

# Terrorism and the Law

By Justice Peter McClellan

**I gratefully acknowledge the considerable research of Garth Riddell and the assistance of Penny Grist in the preparation of this paper.**

# Contents

<b>CHAPTER 1: DEFINING KEY CONCEPTS .....</b>	<b>7</b>
<b>1.1 Introduction.....</b>	<b>7</b>
<b>1.2 What is a “Terrorist Act”?.....</b>	<b>8</b>
1.2.1 Definition of “terrorist act” under NSW and Commonwealth Legislation.....	8
1.2.2 Interpretation.....	10
1.2.3 Geographical Scope of ”Terrorist Acts” .....	10
<b>1.3 What is a “Terrorist Organisation”? .....</b>	<b>12</b>
1.3.1 Historical Background .....	12
1.3.2 Definition of “terrorist organisation” .....	13
1.3.3 Listing Terrorist Organisations .....	13
<b>CHAPTER 2: CONVENTIONAL CRIMINAL LAWS THAT MAY APPLY TO TERRORIST ACTS OR ORGANISATIONS .....</b>	<b>16</b>
<b>2.1 Introduction.....</b>	<b>16</b>
<b>2.2 Treason.....</b>	<b>16</b>
<b>2.3 Treachery and related offences.....</b>	<b>17</b>
<b>2.4 Murder .....</b>	<b>20</b>
2.4.1 Definition and interpretation.....	20
2.4.2 Geographical scope.....	20
2.4.3 Conspiracy .....	21
2.4.4 Attempt .....	21
<b>2.5 Protected Persons.....</b>	<b>22</b>
2.5.1 UN Personnel .....	23
2.5.2 Commonwealth Public Officials.....	23
2.5.3 Internationally protected persons .....	23
<b>2.6 Unlawful Associations.....</b>	<b>25</b>
2.6.1 Definition of “Unlawful Association” .....	25
2.6.2 Listing Unlawful Associations.....	26
<b>2.7 Kidnapping And Threats .....</b>	<b>27</b>
2.7.1 Kidnapping and Hostage Taking .....	27
2.7.2 Threats.....	29
<b>2.8 Suicide .....</b>	<b>30</b>
<b>2.9 Weapons and Explosives .....</b>	<b>31</b>
<b>2.10 Other Offences .....</b>	<b>32</b>
2.10.1 Computer Offences .....	33
2.10.2 Genocide and Crimes Against Humanity .....	33

2.10.3 Hostile activities in a foreign state.....	33
2.10.4 To train or drill another person in the use of arms.....	34
<b>2.11 Conclusion .....</b>	<b>34</b>
<b>CHAPTER 3: NEW TERRORIST OFFENCES .....</b>	<b>36</b>
<b>3.1 Introduction and summary .....</b>	<b>36</b>
<b>TABLE 1: NEW TERRORIST OFFENCES.....</b>	<b>37</b>
<b>3.2 Terrorist Acts .....</b>	<b>39</b>
3.2.1 Offences .....	39
3.2.2 Scope of Application and Relevance of Intention .....	40
3.2.3 Case study of preparatory offences: <i>R v Faheem Khalid Lodhi</i> (unreported, NSWSC, 23 December 2005).....	41
<b>3.3 Terrorist Organisations.....</b>	<b>42</b>
3.3.1 Offences Relating to Involvement with the Activities of a Terrorist Organisation....	42
3.3.2 Intentionally associating with terrorist organisation members .....	44
3.3.3 Potential Problems with the Terrorist Organisation Provisions.....	45
3.3.4 Extraterritorial operation of the terrorist organisation provisions .....	46
<b>3.4 Harming Australians .....</b>	<b>47</b>
<b>3.5 Hoaxes and Other Offences Using Postal or Carriage Services .....</b>	<b>48</b>
<b>3.6 International Terrorism .....</b>	<b>49</b>
<b>3.7 Financing Terrorism: Freezable Assets .....</b>	<b>49</b>
<b>3.8 Espionage and Related Activities .....</b>	<b>50</b>
<b>3.9 Offences Relating to Foreign Travel Documents .....</b>	<b>51</b>
<b>3.10 Aviation Offences .....</b>	<b>52</b>
<b>3.11 Sedition.....</b>	<b>53</b>
<b>CHAPTER 4: TERRORIST OFFENCES AND THE CRIMINAL CHARGE AND TRIAL PROCESS .....</b>	<b>55</b>
<b>4.1 Detention after Arrest.....</b>	<b>55</b>
4.1.1 Detention Warrants in respect of Terrorist Offences – Commonwealth .....	56
4.1.2 Calculation of the Detention Period – Commonwealth Detention Warrants.....	56
4.1.3 Issuing Commonwealth Detention Warrants .....	57
<b>4.2 Bail and Non-parole Periods .....</b>	<b>57</b>
<b>4.3 Disclosure of National Security Information.....</b>	<b>58</b>
4.3.1 Enactment and Objectives.....	58

4.3.2 Definitions.....	58
4.3.3 Alteration to Criminal Procedure.....	59
4.3.4 Disclosure certificates.....	60
4.3.5 Closed hearings.....	61
4.3.6 Breach of a non-disclosure order or certificate, or a failure to notify the Attorney-General.....	62
4.3.7 Criticism and interpretation of the national security information provisions.....	63
4.3.8 Special Advocates.....	64
<b>4.4 Video Link Evidence in Terrorism Related Proceedings.....</b>	<b>65</b>
<b>CHAPTER 5: WARRANTS AND ORDERS: CONVENTIONAL POWERS .....</b>	<b>68</b>
<b>5.1 Introduction.....</b>	<b>68</b>
<b>5.2. Search Warrants .....</b>	<b>68</b>
5.2.1 Authorised officers and applications for search warrants.....	69
5.2.2 Reasonable grounds .....	70
5.2.3 Terms of a search warrant.....	72
5.2.4 Extension of a search warrant.....	74
5.2.5 Occupier’s notices.....	74
5.2.6 Issue of a search warrant by telephone .....	74
5.2.7 Search warrants under the Commonwealth legislation.....	75
<b>5.3 Listening Device Warrants.....</b>	<b>76</b>
5.3.1 Introduction.....	76
5.3.2 Recent changes to Listening Device Warrant Provisions.....	79
5.3.3 Definitions.....	79
5.3.4 Grounds for the Issue of a Listening Device Warrant .....	80
5.3.5 Interpretation of Grounds for the Issue of a Listening Device Warrant .....	80
5.3.6 Validity of Listening Device Warrants and Admissibility of Evidence .....	81
<b>5.4 Surveillance Device Warrants .....</b>	<b>83</b>
5.4.1 Definition .....	83
5.4.2 Issuing Authority .....	84
5.4.3 Grounds for application and issue of a surveillance device warrant .....	84
5.4.4 Emergency authorisations.....	85
5.4.5 Surveillance Devices in NSW.....	88
<b>5.5 Interception Warrants.....</b>	<b>89</b>
5.5.1 Interpretation.....	89
5.5.2 Application for an Interception Warrant.....	90
5.5.3 Grounds for the Issue of an Interception Warrant .....	91
5.5.4 Interceptions that are not authorised by an eligible Judge or AAT member .....	94
5.5.5 Uses to which intercepted evidence may be put .....	95
<b>TABLE 2: SUMMARY OF JUDICIAL ANTI-TERROR POWERS.....</b>	<b>97</b>
<b>CHAPTER 6: COMMONWEALTH WARRANTS AND ORDERS: NEW ANTI-TERROR POWERS .....</b>	<b>99</b>

<b>6.1 Summary.....</b>	<b>99</b>
<b>6.2 Control Orders - Commonwealth.....</b>	<b>99</b>
6.2.1 Obligations, prohibitions and restrictions that a control order may impose – Commonwealth.....	99
6.2.2 Grounds for the issue of an interim control order - Commonwealth.....	100
6.2.3 Terms of an interim control order - Commonwealth.....	101
6.2.4 Confirmation of an interim control order - Commonwealth.....	101
<b>6.3 Detention and Questioning Warrants: Warrants for the Purpose of Interrogation by ASIO - Commonwealth .....</b>	<b>103</b>
6.3.1 Introduction.....	103
6.3.2 <i>Australian Security Intelligence Organisation Act 1979</i> (Cth).....	103
6.3.3 Issuing a detention and questioning warrant – Commonwealth .....	105
6.3.4 Criticisms of the process for the issue of questioning and detention warrants.....	106
<b>6.4 Preventative Detention Orders – Commonwealth .....</b>	<b>106</b>
6.4.1 Initial preventative detention orders - Commonwealth .....	107
6.4.2 Process for continuing an ‘initial preventative detention order’ – Commonwealth .	108
6.4.3 Terms and operation of a preventative detention order - Commonwealth .....	109
6.4.4 Prohibited contact orders - Commonwealth .....	110
 <b>CHAPTER 7: NEW SOUTH WALES WARRANTS AND ORDERS: NEW ANTI-TERROR POWERS .....</b>	 <b>111</b>
<b>7.1 Special NSW Anti-terror Special Police Outside Judicial Oversight.....</b>	<b>111</b>
<b>7.2 Covert Search Warrants – NSW .....</b>	<b>112</b>
7.2.1 Covert Search Warrants – NSW .....	112
7.2.2 Application for a Covert Search Warrant – NSW .....	112
7.2.3 Grounds for the issue of a Covert Search Warrant – NSW .....	114
7.2.4 Terms of a Covert Search Warrant – NSW .....	115
<b>7.3 Preventative Detention Orders – NSW .....</b>	<b>116</b>
7.3.1 Interim preventative detention orders – NSW .....	116
7.3.2 Determination of preventative detention orders by the Court – NSW.....	118
7.3.3 Terms and operation of preventative detention orders – NSW.....	119
7.3.4 Prohibited contact orders – NSW .....	120
 <b>APPENDIX 1: SUMMARY OF ISSUING AUTHORITIES FOR WARRANTS AND ORDERS CONSIDERED IN THIS PAPER .....</b>	 <b>122</b>

## Chapter 1: Defining Key Concepts

### 1.1 Introduction

There are two key concepts in the new terrorism legislation. They are a “terrorist act” and a “terrorist organisation.”

Prior to September 11, the Northern Territory was the only Australian jurisdiction to have enacted specific terrorist offences.<sup>1</sup> It is trite to observe that “terrorism” (in a popular rather than a legal sense) could still have occurred in any other jurisdiction. Presumably, outside of the Northern Territory it was believed that pre-existing laws adequately covered the field of potential terrorist activity, and further legislation was unnecessary. Writing extrajudicially, Judge Rosalyn Higgins, the first female appointed to the Bench of the International Court of Justice, argued in 1997 that:

*Terrorism is a term without any legal significance. It is merely a convenient way of alluding to activities...widely disapproved of and in which either the methods used are unlawful, or the targets protected, or both.*<sup>2</sup>

Obviously, now that the terms “terrorist act” and “terrorist organisation” have been defined by legislation at both state<sup>3</sup> and federal<sup>4</sup> level, it is no longer true to say that in NSW terrorism is a legal concept without content. Nevertheless, Judge Higgins’ comments serve to highlight the fact that at their core, most if not all terrorist acts fall within traditional definitions of criminal conduct. This is particularly apparent in the definitions given to “international terrorism” and “domestic terrorism” under s 2331 of Title 18 of the *United States Code* (as amended by the *Patriot Act*<sup>5</sup>). To fall within either definition, the activities in question must involve acts “that are a violation of the criminal laws of the United States or of any State.”<sup>6</sup> Hence, whether or not something is a terrorist act depends upon whether or not the act is a breach of the pre-existing criminal law. The NSW and Commonwealth definition of a “terrorist act” takes a similar approach.

In their article “What is ‘Terrorism’? Problems of Legal Definition” Golder and Williams examine a number of legislative definitions of terrorism that have been employed around the world. They note that there is a relatively wide consensus in common law countries that terrorism as a concept “refers to political, religious or ideologically-motivated violence that causes harm to people or property, intended either to coerce a civilian population or government, or to instil fear in the population

---

<sup>1</sup> *Criminal Code Act 1983* (NT), Sch 1, ss 54 and 55.

<sup>2</sup> Quoted in: Golder, B and Williams, G, “What is ‘Terrorism’? Problems of Legal Definition” (2004) 27 *UNSWLJ* 270 (hereafter “What is Terrorism?”) at 271 (n 5).

<sup>3</sup> See, eg, *Terrorism (Police Powers) Act 2002* (NSW), s 3 (“terrorist act”) and *Crimes Act 1900* (NSW), s 310I (“terrorist organisation”).

