTrac. As mentioned above, States and Territories are already using ANPR-enabled cameras for their own purposes. Most ANPR-enabled cameras will be owned or operated by State or Territory agencies, or Commonwealth agencies other than CrimTrac.

36. As discussed above, a significant amount of relevant ANPR information which CrimTrac would receive and hold will be ‘personal information’ within the meaning of the Commonwealth Privacy Act. CrimTrac would be the ‘record-keeper’ or ‘collect’ of the information for the purposes of the Commonwealth Privacy Act and the IPPs.

37. IPP 1 provides as follows:

Manner and purpose of collection of personal information

1 Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector, and
(b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

38. In our view, it is not clear that the collection by CrimTrac of relevant ANPR information would fully be in accordance with IPP 1. It may be necessary to expand CrimTrac’s functions to cover clearly the road safety and national security purposes of the ANPR program.

39. IPP 1 has four significant requirements in the present context:
   – the relevant ANPR information must be collected for a ‘lawful purpose’;
   – that purpose must be ‘directly related’ to a function or activity of CrimTrac;
   – the collection of the ANPR information by CrimTrac must be ‘necessary’ for, or ‘directly related’ to, that purpose;
   – the means of collection must not be unlawful or unfair.

"Lawful purpose"

40. The ‘lawful purpose’ element of IPP 1 is generally taken to require simply that the purpose of the collection is not prohibited by law. The question is the lawfulness of the purpose, as distinct from the lawfulness of the actual collection. It is therefore necessary to determine the ‘purpose’ of the collection.

41. The three stated purposes of the collection – road safety, criminal investigations and national security initiatives – are lawful purposes in the sense that they are not prohibited by law. Yet only one of the purposes [criminal investigations] is clearly consistent with the functions of CrimTrac, as specified in the Governor-General’s order under s 65 of the Public Service Act, read with the Intergovernmental Agreement between all States and Territories and the Commonwealth for the establishment and operation of CrimTrac that took effect on 1 July 2008 [the IGA]. It is not clear that road safety and, to some extent, national security would be lawful purposes of CrimTrac.

42. The order establishing CrimTrac specifies that the functions of CrimTrac are as follows:
   a) to implement the CrimTrac initiative comprising a new National Automated Fingerprint Identification System, a National DNA Criminal Investigation System, a National Child Sex Offender System, the provision of rapid access to national operational policing data and other emerging policing requirements across jurisdictions;
   b) to perform the administrative functions required to fulfill the objectives and obligations in the CrimTrac Inter-Governmental Agreement including assistance to the CrimTrac Board of Management.

43. There is no mention of the ANPR program in the order. Para (a) above refers to CrimTrac providing ‘rapid access to national operational policing data and other emerging policing requirements across jurisdictions’ [our emphasis]. To the extent that relevant ANPR information is collected for law enforcement purposes [which would include criminal investigations], we think the order would support this aspect of the ANPR program. CrimTrac’s function of performing the administrative functions required to fulfill the objectives and obligations in the IGA would also be relevant in relation to the law enforcement purposes of the ANPR program. Clause 3.1 of the IGA is relevant in this regard and provides as follows:
3.1 Broad objectives

The broad objectives of CrimTrac are to enhance Australian policing through:

(a) the provision of high quality information services that
   (i) meet the needs of the Australian policing community; and
   (ii) establish best practice service models in relation to the provision of information to support policing; and
   (iii) are project-oriented and cost-benefit driven to achieve outcomes;
(b) support for the jurisdictions in the implementation and use of CrimTrac services; and
(c) providing controlled access to appropriate information by duly accredited third parties.

'Directly related to a function or activity'

44. Even if the collection by CrimTrac of relevant ANPR information were viewed as collection for a 'lawful purpose' (in the sense that the purpose was not expressly prohibited or did not contravene the criminal law), it is not clear that the collection of the information for the purpose or road safety or some aspects of national security would be 'directly related' to a function or activity of CrimTrac. As discussed above, the establishment and maintenance of a database containing relevant ANPR information for the purposes of road safety (and possibly those aspects, if any, of national security that do not relate to policing or law enforcement generally) is not clearly a proper function or activity of CrimTrac.

'Necessary for or directly related to that purpose'

45. As there is a question whether the collection of the information for road safety and some national security purposes would be a 'lawful purpose' of CrimTrac, there is some uncertainty whether the collection of the information could be said to satisfy the requirement in PPT 1.18, namely, that the collection is necessary for or directly related to that purpose' (our emphasis). In this context, the reference to 'that purpose' is a reference to a 'lawful purpose'.

Way ahead

46. The legal position would be clarified if the functions of CrimTrac were extended to cover the road safety and national security purposes of the ANPR program. We think further consideration should be given as to whether clarification of CrimTrac's functions is legally necessary. It may be possible to argue that the collection and disclosure of information for road safety purposes or some national security purposes would be merely an aspect of CrimTrac's broad function in cl 3.1(c) of the IGA of providing controlled access to appropriate information by duly accredited third parties. Alternatively, it is possible that, with minor modification, the ANPR program would be fully supported under CrimTrac's existing functions.

47. If it is necessary or desirable to vary CrimTrac's functions, no legislation would be necessary. However, in this event an amendment to the order made under s 65 of the Public Service Act and to the IGA would be required. In this regard we note that cl 11 of the IGA provides for variations to the IGA and requires the unanimous agreement of the parties.

48. If these changes were made, we think the collection of relevant ANPR information by CrimTrac would clearly be for lawful purposes and would directly assist in achieving the
purposes identified above [see IPP 1.1(b)]. Although it might be suggested that there is an
insufficiently direct relationship between collecting the information and actually preventing,
and detecting crime, improving road safety and protecting national security etc, we think
the broad purposes of CrimTrac collecting the relevant ANPR information would mean this
requirement could be satisfied in the present case.

No collection by 'unlawful or unfair means'  
49. IPP 1 also requires that the information not be collected by unlawful or unfair means.
On our understanding of the ANPR program and our initial consideration of relevant
Commonwealth, State and Territory legislation (e.g. laws regulating the use of optical
surveillance devices), we do not consider the collection of relevant ANPR information by
CrimTrac would occur by 'unlawful means'.

Covert surveillance guidelines

50. There is, however, a question whether the proposed activities would involve the collection
of personal information by 'unfair means'. This aspect is covered in the Covert Surveillance
in Commonwealth administration: Guidelines [the Covert Surveillance Guidelines], which
are available on the Federal Privacy Commissioner’s website. The Covert Surveillance
Guidelines define 'covert surveillance' as follows:

The secretive, continuous or periodic observations of persons, vehicles, places or
objects to obtain information concerning the activities of individuals which is then
recorded in material form including notes and photographs.

51. The Covert Surveillance Guidelines state that covert surveillance is generally intrusive in
that information about an individual is collected without the individual's consent and the
individual is usually unaware that he or she is under surveillance. The Covert Surveillance
Guidelines state that 'national security organisations and agencies using covert
surveillance for law enforcement purposes' are not affected by the Covert Surveillance
Guidelines [p 9]. Although CrimTrac could claim that the collection of relevant ANPR
information is for law enforcement purposes, it is not a national security organisation and
relevent information would be collected also for non-law enforcement purposes such
as road safety. In any case, the Guidelines are not legally binding on agencies and state
that they contain general advice and guidance. Compliance with the Covert Surveillance
Guidelines would not appear to be onerous or to impede the implementation of the ANPR
program. We think the Covert Surveillance Guidelines would generally be applicable in
relation to the ANPR program. We think it would be useful to discuss the application and
effect of the Covert Surveillance Guidelines with the Federal Privacy Commissioner.