<sup>4</sup> See, eg, *Criminal Code* (Cth), s 100.1 (“terrorist act”) and s 102.1 (“terrorist organisation”).

<sup>5</sup> *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001* (US).

<sup>6</sup> Or, in the case of international terrorism, acts that would be a violation of the criminal law if committed within jurisdiction. See subsections 2331(2) and 2331(5) for the full definitions.

or a certain part of it.”<sup>7</sup> The Commonwealth and NSW definition is clearly encapsulated by this description.

## **1.2 What is a “Terrorist Act”?**

The NSW and Commonwealth definitions of a “terrorist act” are proscribed conduct that in most cases will already be illegal. The two definitions are identical to each other in all respects except that the federal definition begins with the words “terrorist act means an action or threat of action,” while the NSW definition omits the words “or threat of action.”<sup>8</sup>

### **1.2.1 Definition of “terrorist act” under NSW and Commonwealth Legislation**

The definition in the Commonwealth *Criminal Code* reads as follows:

***terrorist act*** means an action or threat of action where:

- (a) *the action falls within subsection (2) and does not fall within subsection (3); and*
- (b) *the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and*
- (c) *the action is done or the threat is made with the intention of:*
  - (i) *coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or*
  - (ii) *intimidating the public or a section of the public.*

(2) *Action falls within this subsection if it:*

- (a) *causes serious harm that is physical harm to a person; or*
- (b) *causes serious damage to property; or*
- (c) *causes a person’s death; or*
- (d) *endangers a person’s life, other than the life of the person taking the action; or*
- (e) *creates a serious risk to the health or safety of the public or a section of the public; or*

---

<sup>7</sup> Golder and Williams, “What is Terrorism?” at 288-289.

<sup>8</sup> *Criminal Code (Cth)*, s 100.1 of *Terrorism (Police Powers) Act 2002* (NSW), s 3(1).



*(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:*

*(i) an information system; or*

*(ii) a telecommunications system; or*

*(iii) a financial system; or*

*(iv) a system used for the delivery of essential government services;  
or*

*(v) a system used for, or by, an essential public utility; or*

*(vi) a system used for, or by, a transport system.*

*(3) Action falls within this subsection if it:*

*(a) is advocacy, protest, dissent or industrial action; and*

*(b) is not intended:*

*(i) to cause serious harm that is physical harm to a person; or*

*(ii) to cause a person's death; or*

*(iii) to endanger the life of a person, other than the person taking the action; or*

*(iv) to create a serious risk to the health or safety of the public or a section of the public.*

*(4) In this Division:*

*(a) a reference to any person or property is a reference to any person or property wherever situated, within or outside Australia; and*

*(b) a reference to the public includes a reference to the public of a country other than Australia.<sup>9</sup>*

It would appear that almost any action that satisfies the criteria in subsection (2) is an action that would constitute an independent breach of the criminal law.

---

<sup>9</sup> *Criminal Code (Cth)*, s 100.1.

## 1.2.2 Interpretation

Terrorism is such a broad concept that any attempt to define it in a general way is sure to over-reach to at least some degree. Consequently, subsection (3) of the definition seeks to exclude acts of advocacy, protest, dissent or industrial action, so long as they are not carried out with the intention of creating a serious risk to the health or safety of the public or part thereof, or with the intention of seriously harming, killing or endangering the life of someone. This is notably different to the exception proposed in the original *Security Legislation Amendment (Terrorism) Bill 2002* (Cth), which provided that advocacy, protest, dissent or industrial action would have to be lawful to avoid the possibility of being characterised as a “terrorist act.”<sup>10</sup> Even so, subsection (3) remains problematic. In *R v Faheem Khalid Lodhi* (unreported, NSWSC, 14 February 2006), Whealy J (at [98]) stated that the proper construction of the Commonwealth definition of a “terrorist act” is as follows:

*a terrorist act is an action that is done (or a threat of action that is made) with each of the intentions specified in sub-paragraphs (b) and (c). The action must possess one or more of the features specified in sub-s (2) provided that it does not have the features specified in sub-s (3). The latter excludes advocacy, protest, dissent or industrial action that is not intended to cause the consequences detailed in the sub-section. The breadth of the definition is such that advocacy, protest, dissent or industrial action may be action that falls within sub-s (2), and be capable of founding a terrorist act, if it is not unaccompanied by the intentions specified in sub-s 3(b)(i), (ii), (iii) and (iv).*

It is apparent that the definition of a “terrorist act” is capable of catching conduct that does not fall within popular notions of a terrorist act. In particular, the definition only protects advocacy, protest, dissent and industrial action that is not *intended* to have certain results. Given that much protest and industrial action involves mass gatherings, it may be hard to know what the relevant intention of an individual may be. Would an individual nurse or a police officer<sup>11</sup> who joined in industrial action be guilty of a terrorist act if they, but none of their colleagues, did so with the intention of creating “a serious risk to the health or safety of the public or a section of the public”? Since the offence of engaging in a terrorist act is an offence under the *Criminal Code* (Cth), the definition of intention under s 5.2 will apply. Relevantly, s 5.2(3) provides that

*A person has intention with respect to a result if he or she means to bring it about or is aware that it will occur in the ordinary course of events.*

## 1.2.3 Geographical Scope of “Terrorist Acts”

The bulk of post-September 11 terrorist offences are enacted under federal law. The constitutional foundation for Part 5.3 (“Terrorism”) of the *Criminal Code* (Cth) – at least in its application to NSW – is based on a reference of power made under s 51(xxxvii) of the Constitution.<sup>12</sup>

<sup>10</sup> Ibid at 291.

<sup>11</sup> This example is adapted from: Ibid at 289-290.

<sup>12</sup> *Terrorism (Commonwealth Powers) Act 2002* (NSW).

The broad geographical scope of the definition of a “terrorist act” is immediately apparent. Section 100.4 makes this even clearer when it states that to the extent that Parliament has power,<sup>13</sup> Pt 5.3 of the *Criminal Code* (Cth) applies to:

*(a) all actions or threats of action that constitute terrorist acts (no matter where the action occurs, the threat is made or the action, if carried out, would occur); [and]*

*(b) all actions (preliminary acts) that relate to terrorist acts but do not themselves constitute terrorist acts (no matter where the preliminary acts occur and no matter where the terrorist acts to which they relate occur or would occur).<sup>14</sup>*

Moreover, most offences under Pt 5.3 of the *Criminal Code* (Cth) are category D offences.<sup>15</sup> Category D offences are offences with extended geographical jurisdiction, and they apply:

*(a) whether or not the conduct constituting the alleged offence occurs in Australia; and*

*(b) whether or not the results of the conduct constituting the alleged offence occurs in Australia.<sup>16</sup>*

Consequently, a terrorist act that occurs in a foreign country, that is perpetrated by foreigners exclusively against foreigners, and that has no effects in Australia, is nevertheless punishable under Australian federal domestic law. In *R v Izhar Ul-Haque* it was argued that it was beyond the power of the Commonwealth Parliament to enact legislation that has such an operation.<sup>17</sup> Bell J rejected this submission,<sup>18</sup> relying on statements made by members of the High Court in *Polyukhovich v The Commonwealth* (1991) 172 CLR 501 and *Victoria v The Commonwealth* (1996) 187 CLR 416. In particular, Her Honour quoted from the joint judgment of Brennan CJ, Toohey, Gaudron, McHugh and Gummow JJ in the latter case, where they adopted the statement made by Dawson J (at CLR 233) in *Polyukhovich* that the external affairs power:

*extends to places, persons, matters or things physically external to Australia. The word “affairs” is imprecise, but is wide enough to cover places, persons, matters or things. The word “external” is precise and is unqualified. If a place, person, matter or thing lies outside the geographical limits of the country, then it is external to it and falls within the meaning of the phrase “external affairs.”<sup>19</sup>*

<sup>13</sup> *Criminal Code* (Cth), s 100.4(4).

<sup>14</sup> *Criminal Code* (Cth), s 100.4(1).

<sup>15</sup> *Criminal Code* (Cth), ss 101.1(2), 101.2(4), 101.4(4), 101.5(4), 101.6(3), 102.9 and 103.3.

<sup>16</sup> *Criminal Code* (Cth), s 15.4.

<sup>17</sup> *R v Izhar Ul-Haque* (unreported, NSWSC, 8 February 2006) (Bell J).

<sup>18</sup> *R v Izhar Ul-Haque* (unreported, NSWSC, 8 February 2006) (Bell J) at [32].

<sup>19</sup> Quoted in *R v Izhar Ul-Haque* (unreported, NSWSC, 8 February 2006) (Bell J) at [31].

This means that if a place, person, matter or thing is physically external to Australia then it is ipso facto within the power of the Commonwealth Parliament to legislate in respect of such a place, person, matter or thing.

The question of extraterritoriality is different in respect of NSW, which employs a definition of a “terrorist act” that is almost identical to the Commonwealth definition. The words “peace, welfare and good government” in the *Constitution Act 1902* (NSW)<sup>20</sup> have been interpreted so as to limit, to some degree, the power of the NSW legislature to enact laws that apply extraterritorially.<sup>21</sup>

### **1.3 What is a “Terrorist Organisation”?**

#### **1.3.1 Historical Background**

The practice of outlawing subversive groups is not a new phenomenon. In an article that examines the legislative response of Europe’s democratic nations to the rise of fascist groups in the years immediately preceding World War II, Loewenstein notes that such laws were extremely common. He states that

*In most countries the statutes against subversive parties were rather vaguely phrased and the general criterion for defining the subversive character of a party, organisation, group or movement has been the explicit or implicit intention of leaders, members or sympathisers to aim at or to attempt, the overthrow or change of the existing form of democratic government by force. Such a sweeping statutory definition has permitted broad powers for suspending, dissolving or proscribing subversive parties.*<sup>22</sup>

In 1926 the Commonwealth government enacted laws against unlawful associations that fall neatly within this category. They are still contained in Pt IIA of the *Crimes Act 1914* (Cth) (see 2.6 below).

In 1950 the Menzies government enacted the *Communist Party Dissolution Act*. If valid, the effect of that Act would have been to:

- “(1) declare the Australian Communist Party an unlawful association and dissolve it;
- (2) enable the Governor-General to declare that a body of persons was communist and declare the body to be an unlawful association;
- (3) make it a criminal offence to continue or pretend to continue any activity of an outlawed body.”<sup>23</sup>

---

<sup>20</sup> Section 5. See also

<sup>21</sup> *Union Steamship Co of Australia Pty Ltd v King* (1988) 166 CLR 1 at 14 per Mason CJ, Wilson, Brennan, Deane, Dawson, Toohey and Gaudron JJ.

<sup>22</sup> Loewenstein, K, “Legislative Control of Political Extremism in European Democracies I” (1938) 38 *Columbia Law Review* 592 at 606.

<sup>23</sup> Barker, “Human rights” at 276.

The Act was declared invalid by the High Court.<sup>24</sup> This is so notwithstanding that at the time “most Australians saw communists as a real danger – indeed, their doctrine of world revolution and the dictatorship of the proletariat was widely viewed as a kind of political terrorism.”<sup>25</sup>

### 1.3.2 Definition of “terrorist organisation”

Under the *Criminal Code* (Cth) and for the purposes of Pt 6B (“Terrorism”) of the *Crimes Act 1900* (NSW) (which adopts the Commonwealth Act’s definitions of “terrorist organisation” and “member of a terrorist organisation”<sup>26</sup>), a “terrorist organisation” is

*(a) an organisation that is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not a terrorist act occurs); or*

*(b) an organisation that is specified by the regulations for the purposes of this paragraph.*<sup>27</sup>

An “organisation” is defined as a “body corporate or unincorporated body,” whether or not the body:

*(a) is based outside Australia; or*

*(b) or consists of persons who are not Australian citizens; or*

*(c) is part of a larger organisation.*<sup>28</sup>

In *R v Izhar Ul-Haque*,<sup>29</sup> it was submitted by the Crown (but neither accepted nor rejected by Bell J) that the term organisation refers “to a standing body of people with a particular purpose; not a transient group of conspirators who may come together for a single discrete criminal purpose.”<sup>30</sup>

### 1.3.3 Listing Terrorist Organisations

The Governor-General may specify an organisation under para (b), but before he or she may do so the Minister must be satisfied on reasonable grounds that the organisation:

*(a) is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not a terrorist act has occurred or will occur); or*

---

<sup>24</sup> *Australian Communist Party v Commonwealth* (1951) 83 CLR 1.