IPP 1 - MANNER AND PURPOSE OF COLLECTION OF PERSONAL INFORMATION -
APPLICATION TO THE AFP

52. As discussed above, a significant amount of relevant ANPR information would be likely
to be 'personal information' within meaning of the Commonwealth Privacy Act. If the
AFP collects the information using its own or other agencies' ANPR-enabled cameras,
it would be the 'record-keeper' or 'collector' of the information for the purposes of
the Commonwealth Privacy Act and the IPPs. It is necessary to consider whether
this information, if collected by the AFP, would be collected in accordance with the
requirements of IPP 1.

53. We have examined the Australian Federal Police Act 1979 (the AFP Act). Having regard to
the broad functions of the AFP under s 8 of the AFP Act, it seems likely that the collection
of relevant ANPR information by the AFP would be consistent with the requirements in IPP
Section B of the AFP Act relevantly provides as follows:

8 Functions

(1) The functions of the Australian Federal Police are:

[a] subject to subsection [1A], the provision of police services in relation to
the Australian Capital Territory;

[b] the provision of police services in relation to:

[i] the laws of the Commonwealth;

[ii] the property of the Commonwealth (including Commonwealth
places) and property of authorities of the Commonwealth; and

[iii] the safeguarding of Commonwealth interests;

[b] the provision of police services and police support services for the
purposes of assisting, or cooperating with, an Australian or foreign:

[i] law enforcement agency;

[ii] intelligence or security agency; or

[iii] government regulatory authority; and

(c) to do anything incidental or conducive to the performance of the foregoing
functions.

[1A] The Minister and the Australian Capital Territory may enter into arrangements
for the provision of the police services in relation to the Australian Capital
Territory that are in respect of Territory functions as defined by section 3 of
the ACT Self-Government [Consequential Provisions] Act 1988, and, where the
arrangements have been entered into, the provision of those services shall be
in accordance with the arrangements.

[2B] Arrangements for the provision of services under subsection [1A] ... may
include arrangements for the doing of anything incidental or conducive to the
 provision of the services.

54. The AFP’s functions referred to above must be read with the following broad definitions in s
4 of the AFP Act:

intelligence or security agency means an authority or person responsible for
intelligence gathering for, or the security of, a country or part of a country.

law enforcement agency means an authority or person responsible for
enforcement of laws.

police services includes services by way of the prevention of crime and the
protection of persons from injury or death, and property from damage, whether
arising from criminal acts or otherwise.
**Police Support Services** means services related to:

(a) the provision of police services by an Australian or foreign law enforcement agency; or

(b) the provision of services by an Australian or foreign intelligence or security agency; or

(c) the provision of services by an Australian or foreign regulatory agency.

55. We do not think that the collection of relevant ANPR information by the AFP would contravene IPP 1.2. There is no reason for thinking that the means of collection that would be used by the AFP would be ‘unlawful’. There may be a question whether the collection would be by ‘unfair’ means. However, collection by this means would be likely to be subject to internal AFP instructions that contain safeguards. Even though they are not legally binding, the Covert Surveillance Guidelines do not appear to be directed at covert surveillance conducted by the AFP (see pp 2-3 of the Guidelines).

56. In summary, IPP 1 would not appear to present any difficulties in relation to the collection of relevant ANPR information by the AFP.

**IPP 1 – MANNER AND PURPOSE OF COLLECTION OF PERSONAL INFORMATION – APPLICATION TO ACT AGENCIES**

57. We assume, for the purposes of this report, that the collection by ACT agencies of relevant ANPR information (through the use of their own or others’ ANPR-enabled cameras) would be in accordance with IPP 1.1. In order to provide definitive advice on this issue it would be necessary to identify the relevant ACT agencies and examine and consider their specific functions (including any relevant ACT legislation). This aspect is considered further below.

58. On our understanding of the ANPR program and our initial consideration of relevant legislation applying in the ACT, it appears that the collection of the relevant ANPR information by ACT agencies would not occur by ‘unlawful means’. There may, however, be a question whether the proposed activities would involve the collection of personal information by ‘unfair’ means. Although the Covert Surveillance Guidelines are expressed to apply only to Commonwealth agencies (ie, not ACT agencies), it is possible that the Federal Privacy Commissioner would, as a matter of policy, seek to apply the guidance in the Covert Surveillance Guidelines to ACT agencies involved in covert surveillance.

59. In summary, IPP 1 would not be likely to present any legal difficulties in relation to the collection of relevant ANPR information by ACT agencies provided collection of the information for the purposes of the ANPR program was a function or activity of the agency concerned.

**IPP 3 – SOLICITATION OF PERSONAL INFORMATION GENERALLY – APPLICATION TO CRIMTRAC**

60. IPP 3 is also relevant to CrimTrac’s collection of relevant ANPR information. IPP 2 has no application to CrimTrac in the present circumstances as CrimTrac would not solicit the information from the person to whom it relates. However, by contrast, the application of IPP 3 is not dependent upon a direct connection between the collector and the person to whom the personal information relates (see paragraph [b]).
61. IPP 3 provides as follows:

Solicitation of personal information generally

Where:

   (a) a collector collects personal information for inclusion in a record or in a
        generally available publication; and

   (b) the information is solicited by the collector;

        the collector shall take such steps (if any) as are, in the circumstances,
        reasonable to ensure that, having regard to the purpose for which the
        information is collected:

   (c) the information collected is relevant to that purpose and is up to date and
        complete; and

   (d) the collection of the information does not intrude to an unreasonable extent
        upon the personal affairs of the individual concerned.

62. CrimTrac probably would be held to 'solicit' the relevant ANPR information from
the relevant Commonwealth, State or Territory agencies (or any relevant private sector
organisations). The ordinary meaning of the verb 'solicit' includes 'to make petition or
request, as for something desired' (Macquarie Dictionary, 2nd Revised Edition) and '... a
request or invite [business etc]'. (Australian Pocket Oxford Dictionary, 2nd Edition). While
it may be said that the State and Territory agencies would provide relevant ANPR
information to CrimTrac pursuant to governmental directions within their own jurisdictions,
or simply pursuant to the IGA so that CrimTrac does not actually 'request' the information, it
probably 'invites' it.

63. On that basis, IPP 3 requires CrimTrac to take steps to ensure that the information:

   — is relevant to the purpose of facilitating the exchange of information for national
     law enforcement (including crime prevention and detection), national security and
     national road safety; and

   — is up to date and complete.

64. In relation to the requirement of relevance, there may be questions about the bulk
collection of relevant ANPR information, although the fact that IPP 3 does not stipulate a
relationship of 'direct relevance' is probably sufficient to counter this possible objection.
We are not aware of any relevant judicial discussions about the application of IPP 3 to
agencies such as CrimTrac, performing functions such as those of CrimTrac.

65. However, the Federal Privacy Commissioner has published the Plain English Guidelines
to Information Privacy Principles (the Commonwealth Privacy Guidelines) which provide
some guidance on how the Commissioner approaches the IPPs. In relation to this aspect
of IPP 3, the Commonwealth Privacy Guidelines suggest that an agency should only
solicit information which 'will help it to achieve its purpose of collection', and that 'usually,
information is only relevant if the agency has a use for it at the time the agency collects it
and therefore an agency should not collect information just because it might be useful
in the future'. (vol 1 at 24). However, the Commonwealth Privacy Guidelines (vol 1 at 28)
also acknowledge that there is greater leeway in relation to the application of IPP 3 to law
enforcement agencies:

   Law enforcement agencies such as the Australian Federal Police have their own
guidelines on collecting, recording and using personal information. Their role is
important to the public interest and they have special needs to gather intelligence
information, so they have more freedom than other agencies when collecting information.

A law enforcement agency doesn’t always have to know exactly what it will use personal information for when it collects it. It can collect personal information that is generally related to intelligence purposes, not just a specific purpose. However, it must have good grounds for believing that this kind of information will help it.

66. While it is apparent that the Commonwealth Privacy Guidelines are specifically concerned with agencies which are directly engaged in law enforcement, such as the AFP, we consider that it would be reasonable to adopt a similar approach in respect of the collection by CrimTrac of relevant ANPR information for criminal investigations and for national security initiatives. The application of IPP 3(c) to collection by CrimTrac for road safety purposes is less clear. But we do not think this would be likely to present legal issues.

67. The requirement that efforts be made to ensure that the information is up to date and complete is unlikely to cause difficulties for CrimTrac, as the relevant ANPR information would essentially involve a ‘snapshot’ of personal information that is, by its nature, complete. It would be up to date in the sense that it reflects a moment in past time.

68. For similar reasons, the requirement in IPP 8 is unlikely to cause any difficulties for CrimTrac. IPP 8 provides as follows.

**Record-keeper to check accuracy etc. of personal information before use**

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

69. For the purposes of IPP 8, and other IPPs which apply to ‘record-keepers’, CrimTrac will be the relevant ‘record-keeper’ in relation to the personal information in the ANPR database (see s 10 of the Commonwealth Privacy Act).

70. We mention that we do not think that the requirement in IPP 3(d) would be relevant in the present circumstances, that is, we do not think it would be necessary for CrimTrac to take any steps ‘to ensure that ... the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned’.

**IPP 3 - SOLICITATION OF PERSONAL INFORMATION GENERALLY – APPLICATION TO THE AFP AND ACT AGENCIES**

71. IPP 3 is not relevant to the collection of relevant ANPR information by the AFP and ACT agencies (through the use by those agencies of ANPR-enabled cameras). In such circumstances, the information would not, in the ordinary meaning of the word, be ‘solicited’ by the agencies (see IPP 3(b)).
72. The storage of personal information collected by agencies is dealt with in IPP 4, which provides:

*Storage and security of personal information*

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

73. Provided that CrimTrac implements such security safeguards as it is reasonable in the circumstances to take and does everything reasonably within its power ... to prevent unauthorised use or disclosure of the relevant ANPR information, it would satisfy IPP 4. The Federal Privacy Commissioner has issued comprehensive guidelines about how to comply with IPP 4, mentioning in particular compliance with the Protective Security Manual and guidelines on computer security issued by the Defence Signals Directorate. These are available on the Federal Privacy Commissioner's website.

74. The guidelines also suggest that, to ensure compliance with paragraph [b] of IPP 4, certain clauses should be included in access arrangements between CrimTrac and State, Territory and federal agencies whose staff are to have access to the ANPR database. Although IPP 4(b) does not expressly apply in relation to the main CrimTrac arrangements with the States and Territories, as access would not strictly be given 'in connection with the provision of a service' to CrimTrac, the Federal Privacy Commissioner takes the view that it is relevant also to cooperative arrangements with other governments' (Commonwealth Privacy Guidelines, vol 2 at 7). This may include the CrimTrac initiative. It would, therefore, be sensible for CrimTrac to have formal arrangements with accessing jurisdictions of the nature suggested by the Federal Privacy Commissioner, and to put in place mechanisms to monitor compliance by those jurisdictions with those arrangements. If such measures are taken, we consider that CrimTrac would not infringe IPP 4.

75. As the ANPR database would be in the possession or under the primary control of CrimTrac, it is not necessary for the purposes of this advice to consider the application of IPP 4 to the AFP or ACT agencies.

IPP 6 – ACCESS TO RECORDS CONTAINING PERSONAL INFORMATION – GENERAL COMMENT

76. IPP 6 should be briefly noted. It provides as follows:

*Access to records containing personal information*

Where a record keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.
77. Under this provision, an individual would be entitled generally to have access to relevant ANPR information concerning that individual. For example, in some circumstances a person could ask CrimTrac to provide the person with information it has about the location of his or her vehicle, either generally or in relation to a particular period. In such a case, CrimTrac would be obliged to provide the individual with access to this information, unless it would be required or authorised to refuse access under, for example, the Freedom of Information Act 1982 (the FOI Act). Such information may disclose information that CrimTrac would prefer not to disclose, such as the location of ANPR-enabled cameras, as this may prejudice law enforcement operations or national security. Under the FOI Act there are several categories of documents that are exempt from access (including on national security and law enforcement grounds: see ss 33 and 37, respectively) (see the discussion below concerning FOI laws).

IPP 9 AND 10 - LIMITS ON USE OF PERSONAL INFORMATION - APPLICATION TO CRIMTRAC

78. Both accessing and processing by CrimTrac of relevant ANPR information will, in Commonwealth Privacy Act terms, constitute a 'use', and hence will be affected by IPPs 9 and 10.

79. IPP 9 provides as follows:

    Personal information to be used only for relevant purposes

    A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

80. There is nothing of which we are aware to suggest that CrimTrac would use relevant ANPR information (that is also personal information) for anything other than a purpose for which the information is relevant - that is, for the purposes of the ANPR program. Care may need to be taken particularly in relation to the use of personal information in the ANPR database for road safety purposes. For example, personal information in the database may clearly be relevant for the purpose of investigating a particular vehicle accident. However, personal information would not appear to be relevant for the purpose of investigating or examining road safety more generally, such as road usage at particular places or times. In such circumstances, it would be sufficient for the purposes of IPP 9 if the information were 'depersonalised'.

81. IPP 10 provides:

    Limits on use of personal information

    1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

       [a] the individual concerned has consented to use of the information for that other purpose;

       [b] the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

       [c] use of the information for that other purpose is required or authorised by or under law;
use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

82. Apart from IPP 10.1(e), the elements of IPP 10 are essentially the same as those of IPP 11 dealing with disclosure. The application of these principles to CrimTrac’s activities is discussed together in relation to IPP 11 in the paragraphs below. However, assuming CrimTrac deals with relevant ANPR information only for the purposes of the ANPR program, it seems unlikely that the issue of CrimTrac using it for a purpose other than that for which it was obtained, or for any purpose other than one ‘directly related’ to that original purpose. Hence, the issue of a possible contravention of IPP 10 is unlikely to arise.

83. It is beyond the scope of this report to discuss the application of IPPs 9 and 10 to the AFP or ACT agencies.

IPP 11 – LIMITS ON DISCLOSURE OF PERSONAL INFORMATION – APPLICATION TO CRIMTRAC

84. IPP 11.1 of the Commonwealth Privacy Act prohibits an agency from disclosing personal information except in any of the circumstances outlined in paragraphs (a) to (e). Thus, any disclosure by CrimTrac of the relevant ANPR information it collects would need to comply with IPP 11.1. If access to the ANPR database is to be conferred in advance, for example, by way of access privileges to the database for staff of other agencies, and is to occur by way of an on-line enquiry system that provides direct access to relevant ANPR information, operational data, we consider that ‘disclosure’ for the purposes of IPP 11 would occur at the time access is made available to State, Territory and Commonwealth agencies – not just at the time an employee or officer of those agencies actually logs on to the database. On the other hand, if access is to occur by way of ‘alerts’ arising from automatic data-matching of relevant ANPR information against ‘hot lists’ of the kind described above, disclosure for the purposes of IPP 11 would occur later at the time of the ‘alert’.