<sup>25</sup> Kirby, M, “Terrorism and the Democratic Response 2004” (2005) 28 *UNSWLJ* 221 (hereafter “Terrorism”) at 223.

<sup>26</sup> *Crimes Act 1900* (NSW), s 310I.

<sup>27</sup> *Criminal Code* (Cth), s 102.1(1), definition of “terrorist organisation.”

<sup>28</sup> *Criminal Code* (Cth), s 101.1.

<sup>29</sup> *R v Izhar Ul-Haque* (unreported, NSWSC, 8 February 2006) (Bell J).

<sup>30</sup> Crown written submissions, quoted in *R v Izhar Ul-Haque* (unreported, NSWSC, 8 February 2006) (Bell J) at [51].

*(b) advocates the doing of a terrorist act (whether or not a terrorist act has occurred or will occur).*<sup>31</sup>

Subsection (b) was inserted by the *Anti-terrorism Act (No 2) 2005* (Cth). An organisation “advocates” the doing of a terrorist act if:

*(a) the organisation directly or indirectly counsels or urges the doing of a terrorist act; or*

*(b) the organisation directly or indirectly provides instruction on the doing of a terrorist act; or*

*(c) the organisation directly praises the doing of a terrorist act in circumstances where there is a risk that such praise might have the effect of leading a person (regardless of his or her age or any mental impairment (within the meaning of section 7.3) that the person might suffer) to engage in a terrorist act.*<sup>32</sup>

In addition, the Minister must arrange for the Leader of the Opposition in the House of Representatives to be briefed in relation to the proposed regulation before the Governor-General can specify an organisation.<sup>33</sup>

Until recently there were provisions that provided for the specification of Hizballah, Hamas or Lashkar-e-Tayyiba organisations.<sup>34</sup> These provisions were inserted prior to the enactment of the *Criminal Code Amendment (Terrorist Organisations) Act 2004* (Cth), which repealed the provisions that required an organisation to be identified as a terrorist organisation by a UN mechanism before it could be specified as a “terrorist organisation” by the Governor-General. Following the removal of this requirement, the Hizballah, Hamas and Lashkar-e-Tayyiba provisions became largely redundant.<sup>35</sup> They were repealed by the *Anti-terrorism Act (No 2) 2005* (Cth).

The specification of a “terrorist organisation” by the Governor-General ceases to operate two years after the specification takes effect.<sup>36</sup> The Minister must make a declaration (which essentially revokes the specification) if he or she ceases to be satisfied that the organisation is a terrorist organisation,<sup>37</sup> and must consider an application for de-listing made by any individual or organisation.<sup>38</sup> (Note, however, that since the persons most interested in seeking the de-listing of an organisation will be members of that organisation, any member who comes forward is risking 10

---

<sup>31</sup> *Criminal Code* (Cth), s 102.1(2).

<sup>32</sup> *Criminal Code* (Cth), s 102.1(1A).

<sup>33</sup> *Criminal Code* (Cth), s 102.1(2A).

<sup>34</sup> *Criminal Code* (Cth), s 102.1(1), (former) paras (c)-(e) of the definition of “terrorist organisation.”

<sup>35</sup> Emerton, P, “Paving the Way for Conviction Without Evidence – A Disturbing Trend in Australia’s ‘Anti-Terrorism’ Laws” (2004) 4 *Queensland University of Technology Law and Justice Journal* 1 (hereafter “Paving the Way”) at 8 (n 19).

<sup>36</sup> *Criminal Code* (Cth), ss 102.1(3) and 102.1(8).

<sup>37</sup> *Criminal Code* (Cth), ss 102.1(4), 101.2(9), 101.2(10A) and 101.2(10C).

<sup>38</sup> *Criminal Code* (Cth), s 101.2(17).

years imprisonment for the offence of being a member of a terrorist organisation<sup>39</sup> if the application is unsuccessful.)

The following is a list of the organisations that have been specified as terrorist organisations by the Governor-General under the *Criminal Code Regulations 2002* (Cth) (as at 19 December 2005):

- Al Qaeda
- Jemaah Islamiyah
- Abu Sayyaf Group
- Jamiat ul-Ansar (JuA)
- Armed Islamic Group
- Salafist Group for Call and Combat/GSPC
- Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn
- Ansar al-Islam
- Asbat al-Ansar
- Islamic Movement of Uzbekistan
- Jaish-e-Mohammad
- Lashkar-e Jhangvi (LeJ)
- Egyptian Islamic Jihad
- Islamic Army of Aden (IAA)
- Hizballah's External Security Organisation (ESO)
- Palestinian Islamic Jihad (PIJ)
- Hamas' Izz al-Din al-Qassam Brigades
- Terrorist organisations — Lashkar-e-Tayyiba (LeT)
- Kurdistan Workers Party (PKK)

---

<sup>39</sup> *Criminal Code* (Cth), s 102.3.

## Chapter 2: Conventional Criminal Laws that may apply to Terrorist Acts or Organisations

### 2.1 Introduction

If the new terrorism offences had not been enacted, most terrorist activities would constitute “traditional” crimes. The methods used or the consequences sought to be obtained by terrorists would make their activities criminal. A brief contemplation of the actual or potential behaviour of terrorists will reveal many relevant offences. The following does not seek to be exhaustive – indeed, that would be impossible, given that terrorists often seek to deliberately defy prediction – but I will attempt to outline some of the more obvious offences that might apply to terrorist acts.

### 2.2 Treason

Actions done with the intention required by either (b) or (c) of the definition of a “terrorist act” (see above) will often be conventional criminal offences. The most obvious example is treason.<sup>40</sup>

Offences against the Sovereign are preserved in NSW under ss 11-16 of the *Crimes Act 1900* (NSW), and relate to the compassing, imagining, inventing, devising or intending to wound, maim, kill, depose, or levy war against the Sovereign or her heirs where an overt act has been taken towards expressing, publishing or fulfilling such an intention (etc). Notably, s 12 applies to anyone whether or not they are present in NSW and is punishable by 25 years imprisonment.

The *Treason Act 1351* (UK) (25 Ed III, St 5, c 2), which is preserved by s 16, protects from violation the Sovereign’s “companion,” her “eldest daughter unmarried,” and the wife of her “eldest son and heir” (amongst others).

The *Criminal Code* (Cth) creates an offence of treason that is expressed in language more readily comprehensible to modern readers. The *Security Legislation Amendment (Terrorism) Act 2002* (Cth) was responsible for repealing the old Commonwealth offence of treason (s 24 of the *Crimes Act 1914* (Cth)), and inserting the modernised version in the *Criminal Code* (Cth). Section 80.1(1) extends the concept of treason beyond the monarch to include acts that cause (or are intended to cause) the death of, or harm to, the Governor-General or the Prime Minister. Both the NSW and the Commonwealth Acts proscribe assisting enemies,<sup>41</sup> while the Commonwealth Act makes it treason to engage:

*in conduct that assists by any means whatever, with intent to assist:*

---

<sup>40</sup> Admittedly, it is possible to commit treason without having an intention such as that required by (b) or (c) (for example, if the Queen was subject to domestic violence, this would be treason even though it might not be politically, religiously or ideologically motivated). It is submitted that this would be a rare case, and that the appropriate charge would not be one of treason.

<sup>41</sup> *Criminal Code* (Cth), s 80.1(e); *Treason Act 1351* (UK) as incorporated by the *Crimes Act 1900* (NSW), s 16.



- (i) another country; or
- (ii) an organisation;

that is engaged in armed hostilities against the Australian Defence Force.<sup>42</sup>

It is also an offence under Commonwealth law to commit misprision of treason.<sup>43</sup> All Commonwealth treason offences (including misprision) are punishable by life imprisonment. Moreover, since s 80.1 offences are category D offences<sup>44</sup> (see above).

The federal offence is subject to certain exceptions that do not apply in NSW<sup>45</sup> (see 2.3 below). Even though s 80 was enacted as part of the Commonwealth's bevy of new anti-terror laws, it is recognisable as a treason offence and it is more appropriately characterised as such than as a specific terrorist offence.

### **2.3 Treachery and related offences**

Part II of the *Crimes Act 1914* (Cth) relates to offences against the government. A person commits treachery by doing any act or thing with intent:

- to overthrow the Constitution of the Commonwealth by revolution or sabotage; or
- to overthrow by force or violence the established government of the Commonwealth, of a State or of a proclaimed country.<sup>46</sup>

Treachery is also committed when a person is “within the Commonwealth or a Territory not forming part of the Commonwealth” and the person:

- levies war, or does any act preparatory to levying war, against a proclaimed country;
- assists, by any means whatever, with intent to assist, a proclaimed enemy of a proclaimed country; or
- instigates a person to make an armed invasion of a proclaimed country.<sup>47</sup>

Treachery may also be committed where a person assists (with intent) any person who is opposed or is likely to be opposed to a part of the Defence Force that is on, or proceeding to, service outside the “Commonwealth and the Territories not forming part of the Commonwealth,” or where a person assists (with intent) a person specified by proclamation.<sup>48</sup> Treachery is punishable by life imprisonment.

---

<sup>42</sup> *Criminal Code* (Cth), s 80.1(1)(f).

<sup>43</sup> *Criminal Code* (Cth), s 80.1(2).

<sup>44</sup> *Criminal Code* (Cth), s 80.4.

<sup>45</sup> *Criminal Code* (Cth), s 80.1(1A)-(1B), s 80.3 and *Crimes Act 1914* (Cth), s 24F.

<sup>46</sup> *Crimes Act 1914* (Cth), s 24AA(1)(a).

<sup>47</sup> *Crimes Act 1914* (Cth), s 24AA(1)(b).

<sup>48</sup> *Crimes Act 1914* (Cth), s 24AA(2).

An “act of sabotage” is the destruction, damage or impairment, with the intention of prejudicing the safety or defence of the Commonwealth, of any thing, substance or material, that is on or part of a prohibited place under s 80 or that is (inter alia) used or intended to be used:

- by the Defence Force or the defence force of a proclaimed country;
- in connection with the manufacture or testing of weapons or apparatus of war;
- for any purpose that relates directly to the defence of the Commonwealth.<sup>49</sup>

It is an offence punishable by 15 years imprisonment to commit such an act, or for a person to have in their possession any article that is capable of use, and which they intend to use, in carrying out such an act.<sup>50</sup> A person may be convicted of sabotage without having done an overt act evidencing an intention to prejudice the safety or defence of the Commonwealth so long as “from the circumstances of the case, from his conduct or from his known character as proved, it appears that his intention was to prejudice the safety or defence of the Commonwealth.”<sup>51</sup> The committing magistrate or presiding judge may decline to admit evidence relating to this if it would not tend to show that the accused had the relevant intention or if it would, subject to the warning the judge must give a jury under s 24AB(5), prejudice the fair trial of the accused.<sup>52</sup>

Certain acts that could potentially be acts of treachery or sabotage may not be unlawful if done in good faith.<sup>53</sup> Section 24F provides that:

*(1) Nothing in the preceding provisions of this Part makes it unlawful for a person:*

*(a) to endeavour in good faith to show that the Sovereign, the Governor-General, the Governor of a State, the Administrator of a Territory, or the advisers of any of them, or the persons responsible for the government of another country, has or have been, or is or are, mistaken in any of his or their counsels, policies or actions;*

*(b) to point out in good faith errors or defects in the government, the constitution, the legislation or the administration of justice of or in the Commonwealth, a State, a Territory or another country, with a view to the reformation of those errors or defects;*

*(c) to excite in good faith another person to attempt to procure by lawful means the alteration of any matter established by law in the Commonwealth, a State, a Territory or another country;*

*(d) to point out in good faith, in order to bring about their removal, any matters that are producing, or have a tendency to produce, feelings of*

<sup>49</sup> Crimes Act 1914 (Cth), s 24AB(1).

<sup>50</sup> Crimes Act 1914 (Cth), s 24AB(2).

<sup>51</sup> Crimes Act 1914 (Cth), s 24AB(3).

<sup>52</sup> Crimes Act 1914 (Cth), s 24AB(4).

<sup>53</sup> Crimes Act 1914 (Cth), s 24F.

*ill-will or hostility between different classes of persons; or*

*(e) to do anything in good faith in connexion with an industrial dispute or an industrial matter.*

*(2) For the purpose of subsection (1), an act or thing done:*

*(a) for a purpose intended to be prejudicial to the safety or defence of the Commonwealth;*

*(b) with intent to assist an enemy:*

*(i) at war with the Commonwealth; and*

*(ii) specified by proclamation made for the purpose of paragraph 80.1(1)(e) of the Criminal Code to be an enemy at war with the Commonwealth;*

*(ba) with intent to assist:*

*(i) another country; or*

*(ii) an organisation (within the meaning of section 100.1 of the Criminal Code );*

*that is engaged in armed hostilities against the Australian Defence Force;*

*(c) with intent to assist a proclaimed enemy, as defined by subsection 24AA(4) of this Act, of a proclaimed country as so defined;*

*(d) with intent to assist persons specified in paragraphs 24AA(2)(a) and (b) of this Act; or*

*(e) with the intention of causing violence or creating public disorder or a public disturbance;*

*is not an act or thing done in good faith.*

Note that subsection (ba) was inserted by the *Security Legislation Amendment (Terrorism) Act 2002* (Cth). Section 80.1(6) of the *Criminal Code* (Cth) provides that s 24F applies to the to the Commonwealth offence of treason as though the offence was a provision of Pt II of the *Crimes Act 1914* (Cth).

Part II of the *Crimes Act 1914* (Cth) also makes it an offence punishable by life imprisonment to incite mutiny<sup>54</sup> or to assist a prisoner of war to escape.<sup>55</sup> It is an offence punishable by 10 years imprisonment to intentionally damage property of the Commonwealth, whether real or personal (with strict liability attaching to the fact that

---

<sup>54</sup> *Crimes Act 1914* (Cth), s 25.

<sup>55</sup> *Crimes Act 1914* (Cth), s 26.

the property was property belonging to the Commonwealth).<sup>56</sup> The offence of hindering or interfering by violence, threats or intimidation of any kind with the free exercise of a person's political rights or duties attracts a maximum penalty of three years imprisonment.<sup>57</sup>

## **2.4 Murder**

### **2.4.1 Definition and interpretation**

Section 18(1)(a) of the *Crimes Act 1900* (NSW) provides that:

*Murder shall be taken to have been committed where the act of the accused, or thing by him or her omitted to be done, causing the death charged, was done or omitted with reckless indifference to human life, or with intent to kill or inflict grievous bodily harm upon some person, or done in an attempt to commit, or during or immediately after the commission, by the accused, or some accomplice with him or her, of a crime punishable by imprisonment for life or for 25 years.*

Clearly, this will cover the vast majority of terrorist attacks that result in somebody's death. Recent terrorist acts have tended to be aimed specifically at causing human casualties and it would not be hard to infer an intent to kill or cause grievous bodily harm in such cases. The punishment for murder is life imprisonment.<sup>58</sup>

### **2.4.2 Geographical scope**

Offences against the *Crimes Act 1900* (NSW) – unless the Act otherwise provides<sup>59</sup> - are not to be taken to extend beyond jurisdiction unless there is a "geographical nexus" between the State and the offence.<sup>60</sup> Hence terrorist acts that occur wholly outside of NSW (and a fortiori Australia) may fall outside the scope of s 18. The requisite geographical nexus only exists if:

- (a) the offence is committed wholly or partly in the State (whether or not the offence has any effect in the State), or*
- (b) the offence is committed wholly outside the State, but the offence has an effect in the State.*<sup>61</sup>

Section 10B provides that:

*the place in which an offence has an effect includes:*

- (a) any place whose peace, order or good government is threatened by the offence, and*

---

<sup>56</sup> *Crimes Act 1914* (Cth), s 29.

<sup>57</sup> *Crimes Act 1914* (Cth), s 28.

<sup>58</sup> *Crimes Act 1900* (NSW), s 19A.

<sup>59</sup> *Crimes Act 1900* (NSW), s 10A(3).

<sup>60</sup> *Crimes Act 1900* (NSW), s 10A(2).

<sup>61</sup> *Crimes Act 1900* (NSW), s 10C(2).

*(b) any place in which the offence would have an effect (or would cause such a threat) if the criminal activity concerned were carried out.*

### 2.4.3 Conspiracy

Unlike murder, the offence of conspiracy to murder is expressed to apply outside jurisdiction. Section 26 of the *Crimes Act 1900* (NSW) provides for 25 years imprisonment for anyone who:

*conspires and agrees to murder any person, whether a subject of Her Majesty or not, and whether within the Queen's dominions or not, or solicits, persuades or endeavours to persuade, or proposes to, any person to commit any such murder.*

Since the essence of a conspiracy is an agreement,<sup>62</sup> the offence can be proved even if no overt acts have been taken to implement the agreement<sup>63</sup> (although such acts will usually provide good evidence that an agreement in fact existed). In relation to most other unlawful acts, conspiracy to commit them is a common law offence for which the penalty is at large. The position is somewhat different in relation to federal offences. Under the *Criminal Code* (Cth) the penalty for conspiring to commit an offence punishable by at least 12 months imprisonment or 200 penalty units is the same as the penalty prescribed for the substantive offence.<sup>64</sup> Moreover, to be guilty of a conspiracy offence:

*(a) the person must have entered into an agreement with one or more other persons; and*

*(b) the person and at least one other party to the agreement must have intended that an offence would be committed pursuant to the agreement; and*

*(c) the person or at least one other party to the agreement must have committed an overt act pursuant to the agreement.<sup>65</sup>*

Since conspiracy charges can be laid whether or not the substantive offence has been completed, and whether or not the substantive offence is also charged, conspiracy offences are an attractive option for law enforcement agencies. This is especially so given that wider evidence will be admissible to prove a conspiracy than would be admissible to prove the substantive offence.<sup>66</sup>

### 2.4.4 Attempt

An attempt to commit an unlawful act is another common law offence that has been codified in relation to murder and Commonwealth offences. Unlike attempts to

---

<sup>62</sup> See *O'Brien* (1974) 59 Cr App R 222 per Widgery LCJ.

<sup>63</sup> *Rogerson* (1992) 174 CLR 268.

<sup>64</sup> Section 11.5(1).

<sup>65</sup> *Criminal Code* (Cth), s 11.5(2).

<sup>66</sup> See generally Brown, D, Farrier, D, Egger, S and McNamara, L, *Criminal Laws*, 3<sup>rd</sup> ed, Federation Press, Sydney, 2001, pp. 1310-1322.

commit other offences (for which the penalty is the same as for the completed offence<sup>67</sup>), the penalty for attempted murder is imprisonment for 25 years.<sup>68</sup> The *Crimes Act 1900* (NSW) contains several attempted murder provisions that might be applicable to terrorist acts. For instance, it is attempted murder for anyone, with intent to commit murder, to:

- administer to, or cause to be taken by, any person any poison, or other destructive thing;<sup>69</sup> or
- by any means wound, or cause grievous bodily harm to a person;<sup>70</sup> or
- by the explosion of gunpowder, or other explosive substance, destroy or damage any building.<sup>71</sup>

Section 29 provides that, “whether any bodily injury is effected or not,” it is attempted murder for anyone, with intent to commit murder, to inter alia:

- *attempt* to administer to, or cause to be taken by, any person any poison, or other destructive thing; or
- shoot at, or in any manner attempt to discharge any kind of loaded arms at any person.

These offences would apply, for instance, to any attempt to poison a water supply, or to any explosion directed at an embassy building, and so on. Section 30 provides a catch-all for any attempt to commit murder that falls outside of the acts specified in the other sections. In relation to other attempt offences, the actus reus is not as clearly specified as it is for the attempted murder offences set out above. The *Criminal Code* (Cth) is declaratory of the common law when it states that:

*for the person to be guilty [of an attempt offence], the person’s conduct must be more than merely preparatory to the commission of the offence. The question whether conduct is more than merely preparatory to the commission of the offence is one of fact.*<sup>72</sup>

The distinction between acts of preparation and acts of perpetration is a murky one. It is a distinction best drawn with a view towards proximity: is the act sufficiently proximate in time, place and/or goal to be considered part of a series of acts that would constitute the completed offence if not interrupted?<sup>73</sup>

## **2.5 Protected Persons**

There are a number of Commonwealth offences aimed at protecting persons who might be the likely targets of terrorists.

---

<sup>67</sup> *Crimes Act 1900* (NSW), s 344A; *Criminal Code* (Cth), s 11.1(1).

<sup>68</sup> *Crimes Act 1900* (NSW), ss 27-30.

<sup>69</sup> *Crimes Act 1900* (NSW), s 27.

<sup>70</sup> *Crimes Act 1900* (NSW), s 27.

<sup>71</sup> *Crimes Act 1900* (NSW), s 28. Section 28 provides for other types of attempts but these are less relevant to the discussion at hand.

<sup>72</sup> *Criminal Code Act* (Cth), s 11.1(2).

<sup>73</sup> See *DPP v Stonehouse* [1977] 2 All ER 909 per Lord Edmund-Davies.

### 2.5.1 UN Personnel

Division 71 of the *Criminal Code* (Cth) is titled “Offences against United Nations and associated personnel.” The Division was inserted in 2000.<sup>74</sup> It will only apply where the victim is a UN or associated person who is “engaged in a UN operation that is not an enforcement action,”<sup>75</sup> and only where there is a link between the offence and Australia sufficient to satisfy the Division’s jurisdictional requirement.<sup>76</sup> Where the Division applies, it is an offence, inter alia, to do any of the following in relation UN or associated personnel: murder; intentionally or recklessly cause harm or serious harm; kidnap; unlawfully detain; or intentionally cause damage to property. The penalties for these offences are substantially the same as their equivalents (i.e. where the victim is *not* a UN or associated person) under the *Crimes Act 1900* (NSW).<sup>77</sup> Smaller penalties apply for *threatening* to commit offences against UN or associated personnel.<sup>78</sup>

### 2.5.2 Commonwealth Public Officials

The *Criminal Code* (Cth) makes it an offence to cause harm to a Commonwealth public official.<sup>79</sup> A Commonwealth public official is defined in the *Code’s* Dictionary to include, amongst others, the Governor-General, Commonwealth MPs, and officers and employees of Commonwealth authorities. The offence carries a higher penalty (13 years, as opposed to 10 years in other cases) if the Commonwealth official is a Commonwealth judicial officer or law enforcement officer. It is also an offence punishable by 10 years imprisonment to cause harm to a former Governor-General, former Minister or former Parliamentary Secretary. Threatening to cause harm<sup>80</sup> or serious harm<sup>81</sup> to a Commonwealth public official is an offence, as is threatening to cause serious harm to a former Governor-General etc.<sup>82</sup>

### 2.5.3 Internationally protected persons

Section 8(3C) of the *Crimes (Internationally Protected Persons) Act 1976* (Cth), which carries a maximum sentence of 25 years incarceration, provides that:

*a person who intentionally destroys or damages by means of fire or explosive:*

*(a) any official premises, private accommodation or means of transport, of an internationally protected person; or*

---

<sup>74</sup> Criminal Code Amendment (United Nations and Associated Personnel) Act 2000.

<sup>75</sup> See, eg, *Criminal Code* (Cth), s 71.2(1)(b)-(c).

<sup>76</sup> *Criminal Code* (Cth), s 71.16.

<sup>77</sup> For example the punishment for murder (life imprisonment) and manslaughter (25 years) is the same under both Acts. Similarly, the punishment for kidnapping a UN or associated person is 15 years or 19 years for the aggravated offence; kidnapping under the *Crimes Act 1900* (NSW) (s 86) is punishable by 14 years, or 20 years if aggravated. However, there is no equivalent in the federal provisions to the NSW offence of specially aggravated kidnapping (25 years).

<sup>78</sup> *Criminal Code* (Cth), s 71.12.

<sup>79</sup> *Criminal Code* (Cth), s 147.1.

<sup>80</sup> *Criminal Code* (Cth), s 147.2(2).

<sup>81</sup> *Criminal Code* (Cth), s 147.2(1).

<sup>82</sup> *Criminal Code* (Cth), s 147.2(3).