85. IPP 11 provides as follows:

Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

(d) the disclosure is required or authorised by or under law; or
(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

86. We assume that the collection of relevant ANPR information would not occur in circumstances where individuals concerned would reasonably be likely to have been aware that relevant ANPR information is usually passed to a range of Commonwealth, State and Territory agencies with differing responsibilities. [For example, we assume that the ANPR program would not be widely advertised or brought to the attention of motorists generally] IPP 11.1(a).

87. In addition, it is difficult to see how the ‘consent’ exception in para (b) might be generally applicable in relation to the disclosure of relevant ANPR information by CrimTrac. We note that ‘consent’ is defined in the Privacy Act to include ‘implied consent’ but we do not think this takes the matter any further. The ‘threat to life’ exception in para (c) would usually be applicable only in rare situations and would not be relevant in relation to bulk, routine disclosures of relevant ANPR information envisaged under the ANPR program. Therefore, the main potentially applicable exceptions in relation to the relevant ANPR information are those in paras (d) and (e).

IPP 11.1(e) – reasonably necessary for the enforcement of the criminal law

88. It is convenient to discuss the exception in IPP 11.1(e) before discussing the exception in IPP 11.1(d). IPP 11.1(e) provides an exception to the broad prohibition on disclosure of personal information where the disclosure is ‘reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue’. This last purpose, protection of public revenue would not be relevant in the present circumstances. We think there would be a tenable argument that relevant ANPR information could be disclosed by CrimTrac to other jurisdictions on the basis that, in the terms of the Commonwealth Privacy Act, such disclosure is reasonably necessary for law enforcement of the nature specified in IPP 11.1(e), provided the information were accessed only by police or other law enforcement agencies in the States and Territories for the law enforcement purposes. But, in light of the large volume of relevant ANPR information concerning persons not suspected of wrong-doing, there would be a clear contrary argument. In any event, the ANPR program is clearly intended to apply more broadly than this (ie, to road safety).

89. There is no judicial discussion of the meaning of IPP 11.1. However, we note that the Federal Privacy Commissioner has indicated that IPP 11.1(e) may be relied on to support a disclosure of personal information about a particular person if the agency reasonably believes that it will safeguard one of the public purposes listed in the exception in a predictable way (see the Commonwealth Privacy Guidelines, vol 3 at 45 - 47). However, the Federal Privacy Commissioner also acknowledges that:

in safeguarding one of the public purposes listed in ... IPP 11.1(e), it may be reasonably necessary for an agency to use or disclose information about a range of people – even though none of them has yet been directly linked to an unlawful activity ... As a general rule, ‘reasonably necessary’ implies that a use or disclosure need not be essential or critical to servicing the public interest concerned (for example, enforcing the criminal law).
90. The caveat is then added that:

But it must be more than just helpful, or of some assistance or expedient. Within this range, an agency will inevitably need to exercise its own judgment about what is reasonably necessary.

91. As noted above, in the context of the ANPR program and the Commonwealth Privacy Act, ‘disclosure’ probably occurs as early as when access is given. At this particular point, the disclosure can probably be characterised as no more than expedient to, or possibly of some assistance for, law enforcement.

92. The Commonwealth Privacy Guidelines suggest that in assessing the question of ‘reasonable necessity’ for the purposes of IPP 11.1(d), the following broad factors will generally be relevant:

— whether there are other practical and less intrusive measures available;

— whether the potential harm to the public interest in question is sufficiently strong to outweigh the privacy interests of the people the information is about;

— who is to receive the personal information and whether and how the information is likely to be protected once it is disclosed.

93. In the present case, there would not appear to be any less intrusive, practical measure available. Furthermore, it would be reasonable to decide that one public interest towards which the disclosure of relevant ANPR information is directed – that is, efficient and effective criminal investigation and crime prevention – probably outweighs the privacy interests of people the information is about. In relation to the third factor suggested by the Federal Privacy Commissioner, given the statutory confidentiality obligations on Commonwealth, State and Territory policeservices, we assume that information acquired from CrimTrac would be given appropriate protection. Even so, it may be advisable for CrimTrac to enter into, and monitor compliance with, appropriate agreements with the accessing agencies under which those agencies promise to accord the information appropriate protection and to use it only for relevant purposes.

94. On balance, we consider that there would be reasonable arguments to support the view that the disclosure by CrimTrac of the relevant ANPR information to police and other law enforcement agencies would be ‘reasonably necessary’ for the purpose set out in IPP 11.1(e). It can be argued that the placing of relevant ANPR information on a shared CrimTrac database in accordance with properly established reciprocalsearches between jurisdictions or the provision of electronic ‘alerts’ would be likely to contribute to more effective and efficient future criminal investigations and prevention of criminal activity, and hence, generally speaking, is ‘reasonably necessary for the purposes of the enforcement of criminal law’. In addition, the fact that CrimTrac would be disclosing information to agencies actually engaged in law enforcement activities would strengthen the argument that the disclosure was reasonably necessary for law enforcement.

95. In any case in which reliance is placed upon IPP 11.1(e) or IPP 10.1(d), CrimTrac would have to comply with IPP 11.2, in respect of disclosures, and strictly speaking, with IPP 10.2, and make a note in the relevant record of the use or disclosure. This is obviously an onerous requirement, particularly in terms of use. However, we note that the Commonwealth Privacy Guidelines (Vol 3 at 51-52) state, in relation to IPPs 10.2 and 11.2:

IPP 10.2 seems to say that an agency must note all of its uses of personal information made to safeguard any of the three public interests in exception 10.1(d), even if the agency does not need to rely on 10.1(d). But the wording of IPP 10.2 clearly shows that it is to be read in the context of exception 10.1(d). So the Privacy Commissioner interprets the noting requirement as only applying to uses when an agency relies on this exception.
IPP 11.2 says that when an agency discloses personal information under exception 11.1(e), it must note that disclosure on the record containing that information.

The Commissioner recognises that disclosures of personal information pose a greater threat to privacy than using personal information, and that agencies should take greater care in noting disclosures. So, for disclosures made to safeguard any of the three public interests in IPP 11.2, the Commissioner interprets the noting requirement in IPP 11.2 as applying:

- always – if the agency is relying on 11.1(e), and
- to the extent practical – if the agency is not relying on 11.1(e).

**IPP 11 and disclosure of personal information to ASIO**

96. The prohibition on disclosure of personal information under IPP 11 does not apply in relation to disclosures to ASIO. This is the effect of s.7(1A) of the Commonwealth Privacy Act which provides as follows:

(1A) Despite subsections (1) and (2), a reference in this Act (other than section 8) to an act or to a practice does not include a reference to the act or practice so far as it involves the disclosure of personal information to:

(a) the Australian Security Intelligence Organisation; or

(b) the Australian Secret Intelligence Service; or

(c) the Defence Signals Directorate of the Department of Defence.

97. Accordingly, IPP 11 would not prevent or impede the disclosure by CrimTrac of relevant ANPR information to ASIO.

**IPP 11.1(d) – required or authorised under law**

98. IPP 11.1(d) excepts disclosure of personal information where that disclosure is 'required or authorised by or under law'. In light of our conclusions above in relation to the disclosure by CrimTrac of relevant ANPR information to law enforcement agencies and ASIO, it is necessary to consider the application of the exception in IPP 11.1(d) in relation to disclosures of the information to agencies for road safety purposes (and, possibly, for some national security purposes). Disclosure for road safety purposes clearly would not be accommodated by the exception in IPP 11.1(e). Also, as discussed above, the application of IPP 11.1(e) in relation to the law enforcement purposes of the ANPR program is not clear beyond argument. Reliance on IPP 11.1(d) would, in our view, provide the legally safest and clearest means of complying with IPP 11, in the longer term.