*(b) any other premises or property in or upon which an internationally protected person is present, or is likely to be present;*

*with intent to endanger the life of that internationally protected person by that destruction or damage is guilty of an offence against this Act.*

“Internationally protected person” includes heads of state, officials and representatives of States (and so on) when they are in a foreign territory.<sup>83</sup> The *Crimes (Internationally Protected Persons) Act 1976* (Cth) creates several other offences in similar terms that provide differing penalties depending on whether the damage or destruction was done with or without intent to endanger the life of the internationally protected person, and whether or not fire or explosives are used.<sup>84</sup> The Act also creates offences relating to murdering, kidnapping or attacking an internationally protected person.<sup>85</sup> Notably, the kidnapping offence attracts a maximum sentence of life imprisonment. A threat to do anything that amounts to any of the above-mentioned offences is punishable by 7 years jail.<sup>86</sup> Offences under the *Crimes (Internationally Protected Persons) Act 1976* (Cth) apply extraterritorially<sup>87</sup> as though they were category D offences under the *Criminal Code* (Cth) (see above), but an offender will not be liable to prosecution unless:

*(a) the offence is committed in Australia or on an Australian ship or Australian aircraft; or*

*(b) the offence is committed after the Convention enters into force for Australia and the person is found in Australia or Australia is required by article 3 of the Convention to establish its jurisdiction over the offence.*<sup>88</sup>

### **2.5.3.1 Case study of the Application of ‘Protected Persons’ Legislation to Prosecute acts relating to Terrorism**

An example of the use of protected persons legislation against terrorism is the case of Jack Roche. In pursuance of a plan to attack Israeli or American interests in Australia, Roche travelled to Malaysia, Pakistan and Afghanistan to deliver correspondence and, while in an al-Qaeda camp near Kandahar, to be trained in the use of explosives. Roche claimed that on his travels he met such notorious characters as Osama bin Laden and Abu Bakar Bashir (the spiritual leader of Jemaah Islamiya).

The overt acts Roche took in Australia included taking video footage of the Israeli Consulate in Sydney as well as the Israeli Embassy in Canberra, purchasing igniters for the purpose of bomb-making and attempting to recruit another Australian Muslim to his cause.<sup>89</sup> Roche pleaded guilty to conspiracy to commit an offence against

---

<sup>83</sup> *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents 1973.*

<sup>84</sup> See *Crimes (Internationally Protected Persons) Act 1976* (Cth), s 8(3)-(3B).

<sup>85</sup> *Crimes (Internationally Protected Persons) Act 1976* (Cth), s 8(1)-(2).

<sup>86</sup> *Crimes (Internationally Protected Persons) Act 1976* (Cth), s 8(4).

<sup>87</sup> *Crimes (Internationally Protected Persons) Act 1976* (Cth), s 5.

<sup>88</sup> *Crimes (Internationally Protected Persons) Act 1976* (Cth), s 10. Note that the Convention *has* entered into force for Australia.

<sup>89</sup> This summary is drawn from *R v Roche* [2005] WASCA 4 per McKechnie J at [81-84].



s8(3C)(a) of the *Crimes (Internationally Protected Persons) Act 1976 (Cth)*, and was sentenced to 9 years imprisonment with a non-parole period of 4½ years.<sup>90</sup>

## **2.6 Unlawful Associations**

As we shall see in more detail below, the new terrorist legislation creates several offences pertaining to “terrorist organisations.” As mentioned above, the *Crimes Act 1914 (Cth)* has contained provisions of a similar nature in Pt IIA (which deals with “unlawful associations”) since 1926.

### **2.6.1 Definition of “Unlawful Association”**

Under Pt IIA, an unlawful association is:

*(a) any body of persons, incorporated or unincorporated, which by its constitution or propaganda or otherwise advocates and encourages:*

*(i) the overthrow of the Constitution of the Commonwealth by revolution or sabotage;*

*(ii) the overthrow by force or violence of the established government of the Commonwealth or of a State or of any other civilized [sic] country or of organized [sic] government; or*

*(iii) the destruction or injury of property of the Commonwealth or of property used in trade or commerce with other countries or among the States; [note that under s 30C it is an offence punishable by 2 years imprisonment to advocate or encourage by speech or writing the matters set out in (i)-(iii)]*

*or which is, or purports to be, affiliated with any organization [sic] which advocates or encourages any of the doctrines or practices specified in this paragraph;*

*(b) any body of persons, incorporated or unincorporated, which by its constitution or propaganda or otherwise advocates or encourages the doing of any act having or purporting to have as its object the carrying out of a seditious intention (see subsection (3)).<sup>91</sup>*

Subsection (3) provides that a seditious intention is an intention to use force or violence to effect any of the following purposes:

*(a) to bring the Sovereign into hatred or contempt;*

*(b) to urge disaffection against the following:*

*(i) the Constitution;*

---

<sup>90</sup> The Crown appeal against sentence was dismissed in *R v Roche* [2005] WASCA 4.

<sup>91</sup> *Crimes Act 1914 (Cth)*, s 30A(1).

(ii) *the Government of the Commonwealth;*

(iii) *either House of Parliament;*

(c) *to urge another person to attempt to procure a change, otherwise than by lawful means, to any matter established by law of the Commonwealth;*

(d) *to promote feelings of ill-will or hostility between different groups so as to threaten the peace, order and good government of the Commonwealth.*<sup>92</sup>

## 2.6.2 Listing Unlawful Associations

An unlawful association may also be declared by the Federal Court on application by the Attorney-General.<sup>93</sup> Where such a declaration has been made, any member of “the Committee or Executive” of an unlawful association shall be disqualified from voting in Commonwealth elections for 7 years unless entitled to vote under s 41 of the Constitution.<sup>94</sup> The Attorney-General may require a person to answer questions or furnish information relating to the financial situation of an unlawful association.<sup>95</sup> Failure to do so is punishable by six months imprisonment.<sup>96</sup> All the goods and chattels of an unlawful association are forfeited to the Commonwealth.<sup>97</sup> Part IIA creates the following offences in relation to unlawful associations:

- being a member, officer etc of an unlawful association (1 year imprisonment);<sup>98</sup>
- contributing money or goods to an unlawful association (6 months imprisonment);<sup>99</sup>
- receiving or soliciting contributions for an unlawful association (6 months imprisonment);<sup>100</sup> note that a publisher or printer of a newspaper or periodical is deemed to solicit contributions if their publication contains such a solicitation, or indicates where such contributions can be paid or delivered<sup>101</sup>);
- intentionally printing, publishing, selling, circulating etc a book, poster, newspaper etc for or in the interests of or issued by an unlawful association (6 months imprisonment);<sup>102</sup>
- intentionally permitting an unlawful association to meet in premises that the accused owns, leases etc (6 months imprisonment).<sup>103</sup>

The above offences, like all offences in the *Crimes Act 1914* (Cth) (unless otherwise specified), “appl[y] throughout the whole of the Commonwealth and the Territories and also appl[y] beyond the Commonwealth and the Territories.”<sup>104</sup>

<sup>92</sup> *Crimes Act 1914* (Cth), s 30A(3).

<sup>93</sup> *Crimes Act 1914* (Cth), subs 30A(1A) and s 30AA.

<sup>94</sup> *Crimes Act 1914* (Cth), s 30FD.

<sup>95</sup> *Crimes Act 1914* (Cth), s 30AB.

<sup>96</sup> *Crimes Act 1914* (Cth), s 30AB.

<sup>97</sup> *Crimes Act 1914* (Cth), s 30G.

<sup>98</sup> *Crimes Act 1914* (Cth)s 30B.

<sup>99</sup> *Crimes Act 1914* (Cth), s 30D(1).

<sup>100</sup> *Crimes Act 1914* (Cth), s 30D(1).

<sup>101</sup> *Crimes Act 1914* (Cth), s 30D(2).

<sup>102</sup> *Crimes Act 1914* (Cth), s 30F.

<sup>103</sup> *Crimes Act 1914* (Cth), s 30FC.

<sup>104</sup> *Crimes Act 1914* (Cth), s 3A.

## **2.7 Kidnapping And Threats**

Although the word “terrorism” has its origins in the violence perpetrated by the French government on its citizens during the French revolution,<sup>105</sup> terrorism as the word is now understood typically refers to violence or disruption caused in the name of a purported “higher purpose.” The terrorist acts that attract the most attention today are generally unannounced explosions, but the paradigmatic terrorist act prior to September 11 was the taking of hostages. In relation to this, there are at least two sorts of offences that might be relevant. Firstly, there are laws that proscribe the act of hostage taking itself, such as the offence of kidnapping. Secondly, there are offences that might apply to the threats or demands that terrorists might make following the act of kidnapping.

### **2.7.1 Kidnapping and Hostage Taking**

Under the *Crimes Act 1900* (NSW) it is an offence to kidnap a person<sup>106</sup> or to abduct a child.<sup>107</sup> The basic offence of kidnapping is the taking or detaining of a person without their consent:

*(a) with the intention of holding the person to ransom; or*

*(b) with the intention of obtaining any other advantage.*<sup>108</sup>

This is punishable by 14 years imprisonment. The penalty increases to 20 years for an aggravated offence,<sup>109</sup> or to 25 in the case of a specially aggravated offence.<sup>110</sup> The circumstances of aggravation are present where the person committing the offence does so:

*(a) in the company of another person or persons, and*

*(b) at the time of, or immediately before or after, the commission of the offence, actual bodily harm is occasioned to the alleged victim.*<sup>111</sup>

Where either (a) or (b) occur, the offence is aggravated. Where *both* (a) and (b) occur, the offence is specially aggravated.

The *Crimes (Hostages) Act 1989* (Cth) makes it an offence punishable by life imprisonment to take hostages.<sup>112</sup> Hostage-taking occurs when a person:

*(a) seizes or detains another person (in this section called the hostage); and*

---

<sup>105</sup> Golder and Williams, “What is Terrorism?” at 270.

<sup>106</sup> *Crimes Act 1900* (NSW), s 86.

<sup>107</sup> *Crimes Act 1900* (NSW), s 87.

<sup>108</sup> *Crimes Act 1900* (NSW), s 86(1).

<sup>109</sup> *Crimes Act 1900* (NSW), s 86(2).

<sup>110</sup> *Crimes Act 1900* (NSW), s 86(3).

<sup>111</sup> *Crimes Act 1900* (NSW), s 86(3).

<sup>112</sup> *Crimes (Hostages) Act 1989* (Cth), s 8.

(b) *threatens to kill, to injure, or to continue to detain, the hostage;*

*with the intention of compelling:*

(c) *a legislative, executive or judicial institution of Australia or in a foreign country;*

(d) *an international intergovernmental organisation; or*

(e) *any other person (whether an individual or a body corporate) or group of persons;*

*to do, or abstain from doing, any act as an explicit or implicit condition for the release of the hostage.*<sup>113</sup>

Subject to a contrary intention, the *Crimes (Hostages) Act 1989* (Cth) extends:

(a) *to acts, matters and things outside Australia, whether or not in or over a foreign country; and*

(b) *to all persons, irrespective of their nationality or citizenship.*<sup>114</sup>

However, ss 8 and 9 qualify the extraterritorial operation of the Act to a not insignificant extent.

Hijacking generally involves kidnapping or hostage-taking. The *Crimes (Aviation) Act 1991* (Cth) proscribes the hijacking of certain aircraft. Hijacking of an aircraft is defined as seizing or exercising control of an aircraft by force or threat of force, or by any other form of intimidation while on board the aircraft.<sup>115</sup> Hijacking certain aircraft is an offence punishable by life imprisonment.<sup>116</sup> The Act also creates several other offences relating, inter alia, to the taking control of,<sup>117</sup> destroying<sup>118</sup> or endangering the safety in flight<sup>119</sup> of certain aircraft, assaulting the crew of certain aircraft,<sup>120</sup> acts of violence on passengers and crew,<sup>121</sup> and so on.

The *Crimes (Ships and Fixed Platforms) Act 1992* (Cth) creates the offence of seizing a private ship which is equivalent – in its terms and in its penalty – to the offence of hijacking an aircraft.<sup>122</sup> Life imprisonment is also prescribed where a person destroys a private ship,<sup>123</sup> causes damage knowing it will endanger the safe navigation of a ship,<sup>124</sup> or causes death in the course of committing offences against

---

<sup>113</sup> *Crimes (Hostages) Act 1989* (Cth), s 7.

<sup>114</sup> *Crimes (Hostages) Act 1989* (Cth), s 5.

<sup>115</sup> *Crimes (Aviation) Act 1991* (Cth), s 9.

<sup>116</sup> *Crimes (Aviation) Act 1991* (Cth), s 13.

<sup>117</sup> *Crimes (Aviation) Act 1991* (Cth), s 16.

<sup>118</sup> *Crimes (Aviation) Act 1991* (Cth), s 18.

<sup>119</sup> *Crimes (Aviation) Act 1991* (Cth), s 25.

<sup>120</sup> *Crimes (Aviation) Act 1991* (Cth), s 21.

<sup>121</sup> *Crimes (Aviation) Act 1991* (Cth), s 14.

<sup>122</sup> *Crimes (Ships and Fixed Platforms) Act 1992* (Cth), s 8.

<sup>123</sup> *Crimes (Ships and Fixed Platforms) Act 1992* (Cth), s 10(1).