99. We are not aware of any existing legislation specifically authorising the disclosure of relevant ANPR information. Nor, at this stage of the proposal, is any such legislation proposed (eg, to provide for the ANPR program generally). It is therefore necessary to consider whether any existing general legislation could be relied upon to authorise the disclosure of the information. We think that, if it can be shown that a particular disclosure of particular personal information is reasonably required for the proper performance of an agency's statutory functions, the disclosure can be seen as impliedly required or authorised under law and hence within the exemption in IPP 11.1(d). The Federal Privacy Commissioner has taken a similar view. The Commonwealth Privacy Guidelines (Vol 3 at 43) relevantly state:
A use or disclosure may fall within 10.1(c) or 11.1(d) if the law requires or authorises a function or activity that clearly and directly entails the use or disclosure. Here the use or disclosure is impliedly authorised by law because it is essential to effect a scheme the law lays down.

Section 65 of the Public Service Act

100. If, as discussed above, the provisions of the IGA and the CrimTrac functions specified in the Governor-General's order were clarified to support the road safety purposes of the ANPR program, the disclosure of relevant ANPR information would be essential to the achievement of CrimTrac's functions. If CrimTrac's functions (as clarified) were firmly based in primary legislation, arguably this would suffice for the purposes of IPP 11.1(d), as disclosure of relevant ANPR information in this matter would obviously be essential to the performance of CrimTrac statutory functions.

101. However, CrimTrac's functions are established only by instrument under the Public Service Act and the IGA, rather than through primary legislation or regulations. It cannot be said that the proposed disclosure would be essential for the achievement of the objectives of the parent statute (ie, the Public Service Act). We acknowledge that IPPs 10.1(c) and 11.1(d) refer not only to disclosures and uses authorised 'by law', but also to a use or disclosure authorised 'under' law, a phrase which is usually taken to embrace action taken in the exercise of powers such as that of the Governor-General under s 65 of the Public Service Act to establish executive agencies and to specify their functions. However, although there are arguments to support the view that disclosure by CrimTrac would be permitted by IPP 11.1(d), in our view it would be unsafe to rely upon IPP 11.1(d) to support the disclosure by CrimTrac of relevant ANPR information to relevant road safety agencies.

Reg 2.1 of the Public Service Regulations 1999 (Cth)

102. We have also considered whether reg 2.1 of the Public Service Regulations 1999 (the Public Service Regulations) might authorise the disclosure of relevant ANPR information. In our view, they do not.

103. Regulation 2.1 relevantly provides as follows:

Duty not to disclose information

[1] This regulation is made for subsection 13(13) of the Act,

[2] This regulation does not affect other restrictions on the disclosure of information.

[3] An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.

[4] An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if the information:

(a) was, or is to be, communicated in confidence within the government, or

(b) was received in confidence by the government from a person or persons outside the government;

whether or not the disclosure would found an action for breach of confidence.
5. Subregulations (3) and (4) do not prevent a disclosure of information by an APS employee if:

(a) the information is disclosed in the course of the APS employee's duties; or
(b) the information is disclosed in accordance with an authorisation given by an Agency Head; or
(c) the disclosure is otherwise authorised by law; or
(d) the information that is disclosed:
   (i) is already in the public domain as a result of a disclosure of information that is lawful under these Regulations or another law; and
   (ii) can be disclosed without disclosing, expressly or by implication, other information to which sub regulation (3) or (4) applies.

104. Arguably, disclosure of personal information pursuant to the general permissions in reg 2.1(3)(a) or (b) would be 'authorised by or under law' for the purposes of the exception in IPP 11.1(d). However, regs 2.1(b)(a) and (b) apply in relation only to the prohibitions in regs 2.1(3) and (4). We do not think relevant ANPR information would fall within the category of information protected by reg 2.1(3). Nor is it clear, on the basis of our understanding of the ANPR program, that relevant ANPR information would be communicated or received 'in confidence' and thus fall within the category of information protected by reg 2.1(4). Even if the prerequisite of confidence in reg 2.1(4) were satisfied, in the absence of something more in the relevant statutory provisions discussed above, it is not clear that the general permissions in reg 2.1(b)(a) and (b) would qualify as an authorisation under law for the purposes of IPP 11.1(d).

105. In summary, there is some doubt that the exception in IPP 11.1(d) would be applicable in relation to disclosures by CrimTrac of relevant ANPR information to relevant agencies for road safety purposes (and possibly for the other purposes of the ANPR program). Accordingly, the effect of IPP 11.1 is that it may prohibit the disclosure of the information to relevant road safety agencies.

Public interest determination

106. A possible option would be to obtain a 'public interest' determination under Part VI of the Commonwealth Privacy Act (see especially ss 72 and 80A). The process for obtaining such a determination is broadly as follows:

a) an agency makes an application to the Federal Privacy Commissioner;
b) the Commissioner publishes notice of receipt of the application;
c) the Commissioner prepares a draft of the proposed determination in relation to the application;
d) the Commissioner invites the agency (and any other persons the Commissioner thinks appropriate) to notify the Commissioner whether the agency wishes the Commissioner to hold a conference about the draft determination;
e) the Commissioner holds a conference if notified to do so by the agency;
f) the Commissioner makes the public interest determination or dismisses the application, giving reasons for the determination or dismissal;
the determination is required to be tabled in Parliament and is subject to disallowance;

h) the Commissioner may make the determination if satisfied that;
   - an act or practice of the agency breaches, or may breach, an IPP; but
   - the public interest in the agency doing the act, or engaging in practice, substantially outweighs the public interest in adhering to that IPP.

107. While the determination is in force, the agency does not breach the IPP by doing the act or engaging in the practice the subject of the determination.

108. There is also a process for the Federal Privacy Commissioner to make temporary public interest determinations in urgent circumstances where an application for a permanent public interest determination has been made (sections 80A to 80D).

109. The Office of the Federal Privacy Commissioner has published the Public Interest Determination Procedure Guidelines, which are available on the Office of the Federal Privacy Commissioner’s website. The website also lists determinations that have been made and are in force. If you wish to consider applying for a public interest determination, we recommend that you consult with the Office of the Federal Privacy Commissioner in the first instance.

IPP 11 – LIMITS ON DISCLOSURE OF PERSONAL INFORMATION – APPLICATION TO THE AFP

110. As it is likely that the AFP would provide relevant ANPR information (collected from its own or others’ ANPR-enabled cameras) to CrimTrac, it is necessary to consider the application of IPP 11 to the AFP.

111. For reasons similar to those discussed above, we think a reasonable argument could be made that the exception in IPP 11.1(e) would apply to support the disclosure of relevant ANPR information for criminal investigations (and related law enforcement) purposes. However, we do not think the exception would apply to disclosure of the information to CrimTrac for road safety purposes (or all national security purposes). In this regard, we note that the exemption for disclosure of personal information to ASIO (see s 7(1A) of the Commonwealth Privacy Act, discussed above) applies only insofar as it involves the disclosure of information ‘to ASIO’. We doubt this particular provision would exempt from IPP 11.1 the disclosure of personal information to other agency where that agency may possibly later disclose the information to ASIO.