<sup>124</sup> *Crimes (Ships and Fixed Platforms) Act 1992* (Cth), s 10(2).

ss 8-13 of the *Crimes (Ships and Fixed Platforms) Act 1992* (Cth).<sup>125</sup> There are equivalent provisions relating to fixed platforms.<sup>126</sup> Serious penalties attach to other offences such as placing destructive devices on a ship<sup>127</sup> and destroying or damaging navigational facilities.<sup>128</sup> Both the *Crimes (Ships and Fixed Platforms) Act 1992* (Cth)<sup>129</sup> and the *Crimes (Aviation) Act 1991* (Cth)<sup>130</sup> are expressed to apply extraterritorially in the same terms as the *Crimes (Hostages) Act 1989* (Cth) (see above).

## 2.7.2 Threats

Pt 4AA of the *Crimes Act 1900* (NSW) (“Offences relating to transport services”) creates offences that would apply in the event of an aircraft, vessel or train being hijacked in NSW. Section 208 (“threatening to destroy etc an aircraft, vessel or vehicle”) goes further than the other provisions of Div 1 of Pt 4AA by applying to “transport vehicles” (such as buses) as well as aircrafts and vessels. Subsection (2) of s 208 makes it an offence punishable by 14 years imprisonment to make:

*a demand of another person with a threat:*

*(a) to destroy or damage, or endanger the safety of, an aircraft, vessel or transport vehicle, or*

*(b) to kill, or inflict bodily injury on, persons who are in or on an aircraft, vessel or transport vehicle.*

There are several other offences that apply to threats made in the course of a kidnapping (or indeed, in respect of most other types of terrorists acts). For instance, it is an offence punishable by 10 years imprisonment to knowingly send or deliver a document threatening to kill or inflict bodily harm on a person.<sup>131</sup> A person is guilty of affray (which can be committed in private as well as public places<sup>132</sup>) if he or she uses or threatens unlawful violence towards another person and the conduct is such as would cause a person of reasonable firmness present at the scene to fear for his or her personal safety (but note that for affray to be made out a threat cannot be made by the use of words alone).<sup>133</sup> Threatening injury to any person or property with intent to commit an indictable offence or to resist arrest attracts a penalty of 12 years jail (15 if aggravated).<sup>134</sup> Under s 199 of the *Crimes Act 1900* (NSW), it is an offence punishable by 5 years imprisonment to make

*a threat to another, with the intention of causing that other to fear that the threat would be carried out:*

---

<sup>125</sup> *Crimes (Ships and Fixed Platforms) Act 1992* (Cth), s 14.

<sup>126</sup> *Crimes (Ships and Fixed Platforms) Act 1992* (Cth), Pt 3.

<sup>127</sup> *Crimes (Ships and Fixed Platforms) Act 1992* (Cth), s 11.

<sup>128</sup> *Crimes (Ships and Fixed Platforms) Act 1992* (Cth), s 12.

<sup>129</sup> Section 5.

<sup>130</sup> Section 12.

<sup>131</sup> *Crimes Act 1900* (NSW), s 31.

<sup>132</sup> *Crimes Act 1900* (NSW), s 93C(5).

<sup>133</sup> *Crimes Act 1900* (NSW), s 93C.

<sup>134</sup> *Crimes Act 1900* (NSW), s 33B(1)(b).

*(a) to destroy or damage property belonging to that other or to a third person, or*

*(b) to destroy or damage the first-mentioned person's own property in a way which that person knows will or is likely to endanger the life of, or to cause bodily injury to, that other or a third person.*

The *Crimes Act 1900* (NSW) also makes provision with respect to hoaxes,<sup>135</sup> as well as threats of sabotage<sup>136</sup> and threats to contaminate goods with intent to cause public alarm or economic loss.<sup>137</sup>

The *Criminal Code* (Cth) contains offences proscribing threatening conduct in certain circumstances. For instance, s 139.1 makes it an offence punishable by 12 years imprisonment to make unwarranted demands with menaces against a Commonwealth public official.

The offence of piracy under s 52 of the *Crimes Act 1914* (Cth) (punishable by life imprisonment) might also be relevant. An act of piracy means

*any act of violence, detention or depredation committed for private ends by the crew or passengers of a private ship or aircraft and directed:*

*(a) if the act is done on the high seas or in the coastal sea of Australia – against another ship or aircraft or against persons or property on board another ship or aircraft; or*

*(b) if the act is done in a place beyond the jurisdiction of any country – against a ship, aircraft, persons or property.<sup>138</sup>*

However, given that the definition of “terrorist act” adopted by both the NSW and Commonwealth governments refers to an intention “of advancing a political, religious or ideological cause,”<sup>139</sup> it is questionable whether an act committed “for private ends” falls within the legal (distinct, perhaps, from the popular) concept of terrorism.

## **2.8 Suicide**

Although it is no longer an offence to commit or attempt to commit suicide,<sup>140</sup> any (surviving) accomplices of a suicide bomber may be guilty of an offence against s 31C of the *Crimes Act 1900* (NSW). Section 31C provides:

*(1) A person who aids or abets the suicide or attempted suicide of another person shall be liable to imprisonment for 10 years.*

*(2) Where:*

---

<sup>135</sup> *Crimes Act 1900* (NSW), Pt 3D.

<sup>136</sup> *Crimes Act 1900* (NSW), s 203C.

<sup>137</sup> *Crimes Act 1900* (NSW), s 93IC. See also *Criminal Code* (Cth), s 380.3.

<sup>138</sup> *Crimes Act 1914* (Cth), s 51.

<sup>139</sup> See, eg, *Terrorism (Police Powers) Act 2002* (NSW), s 3(1)(b).

<sup>140</sup> *Crimes Act 1900* (NSW), s 31A.

(a) a person incites or counsels another person to commit suicide; and

(b) that other person commits, or attempts to commit, suicide as a consequence of that incitement or counsel,

the first mentioned person shall be liable to imprisonment for 5 years.

The *Criminal Code Amendment (Suicide Related Material Offences) Act 2005* (Cth) inserted provisions into the *Criminal Code* (Cth) that commenced on the 6<sup>th</sup> of January this year. The provisions create offences punishable by a fine of 1000 penalty units in relation to using a telecommunications carriage service for accessing, transmitting etc suicide related material.

## **2.9 Weapons and Explosives**

Terrorist acts will often involve the use of a weapon or explosive. Part 3B of the *Crimes Act 1900* (NSW) creates several relevant offences including:

- possession of explosives in a public place (sentence is at large);<sup>141</sup>
- summary offence of making or possessing explosives for an unlawful purpose;<sup>142</sup>
- firing a firearm:
  - in or near a public place (10 years imprisonment);<sup>143</sup>
  - in or into any building or land (10 years imprisonment);<sup>144</sup>
  - at a building with reckless disregard for the safety of any person (14 years imprisonment);<sup>145</sup>
- possession of a firearm in a public place (10 years imprisonment);<sup>146</sup>
- possession of a firearm “in any other place so as to endanger the life of any other person” (imprisonment for 10 years);<sup>147</sup>
- possession of an unregistered firearm in a public place (10 years imprisonment, 14 if aggravated).<sup>148</sup>

Of course, reliance on such offences would not be necessary in any case where property is in fact damaged, a person is in fact harmed or a more culpable intent can be proved. In such cases offences such as murder, attempted murder, malicious damage to property (and so on) might be more appropriate. Division 6 of Pt 3 of the

---

<sup>141</sup> *Crimes Act 1900* (NSW), s 93F(1).

<sup>142</sup> *Crimes Act 1900* (NSW), s 93F(2).

<sup>143</sup> *Crimes Act 1900* (NSW), s 93G(1)(b).

<sup>144</sup> *Crimes Act 1900* (NSW), s 93H(2).

<sup>145</sup> *Crimes Act 1900* (NSW), s 93GA.

<sup>146</sup> *Crimes Act 1900* (NSW), s 93G(1)(a)(i).

<sup>147</sup> *Crimes Act 1900* (NSW), s 93G(1)(a)(ii).

<sup>148</sup> *Crimes Act 1900* (NSW), s 93I.

*Crimes Act 1900* (NSW) creates several serious offences that apply to the use or possession of weapons and explosives with intent. The most relevant offences include:

- maliciously discharging loaded arms with intent to cause grievous bodily harm or to resist arrest (14 years imprisonment, 20 if aggravated);<sup>149</sup>
- possessing, using, attempting to use or threatening to use an offensive weapon or instrument with intent to commit an indictable offence or to resist arrest (12 years imprisonment, 15 if aggravated);<sup>150</sup>
- burning, maiming, disfiguring, disabling or doing grievous bodily harm to any person by maliciously exploding gunpowder or other substance, or through the use of any corrosive fluid or destructive matter (25 years imprisonment);<sup>151</sup>
- maliciously exploding, sending, delivering, laying, casting, throwing or applying any explosive substance (etc) with intent to burn, maim, disfigure, disable or do grievous bodily harm to any person, whether or not bodily injury is effected (25 years imprisonment);<sup>152</sup>
- knowingly possessing, making or manufacturing any gunpowder, explosive substance, or dangerous or noxious thing (etc) with intent to injure or commit a serious indictable offence against the person of anyone, or for the purpose of enabling someone else so to do (10 years imprisonment);<sup>153</sup>
- causing an explosive to be placed in or near a building, vehicle, vessel, train, conveyance or public place with intent to cause bodily harm to any person, whether or not an explosion occurs or any bodily harm is cause (sentence at large).<sup>154</sup>

Use or manufacture of biological weapons by terrorists is increasingly becoming a matter of concern. Since 1976 the federal government has had legislation in place forbidding the development, production, stockpiling or acquisition of biological agents or toxins that have no peaceful justification.<sup>155</sup> It is also an offence to develop, produce (etc) weapons, equipment or means of delivery of such agents or toxins for hostile purposes.<sup>156</sup> The penalty for both offences is imprisonment for life and/or a \$10,000 fine for a natural person, or a \$200,000 fine for a corporation.<sup>157</sup>

## **2.10 Other Offences**

---

<sup>149</sup> *Crimes Act 1900* (NSW), s 33A.

<sup>150</sup> *Crimes Act 1900* (NSW), s 33B(1)(a).

<sup>151</sup> *Crimes Act 1900* (NSW), s 46.

<sup>152</sup> *Crimes Act 1900* (NSW), s 47.

<sup>153</sup> *Crimes Act 1900* (NSW), s 55.

<sup>154</sup> *Crimes Act 1900* (NSW), s 48.

<sup>155</sup> *Crimes (Biological Weapons) Act 1976* (Cth), s 8.

<sup>156</sup> *Crimes (Biological Weapons) Act 1976* (Cth), s 8.

<sup>157</sup> *Crimes (Biological Weapons) Act 1976* (Cth), s 8.



There are a vast array of other general offences that are capable of applying to terrorist acts. Not all of them can be dealt with here. However, there are some areas of the criminal law that it would be remiss not to mention.

### 2.10.1 Computer Offences

The first area is computer offences. The definition of “terrorist act” adopted in NSW and federal legislation recognises this potential area of terrorist activity by providing that actions that seriously interfere with, seriously disrupt, or destroy “an electronic system”<sup>158</sup> may constitute terrorist acts. In NSW, Pt 6 of the *Crimes Act 1900* (NSW) (“Computer offences”) has been in place since August 2001. The *Criminal Code* (Cth) also has a Part dealing with computer offences<sup>159</sup> (this Part was enacted after September 11 but the offences created are general in nature and were perhaps inevitable in the computer age).

### 2.10.2 Genocide and Crimes Against Humanity

Another set of provisions that were enacted after September 11 but that are general in scope are the provisions relating to genocide and crimes against humanity.<sup>160</sup> Terrorist acts are quite often done with a genocidal intent (i.e. an intention “to destroy, in whole or in part, [a] national, ethnical, racial or religious group, as such”<sup>161</sup>) or the intent requisite to constitute a crime against humanity (i.e. the conduct is committed “intentionally or knowingly as part of a widespread or systematic attack directed against a civilian population”<sup>162</sup>).

### 2.10.3 Hostile activities in a foreign state

The *Crimes (Foreign Incursions and Recruitment) Act 1978* (Cth) is also worth noting. That act prohibits engaging in hostile activities in a foreign state (20 years imprisonment – increased from 14 years by the *Anti-terrorism Act 2004* (Cth)),<sup>163</sup> doing certain acts preparatory to such activities (10 years imprisonment)<sup>164</sup> and recruiting persons in Australia to join organisations engaged in hostile activities against foreign governments (7 years imprisonment).<sup>165</sup> These offences are contained in ss 6, 7 and 8, respectively. The Act provides that

*engaging in a hostile activity in a foreign State consists of doing an act with the intention of achieving any one or more of the following objectives (whether or not such an objective is achieved):*

*(a) the overthrow by force or violence of the government of the foreign State or of a part of the foreign State;*

*(aa) engaging in armed hostilities in the foreign State;*

<sup>158</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 3(2)(f).