112. However, we think it would be possible to rely on the exception in IPP 11.1(b) to allow the disclosure of relevant ANPR information to CrimTrac for the broader purposes of the ANPR program. Section 60A of the AFP Act relevantly provides as follows:

60A Secrecy

(a) This section applies to a person who is, or was at any time:

   (a) the Commissioner, or
   (b) a Deputy Commissioner, or
   (c) an AFP employee, or
   (d) a special member, or
   (da) a special protective service officer, or
   (e) a person engaged under section 35, or
[2] A person to whom this section applies must not, directly or indirectly:

[a] make a record of any prescribed information; or

[b] divulge or communicate any prescribed information to any other person;

except for:

[c] the purposes of this Act or the regulations; or

[d] the purposes of the Law Enforcement Integrity Commissioner Act 2006 or regulations under that Act; or

[e] the purposes of the Witness Protection Act 1994 or regulations under that Act; or

[f] the carrying out, performance or exercise of any of the person’s duties, functions or powers under Acts or regulations mentioned in paragraphs (c), (d) and (e).

[3] In this section:

personal information has the same meaning as in the Privacy Act 1988.

prescribed information means information obtained by a person to whom this section applies:

[a] in the course of carrying out, performing or exercising any of the person’s duties, functions or powers under:

[i] this Act or the regulations; or

[ii] the Law Enforcement Integrity Commissioner Act 2006 or regulations under that Act; or

[iii] the Witness Protection Act 1994 or regulations under that Act; or

[b] otherwise in the course of the person’s service, employment or engagement under Acts or regulations mentioned in paragraph [a].

Note: The Privacy Act 1988 contains provisions relevant to the use and disclosure of information divulged or communicated under this Act.

113. Section 60A(2)(c) and (f) contemplate the disclosure of prescribed information ‘for the purposes of the Act’ or ‘for the carrying out, performance or exercise of any of the person’s duties, functions or powers under [the AFP Act]’. In our view, information disclosed in accordance with s 60A would be authorised under law for the purposes of IPP 11.1(d). Relevant ANPR information would be likely to be ‘prescribed information’ for the purposes of s 60A. Having regard to the functions of the AFP, particularly those under s 8(a), 16(b), (d) and (c) of the AFP Act (see above), we think disclosure of relevant ANPR information to CrimTrac by the AFP would be ‘for the purposes of the Act’ or ‘for the carrying out, performance or exercise of any of the person’s duties, functions or powers under [the AFP Act]’ (s 60A(2)(c) and (f)).
IPP 11 – LIMITS ON DISCLOSURE OF PERSONAL INFORMATION – APPLICATION TO ACT AGENCIES

114. As ACT agencies may also provide relevant ANPR information (collected from their own or others’ ANPR-enabled cameras) to CrimTrac, it is necessary to consider the application of IPP 11 to ACT agencies.

115. For the reasons discussed above, we think the exception in IPP 11.1(c) would apply to support the disclosure to CrimTrac of relevant ANPR information for criminal investigation and related law enforcement purposes. However, we do not think the exception would apply to disclosure of the information to CrimTrac for road safety purposes (and possibly some national security purposes). As discussed above in relation to the AFP, we doubt that the exemption for disclosure of personal information to ASIO would effectively allow ACT agencies to disclose personal information to CrimTrac so that CrimTrac could, if it wished, subsequently disclose the information to ASIO.

116. It may be possible to rely on the exception in IPP 11.1(d) to allow ACT agencies to disclose specific ANPR information to CrimTrac. It would be necessary to consider the terms of relevant ACT legislation in order determine whether this exception would be applicable. This aspect is considered below.

Application of the Commonwealth Privacy Act to the private sector

117. We mention that the Commonwealth Privacy Act also applies to certain private sector organisations. It does so by regulating the collection, storage, use and disclosure of personal information by such organisations. The key rules are set out in the National Privacy Principles in Schedule 3 to the Commonwealth Privacy Act. Generally speaking, the NPPs are similar but less prescriptive than the IPPs and there are more exceptions to the various requirements and prohibitions.

118. It is not clear whether and, if so, to what extent private sector organisations would be involved in the collection and disclosure of relevant ANPR information. If such organisations are so involved, issues broadly similar to those discussed in this advice may arise in relation to those organisations. This aspect is not considered further in this report.
NSW privacy law – the Privacy and Personal Information Protection Act 1998 [NSW]

OVERVIEW AND SUMMARY

119. The Privacy and Personal Information Protection Act 1998 (the NSW Privacy Act) is broadly equivalent to the Commonwealth Privacy Act. The NSW Privacy Act regulates the collection, storage, use and disclosure of personal information by NSW public sector agencies by stipulating a number of ‘information protection principles’ (NSW IPPs). The NSW IPPs correspond to the IPPs. The concept of ‘personal information’ is central to the NSW Privacy Act. The term is defined in the Act and is generally the same as the definition of the term in the Commonwealth Privacy Act.

120. The NSW IPPs do not impose obligations or requirements on Commonwealth agencies. With this exception, the scope and general operation of the NSW Privacy Act is broadly equivalent to that of the Commonwealth Privacy Act (discussed above).

121. We concluded above that some relevant ANPR information would be likely to be ‘personal information’ as defined. It is therefore necessary to consider the application of the NSW Privacy Act in two main respects. First, as relevant ANPR information would be collected by ANPR-enabled cameras owned, operated or controlled by NSW public sector agencies, it is necessary to consider the rules in the NSW Privacy Act that regulate collection of personal information. Secondly, as this information would be provided to CrimTrac, it is necessary to consider the rules in the NSW Privacy Act that regulate the disclosure of personal information.

122. We do not think there would be an impediment in the NSW Privacy Act to the collection and subsequent disclosure by NSW public sector agencies (including the NSW Police Force) of relevant ANPR information for the purposes of the ANPR program, provided that it was a clear function or activity of relevant NSW public sector agencies to do so. Legislation may be necessary to give NSW agencies this particular function or activity (see further below). In any event, there are several options, including non-legislative options, that could be adopted to overcome any impediment in the NSW Privacy Act and thereby allow relevant ANPR information to be disclosed by NSW public sector agencies to CrimTrac for all purposes of the ANPR program, particularly national security and road safety purposes.

COLLECTION

123. Section 8 of the NSW Privacy Act provides as follows:

8 Collection of personal information for lawful purposes

[1] A public sector agency must not collect personal information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and

(b) the collection of the information is reasonably necessary for that purpose.


124. A ‘public sector agency’ is defined broadly in the NSW Privacy Act and covers, eg. NSW departments and statutory authorities, and also the NSW Police Force [s 3]. It does not include Commonwealth agencies.
125. We assume, for the purposes of this report, that the collection by NSW public sector agencies of relevant ANPR information (through the use of their own or others' ANPR-enabled cameras) would satisfy the requirements in s 8(1). In order to provide definitive advice on this issue it would be necessary to identify the relevant NSW agencies and examine and consider their specific function (including any relevant NSW legislation). This aspect is considered further below. We note that, in any event, there is a limited exemption in the NSW Privacy Act for the NSW Police Force (see further below).

126. On our understanding of the ANPR program and our initial consideration of relevant NSW legislation (e.g., the Surveillance Devices Act 2007 [NSW], which is yet to commence, or the Workplace Surveillance Act 2005 [NSW]), it appears that the collection of relevant ANPR information by NSW public sector agencies would not occur by 'unlawful means' (i.e., by means contrary to law).

DISCLOSURE

127. Section 18 of the NSW Privacy Act relevantly provides as follows:

18  Limits on disclosure of personal information

     (1) A public sector agency that holds personal information must not disclose the
         information to a person [other than the individual to whom the information
         relates] or other body, whether or not such other person or body is a public
         sector agency, unless:

         (a) the disclosure is directly related to the purpose for which it was collected
             and the agency disclosing the information has no reason to believe that
             the individual to whom the information to be disclosed relates would
             object to the disclosure, or

         (b) the individual concerned is reasonably likely to have been aware, or has
             been made aware under section 10, that information of that kind is usually
             disclosed to that other person or body, or

         (c) the agency believes on reasonable grounds that the disclosure is
             necessary to prevent or lessen a serious and imminent threat to the life
             or health of the individual concerned or another person.