<sup>159</sup> Part 10.7.

<sup>160</sup> *Criminal Code* (Cth), Subdivs B and C of Div 268.

<sup>161</sup> See, eg, *Criminal Code* (Cth), s 268.3(c).

<sup>162</sup> See, eg, *Criminal Code* (Cth), s 268.8(b).

<sup>163</sup> *Crimes (Foreign Incursions and Recruitment) Act 1978* (Cth), s 6.

<sup>164</sup> *Crimes (Foreign Incursions and Recruitment) Act 1978* (Cth), s 7.

<sup>165</sup> *Crimes (Foreign Incursions and Recruitment) Act 1978* (Cth), s 8.

(b) causing by force or violence the public in the foreign State to be in fear of suffering death or personal injury;

(c) causing the death of, or bodily injury to, a person who:

(i) is the head of state of the foreign State; or

(ii) holds, or performs any of the duties of, a public office of the foreign State or of a part of the foreign State; or

(d) unlawfully destroying or damaging any real or personal property belonging to the government of the foreign State or of a part of the foreign State.<sup>166</sup>

Offences against ss 6 and 7 cannot be made out unless the accused was an Australian citizen or resident, or was present in Australia “before” (changed from “during the period of one year immediately preceding” by the *Anti-terrorism Act 2004* (Cth)) the act for a purpose connected with the act.<sup>167</sup>

The *Anti-terrorism Act 2004* (Cth) has narrowed the operation of the defence in s 6(4). That is, it is no longer a defence to an offence under s 6 if the acts alleged are performed as part of a person’s service with the armed forces of the government of a foreign State if:

- the person engages in hostile activity in a foreign State in or with a prescribed organisation,<sup>168</sup> or
- the person entered the foreign state with the intention to engage in armed hostilities while in or with a prescribed organisation.

A prescribed organisation is a terrorist organisation specified under paragraph (b) of the definition of terrorist organisation in s 102.1 of the *Criminal Code* (Cth), or any organisation prescribed by the regulations.

#### **2.10.4 To train or drill another person in the use of arms**

It is an offence under s 27 of the *Crimes Act 1914* (Cth) to train or drill another person in the use of arms in contravention of a proclamation made by the Governor-General (punishable by 5 years imprisonment), or to be so trained or drilled (2 years imprisonment).

#### **2.11 Conclusion**

There are a host of other offences – such as poisoning a water supply with intent to injure<sup>169</sup> - that could conceivably apply to terrorist acts. Quite often we will not even

---

<sup>166</sup> *Crimes (Foreign Incursions and Recruitment) Act 1978* (Cth), s 6(3).

<sup>167</sup> *Crimes (Foreign Incursions and Recruitment) Act 1978* (Cth), ss 6(2) and 7(2).

<sup>168</sup> *Crimes (Foreign Incursions and Recruitment) Act 1978* (Cth), ss 6(5)-(6).

<sup>169</sup> *Crimes Act 1900* (NSW), s 41A.

realise that some offences could have such an application until an appropriate case arises.

## Chapter 3: New Terrorist Offences

### **3.1 Introduction and summary**

Following September 11, there has been a significant amount of legislative activity dealing with terrorism. Some of the most significant pieces of federal legislation in this area are as follows (in chronological order):

- *Criminal Code Amendment (Anti-hoax and Other Measures) Act 2002* (Cth);
- *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* (Cth);
- *Security Legislation Amendment (Terrorism) Act 2002* (Cth);
- *Suppression of the Financing of Terrorism Act 2002* (Cth);
- *Criminal Code Amendment (Terrorist Organisations) Act 2002* (Cth);
- *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth);
- *Criminal Code Amendment (Offences Against Australians) Act 2002* (Cth);
- *Criminal Code Amendment (Terrorism) Act 2003* (Cth);
- *Criminal Code Amendment (Hizballah) Act 2003* (Cth);
- *Criminal Code Amendment ( Hamas and Lashkar-e-Tayyiba) Act 2003* (Cth);
- *ASIO Legislation Amendment Act 2003* (Cth);
- *ASIO Legislation Amendment (Terrorism) Act 2003* (Cth);
- *Criminal Code Amendment (Terrorist Organisations) Act 2004* (Cth);
- *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth);
- *Aviation Transport Security Act 2004* (Cth);
- *Anti-terrorism Act 2004* (Cth);
- *Anti-terrorism Act (No 2) 2004* (Cth);
- *Anti-terrorism Act (No 3) 2004* (Cth);
- *Anti-terrorism Act 2005* (Cth);
- *Anti-terrorism Act (No 2) 2005* (Cth);

In NSW, the most significant provisions are contained in:

- *Terrorism (Police Powers) Act 2002* (NSW);
- *Terrorism Legislation Amendment (Warrants) Act 2005* (NSW);
- *Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005* (NSW).

The following table provides a summary of some of the most significant new terrorist offences. The Acts referred to are federal Acts unless otherwise stated.

Table 1: New Terrorist Offences

<b>Offence</b>	<b>Section in the Criminal Code (Cth) [unless otherwise specified]</b>	<b>Degree of culpability (if relevant)</b>	<b>Max. Penalty</b>
Engaging in a terrorist act (created 2003)	s101.1		Life
Training in preparation for a terrorist act (created 2003)	s101.2	Knowingly Recklessly	25 15
Possessing a thing connected with preparation for a terrorist act (created 2003)	s101.4	Knowingly Recklessly	15 10
Collecting/making a document in preparation for a terrorist act (created 2003)	s101.5	Knowingly Recklessly	15 10
Doing an act in preparation for or planning a terrorist act (created 2003)	s101.6.		Life
Directing the activities of a terrorist organisation (created 2003)	s102.2	Knowingly Recklessly	25 15
Intentionally being a member of a terrorist organisation (created 2003)	s102.3 [Also <i>Crimes Act 1900</i> (NSW), s 310J] (created 2005)		10
Recruiting for a terrorist organisation (created 2003)	102.4	Knowingly Recklessly	25 15
Recklessly training with an organisation that is a terrorist organisation or a specified terrorist organisation (created 2004)	s102.5		25
Receiving funds from, or collecting funds for, a terrorist organisation (created 2005)	s102.6	Knowingly Recklessly	25 15
Providing support to a terrorist organisation (created 2003)	s102.7	Knowingly Recklessly	25 15

Knowingly associating with a member of a terrorist organisation with intention to assist the organisation (created 2004)	s 102.8		3
Providing or collecting funds where the person is reckless as to whether they will be used to engage in a terrorist act (created 2005)	ss 103.1 and 103.2		Life
Murdering an Australian citizen/resident overseas (created 2002)	s 115.1		Life
Manslaughtering an Australian citizen/resident overseas (created 2002)	s 115.2		25
Causing serious harm to an Australian citizen/resident overseas (created 2002)	s115.3	Knowingly Recklessly	20 15
Making bomb hoaxes using a postal or similar service (created 2002)	ss 471.10 and 471.11		10
Making bomb hoaxes using a telecommunications carriage service (created 2004)	ss 474.15 and 474.16		10
Recklessly causing an article to be carried by a postal service that gives rise to a danger of death or serious physical harm (created 2002)	s 471.13		10
Causing an explosive to be carried by post (created 2002)	s 471.15.		10
Placing or discharging a lethal device in certain places with the intention of causing death or serious harm (created 2002)	s72.3(1)		Life
Placing or discharging a lethal device in certain places with the intention of causing extensive destruction to the place if reckless as to whether destruction will result in major economic loss (created 2002)	s72.3(2)		Life
Making an asset available to a prescribed person or entity (created 2002)	<i>Charter of the United Nations Act 1945, s 21.</i>		5
Dealing with freezable assets (created 2002)	<i>Charter of the United Nations Act 1945, s 20.</i>		5
Communicating security or defence information to a foreign country/organisation (created 2002)	ss 91.1(1)-(2)		25

Copying or recording security or defence information for a foreign country/organisation (created 2002)	ss 91.1(3)-(4)		25
Urging the overthrow of the Constitution or Government by force or violence (created 2005)	s 80.2(1)		7
Urging interference in elections by force or violence (created 2005)	s 80.2(3)		7
Urging violence within the community (created 2005)	s 80.2(5)		7
Urging a person to assist the enemy (created 2005)	s 82(7)		7
Urging a person to assist those engaged in armed hostilities against the ADF (created 2005)	s 80.2(8).		7
Offences relating to foreign travel documents (created 2004)	<i>Passports Act 1938, Part 3.</i>		10
Offences relating to possession of weapons at airports or in aircraft (created 2004)	<i>Aviation Transport Security Act 2004, Pt 4, Div 3.</i>	Knowingly Strict liability	7 100 pen units
Offences relating to possession of prohibited items at airports or in aircraft (created 2004)	<i>Aviation Transport Security Act 2004, Pt 4, Div 4.</i>	Knowingly Strict liability	2 20 pen units

## **3.2 Terrorist Acts**

### **3.2.1 Offences**

It is an offence punishable by imprisonment for life to engage in a “terrorist act.”<sup>170</sup> Most other specific terrorist offences rely on the concept of a “terrorist act” to some extent.

The *Criminal Code* (Cth) creates several serious offences in relation to terrorist acts:

- Section 101.2 is directed against providing or receiving training that is “connected with preparation for, the engagement of a person in, or assistance in a terrorist act.”<sup>171</sup> The offence is punishable by 25 years imprisonment if the person providing or receiving training knows that the training is so connected with a terrorist act,<sup>172</sup> or 15 years if the person is reckless as to the existence of such a connection.<sup>173</sup>

<sup>170</sup> *Criminal Code* (Cth), s 101.1.

<sup>171</sup> Sections 101.2(1)(a)-(b) and 101.2(2)(a)-(b).

<sup>172</sup> Section 101.2(1)(c).

<sup>173</sup> Section 101.2(2)(c)

- Similar offences are created in relation to the possession of a thing, or the collection or making of a document, which is “connected with preparation for, the engagement of a person in, or assistance in a terrorist act.” Where the person knows of the connection, they are subject to 15 years imprisonment; where they are reckless as to the existence of the connection, the penalty is 10 years imprisonment.<sup>174</sup>

Unlike the training offence, the offences in the second point above are subject to an exception. They cannot be made out where the possession of the thing, or the collection or making of the document, “was not intended to facilitate preparation for, the engagement of a person in, or assistance in a terrorist act.”<sup>175</sup>

It is also an offence, punishable by life imprisonment, to:

- do any act “in preparation for, or planning, a terrorist act.”<sup>176</sup> This offence would seem to make the offences in ss 101.2-101.5 somewhat redundant, given that most acts that would fall within these sections would constitute “preparation for, or planning, a terrorist act;”
- provide or collect funds where the person is “reckless as to whether the funds will be used to facilitate or engage in a terrorist act;”<sup>177</sup> or
- intentionally make funds available to, or to collect funds for or on behalf of, another person where the first-mentioned person is reckless as to whether the other person will use the funds to facilitate or engage in a terrorist act.<sup>178</sup>

### 3.2.2 Scope of Application and Relevance of Intention

Schedule 1 of the *Anti-terrorism Act 2005* (Cth) inserts provisions into the *Criminal Code* (Cth) stating that a person commits any of the offences mentioned above (except for the offence of engaging in a terrorist act) even if:

- a terrorist act does not in fact occur;<sup>179</sup> or
- the training, thing, document or act (as the case may be) is not referable to a *specific* terrorist act;<sup>180</sup> or
- the training, thing, document or act (as the case may be) is referable to more than one terrorist act.<sup>181</sup>

Very recently, a new s 106.3 of the *Criminal Code* (Cth) was proclaimed to come into effect. The Explanatory Statement that accompanied the Proclamation states, inter alia, that:

<sup>174</sup> Sections 101.4 and 101.5.

<sup>175</sup> Sections 101.4(5) and 101.5(5).

<sup>176</sup> Section 101.6.

<sup>177</sup> Section 103.1.

<sup>178</sup> Section 103.2. Commenced 15/12/05. Inserted by *Anti-terrorism Act (No 2) 2005* (Cth).

<sup>179</sup> Sections 101.2(3)(a), 101.4(3)(a), 101.5(3)(a) and 101.6(2)(a).