128. If collection of relevant ANPR information for the purposes of the ANPR program were
     clearly a function or activity of the NSW public sector agency concerned, it is likely that
     the exception in s 18(1)(a) would be applicable and therefore the prohibition in s 18(1) would
     generally not be an impediment. The exceptions in s 18(1)(b) and (c) would not likely be
     generally applicable in relation to the ANPR program.

129. The exception in s 18(1)(a) would not apply, however, if the relevant NSW public sector
     agency had reason to believe that the individual to whom the relevant ANPR information
     to be disclosed relates would object to the disclosure. This is unlikely to give rise to any major
     difficulties in practice, although there may be some situations where the exception in s
     18(1)(a) is not satisfied, for example, where an individual notifies the relevant NSW agency
     of his or her objection to the disclosure of relevant ANPR information. It is also possible
     that NSW public sector agencies may collect relevant ANPR information for different or
     narrower purposes than the purposes of the ANPR program, but may wish to disclose
     the information to CrimTrac for the broader purposes of the ANPR program. For these
     reasons, it is necessary to consider the operation of the general prohibition in s 18(1) in
     cases where the exception in s 18(1)(a) is inapplicable.
Exemption for NSW Police Force

130. Section 27 of the NSW Privacy Act exempts the NSW Police Force from compliance with any of the NSW IPPs, including the principle set out in s 18, except in relation to its ‘administrative and educative functions’. We do not consider that the activity of disclosing relevant ANPR information to CrimTrac would be part of the ‘administrative’ functions of the NSW Police Service. Rather, it would relate to its law enforcement, policing or other functions. The term ‘administrative’ in this context does not have a technical legal meaning, and hence takes its ordinary meaning – namely, pertaining to ‘the management or direction of any office or employment’ [Macquarie Dictionary, 2nd Revised Edition]. An argument could be put that the term here is used to refer to the exercise by the police service of its ‘governmental’ powers. However, in our view, the context suggests that here the NSW Privacy Act is referring to the internal management and organisational activities of the NSW Police Service, as distinct from its functions of law enforcement, crime prevention etc. In our view, therefore, the NSW Privacy Act would not prevent the NSW Police Service from disclosing relevant ANPR information to CrimTrac.

Police Regulation 2000 (NSW)

131. However, reg 46 of the Police Regulation 2000 (NSW) should be noted. It provides:

(1) A member of the NSW Police Force ... must treat all information which comes to his or her knowledge in his or her official capacity as strictly confidential, and on no account without proper authority divulge it to anyone.

(2) ... must observe the strictest secrecy in regard to this Police Force business, and is forbidden to communicate without proper authority in any way to any person outside the NSW Police Force any information in regard to police or other official business connected with his or her duties, or which may come to his or her knowledge in the performance of them.

(3) Nothing in this clause operates so as to impede the due performance of operational police duties or to prevent the giving of information if it is reasonable to do so for the purpose of dealing with an emergency when life or property is at risk.

132. This provision would operate as an absolute prohibition on disclosure of relevant ANPR information by any member of the NSW Police Force except with proper authority. (We doubt that the proposed disclosure would constitute ‘the due performance of operational police duties’ in reg 46(3), which, in our view, is concerned with the actual performance of police functions such as detecting a particular offender etc. However, if police were given the function of collecting relevant ANPR information for the purposes of the ANPR program, it may be possible to rely on reg 46(3).) Therefore, it may be legally safest that there be a ‘proper authority’ in place. If this were done, we think members of the NSW Police Force would be able to disclose relevant ANPR information to CrimTrac. The NSW does not specify who may give such an authorisation – however, in view of the fact that under s 8 of the Police Act 1990 (NSW) the Commissioner of Police is responsible for the management and control of the police service, it would seem appropriate for the authorisation to be given by the Commissioner (or, pursuant to s 31, by his or her delegate).

Other NSW public sector agencies

133. It is necessary also to consider the application of the NSW IPPs to NSW public sector agencies (other than the NSW Police Force) that might be involved in the disclosure of relevant ANPR information to CrimTrac.
134. In addition, s 19 of the NSW Act should also be noted in this regard. It relevantly provides that a NSW public sector that holds personal information must not disclose the information to a 'Commonwealth agency' unless:

a) a 'relevant privacy law' that applies to the personal information concerned applies to that Commonwealth agency; or
b) the disclosure is permitted under a privacy code of practice.

135. The term 'Commonwealth agency' is defined in s 3 of the NSW Privacy Act and would, in our view, clearly include CrimTrac.

136. The term 'relevant privacy law' is defined to mean a law that has been determined by the NSW Privacy Commissioner, by notice published in the NSW Gazette, to be a privacy law for the jurisdiction concerned (s 19(3)). We have not been able to determine whether the NSW Privacy Commissioner has exercised this power (eg, by determining that the Commonwealth Privacy Act is a relevant privacy law).

137. In addition, the NSW Privacy Commissioner is required to prepare a privacy code relating to the disclosure of personal information by NSW public sector agencies to, among others, Commonwealth agencies (s 19(4)). Unless such a code has been prepared, s 19 does not apply (see s 19(5)). We have not been able to determine, from the NSW Privacy Commissioner's website, whether such a code has been prepared. For the purposes of this report, we assume that such a code has not been made and s 19 does not apply.

138. It appears therefore that NSW public sector agencies (except the NSW Police Force) may, in some situations, be prohibited from disclosing relevant ANPR information to CrimTrac unless one or more of the exemptions from s 18 are applicable. There are several partly or potentially applicable exemptions.

EXEMPTION – LAW ENFORCEMENT PURPOSES

139. First, a NSW public sector agency is not required to comply with s 18 if the disclosure of the information concerned is made in connection with proceedings for an offence or for law enforcement purposes (s 235(c)(i)). This exception, by its reference to 'law enforcement purposes' (which are not defined), would arguably apply in relation to the bulk disclosure of relevant ANPR information to CrimTrac for the purpose of criminal investigations and related law enforcement activities. However, it is possible this exception may not apply as broadly as its terms might suggest, particularly in light of the specific exemption in s 25(3)(d)(ii) for a disclosure of personal information that is 'reasonably necessary...in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed'. It would not appear to be necessary to finally resolve the question of the scope of the 'law enforcement' exception in s 235(c)(i) since the exception would clearly not apply in relation to disclosure of the information to CrimTrac for road safety purposes or broader national security purposes.

EXEMPTION – AUTHORISED NON-COMPLIANCE WITH THE NSW IPPS

140. Section 25 of the NSW Privacy Act provides that NSW public sector agencies are not required to comply with the general prohibition on disclosure in s 18 if non-compliance is authorised or required under law. Section 25 provides as follows:

25 Exemptions where non-compliance is lawfully authorised or required

A public sector agency is not required to comply with section 9, 10, 13, 14, 15, 17, 18, or 19 if:
(a) the agency is lawfully authorised or required not to comply with the principle concerned; or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the [State Records Act 1998]).

141. Section 25 recognises that NSW public sector agencies can be authorised by law to disclose personal information. This authorisation can be express or implied by or under any NSW Act or any other law.

142. The application of the exemption in s 25 to a NSW public sector agency in relation to disclosure of relevant ANPR information to CrimTrac would depend primarily on the terms of other legislation and whether that legislation could be said to authorise or permit the agency’s disclosure of relevant ANPR information. We have attempted to identify particular NSW legislation for this purpose (see further below). Clearly, s 25 of the NSW Privacy Act provides a specific mechanism, by means of legislation, for relaxing the general prohibition on disclosure in s 18 and enabling the disclosure of ANPR information to CrimTrac.

EXEMPTION – MODIFICATION OF NSW IPPS

143. Part 3 of the NSW Privacy Act provides that ‘privacy codes of practice may be made for the purpose of protecting the privacy of individuals’ [s 29(1)]. A privacy code of practice may regulate, among other things, the disclosure of personal information held by NSW public sector agencies [s 29(2)]. Notably, a privacy code of practice may also provide for the disclosure of personal information to persons or bodies outside New South Wales [s 29(4)]. CrimTrac would be such a body.

144. A privacy code of practice can apply to:
- any specified class of personal information;
- any specified NSW public sector agency or class of NSW public sector agency; or
- any specified activity or specified class of activities.

145. Furthermore, a privacy code of practice can modify the application to any NSW public sector agency of one or more of the NSW IPPs [eg, the prohibition on disclosure in s 18], including, for example, exempting a NSW public sector agency or class of NSW public sector agency, from the requirement to comply with any NSW IPP [s 30].

146. Privacy codes of practice may be prepared by the NSW Privacy Commissioner or a NSW public sector agency. The codes are made by the relevant NSW Minister [s 31]. They are legally binding on NSW public sector agencies to which they apply [s 32].

147. A privacy code of practice would clearly be a possible option for overcoming any impediment in s 18 to the disclosure by NSW public sector agencies other than the NSW Police Force of relevant ANPR information to CrimTrac. As mentioned above, although a privacy code of practice may provide for the disclosure of personal information and may modify the application of s 18 including exempting an agency from compliance with s 18, a code of practice would need to be for the purpose of protecting the privacy of individuals [see s 29(1)]. It would not seem possible, therefore, for a privacy code of practice to do nothing more than simply allow a NSW public sector agency to disclose relevant ANPR information. A code may need to include measures for protecting individual privacy [eg, by allowing disclosure to occur only by secure means or to persons or bodies with responsibilities or systems for protecting the information from public disclosure].
EXEMPTION - REGULATIONS

148. One option for avoiding any restrictions in the NSW IPPs in relation to the disclosure of relevant ANPR information by NSW public sector agencies would be to make regulations for the purposes of s 4(3)(b) of the NSW Privacy Act. This provision provides that 'personal information does not include ... information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection'. It would be legally possible for the NSW Governor to make regulations under s 71(1) of the NSW Privacy Act prescribing relevant ANPR information for the purposes of s 4(3).

149. Regulations under s 71(2)(b) of the NSW Privacy Act provide another possible legal option. Section 71(2)(b) relevantly allows the NSW Governor to make regulations exempting NSW public sector agencies from any of the requirements of the NSW Privacy Act relating to the disclosure of specified classes of personal information or any other provision of the Act.
Victoria - Information Privacy Act 2000 [Vic]

OVERVIEW AND SUMMARY

150. The Information Privacy Act 2000 [Vic] (the Victorian Privacy Act) is broadly equivalent to the Commonwealth Privacy Act. The Victorian Privacy Act regulates the collection, storage, use and disclosure of personal information by Victorian public sector agencies. The concept of 'personal information' is central to the Victorian Privacy Act. The term is defined in the Act and is substantially the same as the definition of the term in the Commonwealth Privacy Act.

151. However, the Victorian Privacy Act does not apply to Commonwealth agencies subject to the Commonwealth Privacy Act (s 9(1)). With this exception, the scope and general operation of the Victorian Privacy Act is broadly similar to that of the Commonwealth Privacy Act (discussed above).

152. We concluded above that some relevant ANPR information would be 'personal information' as defined. It is therefore necessary to consider the application of the Victorian Privacy Act in two main respects. First, as relevant ANPR information would be collected by ANPR-enabled cameras owned, operated or controlled by Victorian agencies, it is necessary to consider the rules in the Victorian Privacy Act that regulate collection of personal information. Secondly, as this information would be provided to CrimTrac, it is necessary to consider the rules in the Victorian Privacy Act that regulate the disclosure of personal information.

153. In our view, provided it were a clear function or activity of relevant Victorian public sector agencies to collect relevant ANPR information for the purposes of the ANPR program, we do not think there would be any legal difficulties in the Victorian Privacy Act with the collection by Victorian public sector agencies of the relevant ANPR information and its subsequent use by CrimTrac for the purposes of the ANPR program. If this were not a function or activity of relevant Victorian agencies, there would be an impediment to the disclosure of the information to CrimTrac for the broader purposes of the ANPR program. In particular, legislation or delegated legislation would appear to be necessary to allow relevant ANPR information to be disclosed to CrimTrac for road safety purposes and possibly national security purposes.

PRINCIPLE 1 - COLLECTION

154. Victorian IPP 1 relevantly provides as follows:

1 Principle 1 - Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

155. An 'organisation' is a person or body to which the Victorian Privacy Act applies (ss 3 and 9) (ie, all or most Victorian public sector agencies).
156. We assume, for the purposes of this report, that the collection by Victorian agencies of relevant ANPR information (through the use of their own or others' ANPR-enabled cameras) would be necessary for one or more of their respective functions or activities. In order to provide definitive advice on this issue it would be necessary to identify the relevant Victorian agencies and examine and consider their specific functions (including any relevant Victorian legislation). This aspect is considered further below.

157. On our understanding of the ANPR program and our initial consideration of relevant Victorian legislation (eg, the Surveillance Devices Act 1999 (Vic), it appears that the collection of the relevant ANPR information by Victorian agencies would occur by 'lawful means' (ie, by means not contrary to law).

158. There may, however, be a question whether the proposed activities would involve the collection of personal information by 'fair' means. In this regard, the Office of the Victorian Privacy Commissioner has published Guidelines to the Information Privacy Principles [September 2006] (the Victorian Privacy Guidelines). The Victorian Privacy Guidelines relevantly provide as follows:

- Collecting information or monitoring individuals without notice and without their consent or knowledge as in the case of covert surveillance, will be regarded as unfair in most circumstances. There are some situations in which the use of covert surveillance may be justified and not considered unfair, depending on how it is conducted. Examples of such instances of covert surveillance include where it is:
  
  (a) expressly authorised under law by a decision maker required to take privacy interests into account, such as where a judge grants a covert warrant; or
  
  (b) carried out with prior notice that covert surveillance may be used for limited and specified purposes, such as might permit an employer to investigate suspected unlawful activity or misconduct of a serious kind, or allow an insurer to investigate a suspected fraudulent compensation claim.

Additional safeguards are generally required to ensure that less intrusive options are considered, that there is an identified legitimate need justifying the use of this intrusive option, that the surveillance is limited in scope and duration, that the privacy interests of any person (including third parties) are taken into account, and appropriate oversight and accountability mechanisms are in place to deter and detect any misuse.

159. We note that the Victorian Privacy Guidelines are expressed to be 'not legally binding ... [and] intended to indicate how the Privacy Commissioner interprets and applies the Information Privacy Principles' [para 4]. For these reasons, it would be advisable to discuss the ANPR program with the Victorian Privacy Commissioner. Depending on the precise circumstances in which collection of relevant ANPR information would occur, the collection may not occur by unfair means.

160. We mention that, as relevant ANPR information would be collected while individuals are using vehicles on public roads, we doubt that the information would be seen as having been collected in 'an unreasonably intrusive way'.

161. Our initial view is that the terms of Victorian IPP 1 would be unlikely to present any insurmountable legal difficulties for the ANPR program.