<sup>180</sup> Sections 101.2(3)(b), 101.4(3)(b), 101.5(3)(b) and 101.6(2)(b).

<sup>181</sup> Sections 101.2(3)(c), 101.4(3)(c), 101.5(3)(c) and 101.6(2)(c).



*The purpose of the Proclamation is to fix 16 February 2006 as the day on which Item 22 of Schedule 1 to the Act commences.*

*Item 22 of Schedule 1 of the Anti-Terrorism Act (No. 2) 2005 inserts a new section 106.3 into the Criminal Code Act 1995 and provides that the amendments made by Schedule 1 to the Anti-Terrorism Act 2005 apply to offences committed whether before or after the commencement of the section.*

*Schedule 1 to the Anti-Terrorism Act 2005 amends subsections 101.2(3), 101.4(3), 101.5(3), 101.6(2) and 103.1(2) of the Criminal Code Act to clarify that, in a prosecution for a terrorism offence, it is not necessary to identify a particular terrorist act. The amendments make it sufficient for the prosecution to prove that the particular conduct was related to 'a' terrorist act, instead of 'the' terrorist act.*

*No consultation was undertaken in relation to the Proclamation.*

Section 106.3 of the *Criminal Code* (Cth) provides that:

*The amendments to this Code made by Schedule 1 to the Anti-Terrorism Act 2005 apply to offences committed:*

*(a) before the commencement of this section (but not before the commencement of the particular section of the Code being amended); and*

*(b) after the commencement of this section.*

It is interesting to note that the matters to which s 106.3 relate are presently being considered in the *Lodhi* proceedings.

### **3.2.3 Case study of preparatory offences: *R v Faheem Khalid Lodhi* (unreported, NSWSC, 23 December 2005)**

In the recent case of *R v Faheem Khalid Lodhi* (unreported, NSWSC, 23 December 2005), it was contended by the Crown and accepted by Whealy J that even prior to the amendments by the *Anti-terrorism Act 2005* (Cth) it was not necessary to prove, in relation to the preparatory offences mentioned above, that the accused had a specific or ultimate target in mind. Whealy J said at [52];

*in my opinion, an offence will have been committed by a person acting in a preliminary way in preparation for a terrorist act even where no final decision has been made finally as to the ultimate target. I cannot accept Mr Boulton's argument [for the accused] that there needs to be a 'different mens rea to bomb position X than to bomb position Y.'*

This analysis recognises that preparatory offences are designed so that “the criminal offence will or may occur long before any terrorist act itself is carried out,”<sup>182</sup> the idea being that it is desirable to avoid a situation where “cities would be bombed and scores of people killed before the legislation would have the capacity to bite.”<sup>183</sup> The definition of a terrorist act must, “as a matter of logic and common sense,”<sup>184</sup> be construed so as to encompass the wide array of activities that might be considered to be preparatory to a terrorist act.<sup>185</sup> Whealy J gives an example of a person who packs the bags of a suicide bomber with explosives, knowing that the bomber will detonate the explosives in either the Queen Victoria Building or the Dymocks Book Store in George Street (but not knowing which building will ultimately be bombed). Such a person would be guilty of an offence even if the terrorist act does not occur and notwithstanding that the ultimate target has not been finally determined.<sup>186</sup>

With respect to offences that proscribe conduct that is preparatory to a terrorist act, it is not necessary to prove that the accused held the intentions mentioned in subsections (b) and (c) of the definition of a terrorist act.<sup>187</sup> This is because the accused may have no personal interest in carrying out the terrorist act. “He might, for example, simply be a paid mercenary. He might simply be doing a favour for a friend or repaying a debt.”<sup>188</sup> The requisite intention that an accused must have under s 101.4(1), for instance, is an intention to possess the thing, and knowledge that the thing is connected with the preparation for a terrorist act.<sup>189</sup> The Crown does not have to prove that the accused did the act of preparation with the intention of coercing a nominated government, intimidating the public or a section thereof, or with the intention of advancing a political, religious or ideological cause.

### **3.3 Terrorist Organisations**

#### **3.3.1 Offences Relating to Involvement with the Activities of a Terrorist Organisation**

It is an offence for a person to:

- intentionally direct the activities of a terrorist organisation when the person knows that (25 years imprisonment), or is reckless as to whether (15 years imprisonment), the organisation is a terrorist organisation;<sup>190</sup>
- intentionally be a member of an organisation that a person knows to be a terrorist organisation, unless the person can prove on the balance of probabilities that they took all reasonable steps to cease to be a member as soon as practicable after the person knew that the organisation was a terrorist organisation<sup>191</sup> (punishable by 10 years imprisonment). The term

<sup>182</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 23 December 2005) (Whealy J) at [46].

<sup>183</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 23 December 2005) (Whealy J) at [47].

<sup>184</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 23 December 2005) (Whealy J) at [47].

<sup>185</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 23 December 2005) (Whealy J) at [47].

<sup>186</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 23 December 2005) (Whealy J) at [55].

<sup>187</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 14 February 2006) (Whealy J) at [103].

<sup>188</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 14 February 2006) (Whealy J) at [88].

<sup>189</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 14 February 2006) (Whealy J) at [81-88].

<sup>190</sup> *Criminal Code* (Cth), s 102.2.

<sup>191</sup> *Criminal Code* (Cth), s 102.3.

“member” includes “informal” members as well as a person who has taken steps to become a member.<sup>192</sup> An identical crime has been created under s 310J of the *Crimes Act 1900* (NSW);

- intentionally recruit a person to join, or participate in the activities of, a terrorist organisation<sup>193</sup> when the person knows that (25 years imprisonment), or is reckless as to whether (15 years imprisonment), the organisation is a terrorist organisation. The term “recruiting” includes inducing, inciting and encouraging;<sup>194</sup>
- intentionally receive funds from, or make funds available to, a terrorist organisation (whether directly or indirectly), or intentionally collecting funds for or on behalf of a terrorist organisation (whether directly or indirectly) when the person knows that (25 years imprisonment), or is reckless as to whether (15 years imprisonment), the organisation is a terrorist organisation;<sup>195</sup>
- intentionally provide support or resources to a terrorist organisation that would help the organisation engage in an activity described in paragraph (a) of the definition of terrorist organisation when the person knows that (25 years imprisonment), or is reckless as to whether (15 years imprisonment), the organisation is a terrorist organisation;<sup>196</sup> or
- intentionally provide training to, or receive training from, a terrorist organisation where the person is reckless as to whether or not the organisation is a terrorist organisation (punishable by 25 years incarceration).<sup>197</sup> Where the organisation is alleged to be a terrorist organisation by reason of para (a) of the definition of a “terrorist organisation,” the Crown must establish that the accused was reckless as to whether the organisation “was directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act being the action or threat of action that the Crown relies on to prove the fact that [the organisation] was a terrorist organisation at the material time.”<sup>198</sup> If the organisation is a terrorist organisation specified by the Governor-General under para (b) of the definition of a “terrorist organisation” and the accused is charged under s 102.5(2) rather than s 102.5(1), then the accused bears the evidential burden in relation to whether or not he or she was reckless as to whether the organisation was a terrorist organisation<sup>199</sup> (i.e. the accused must adduce or point to evidence that suggests a reasonable possibility that he or she was not in fact reckless<sup>200</sup>).

---

<sup>192</sup> *Criminal Code* (Cth), s 102.1(1).

<sup>193</sup> *Criminal Code* (Cth), s 102.4.

<sup>194</sup> *Criminal Code* (Cth), s 102.1(1).

<sup>195</sup> *Criminal Code* (Cth), s 102.6.

<sup>196</sup> *Criminal Code* (Cth), s 102.7.

<sup>197</sup> *Criminal Code* (Cth), s 102.5(1).

<sup>198</sup> *R v Izhhar Ul-Haque* (unreported, NSWSC, 8 February 2006) (Bell J) at [56]. Note that this case deals with the training offence as it stood in January 2003. The reasoning applied by Bell J is nevertheless applicable to the offence as it now stands.

<sup>199</sup> *Criminal Code* (Cth), s 102.5(2).

<sup>200</sup> *Criminal Code* (Cth), s 13.3(6).

### 3.3.2 Intentionally associating with terrorist organisation members

The *Criminal Code* (Cth) also creates offences (punishable by three years imprisonment) relating to intentionally associating with a member of a terrorist organisation that has been specified by the Governor-General. A person commits an offence if:

(a) on 2 or more occasions:

(i) the person intentionally associates [note that “a person associates with another person if the person meets or communicates with the other person”<sup>201</sup>] with another person who is a member of, or a person who promotes or directs the activities of, an organisation; and

(ii) the person knows that the organisation is a terrorist organisation; and

(iii) the association provides support to the organisation; and

(iv) the person intends that the support assist the organisation to expand or to continue to exist; and

(v) the person knows that the other person is a member of, or a person who promotes or directs the activities of, the organisation; and

(b) the organisation is a terrorist organisation because of paragraph (b) of the definition of terrorist organisation in this Division (whether or not the organisation is a terrorist organisation because of paragraph (a) of that definition also).<sup>202</sup>

It is also an offence if a person who has been convicted of the above offence at a later time (even if only on one occasion) satisfies all the elements listed in (a) and (b) above.<sup>203</sup> There are notable qualifications to the operation of these provisions:

- A person who is convicted for this offence cannot be convicted of the same offence in relation to conduct that takes place at the same time as the conduct that forms the basis of the conviction, or for conduct that occurs 7 days before or after the occasions relied upon to prove the offence;<sup>204</sup>
- A person is not guilty of an association offence if the person was not reckless as to whether or not the organisation was in fact an organisation specified by the Governor-General, but the accused bears an evidential burden in relation to such a lack of recklessness.<sup>205</sup>

<sup>201</sup> *Criminal Code* (Cth), s 101.1(1).

<sup>202</sup> *Criminal Code* (Cth), s 102.8(1).

<sup>203</sup> *Criminal Code* (Cth), s 102.8(2).

<sup>204</sup> *Criminal Code* (Cth), s 102.8(7).

<sup>205</sup> *Criminal Code* (Cth), s 102.8(5).

- The section creating the association offences “does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication;”<sup>206</sup> and,
- An association offence does not occur if:

*a) the association is with a close family member and relates only to a matter that could reasonably be regarded (taking into account the person's cultural background) as a matter of family or domestic concern; or*

*(b) the association is in a place being used for public religious worship and takes place in the course of practising a religion; or*

*(c) the association is only for the purpose of providing aid of a humanitarian nature; or*

*(d) the association is only for the purpose of providing legal advice or legal representation in connection with [various legal proceedings].<sup>207</sup>*

### 3.3.3 Potential Problems with the Terrorist Organisation Provisions

It has been argued that there are several potential problems with the terrorist organisation provisions. One possible problem that has been ventilated in the literature is that, because of the breadth of the definition of a terrorist act, the range of organisations that are liable to be specified as terrorist organisations is perhaps too wide. One commentator has suggested, for instance, that

*any organisation that offers support to political protesters who clash with police is liable to be banned [as a terrorist organisation], on the grounds that it is directly fostering politically motivated activity which is intended to intimidate a government, and which is both intended to, and does, create a serious risk to the health and safety of a section of the public (by provoking the police to attack them).<sup>208</sup>*

The same commentator argues, in relation to the training offence in s 102.5(2), that the *Criminal Code Act 1995* (Cth) “clearly permits arbitrary imprisonment.”<sup>209</sup> Without coming to a conclusion as to the correctness of this view, the steps of reasoning that are put forward to justify this position are as follows.<sup>210</sup> The first step is rather straightforward, and merely involves recognition that s 102.5(2) does not require proof that the accused themselves had any terrorist aims – it is sufficient that the accused intentionally trained with the organisation. The second step relies on the proposition that once a terrorist organisation is specified by the Governor-General, it is not necessary to prove that the organisation in fact had terrorist aims at the time the training took place. The third step involves an analysis of the effect of placing an

<sup>206</sup> *Criminal Code* (Cth), s 102.8(6).

<sup>207</sup> *Criminal Code* (Cth), s 102.8(4).

<sup>208</sup> Emerton, “Paving the Way” at 9.

<sup>209</sup> *Ibid*, at 13.

<sup>210</sup> The following is borrowed from: *Ibid*, especially at 1-14.

evidentiary burden on the accused in relation to showing his or her lack of recklessness in relation to whether or not the organisation was a specified organisation. In this regard it is notable that all of the terrorist organisations that have so far been banned are organisations that are based overseas.<sup>211</sup> Hence, if – as is likely – the acts complained of were committed overseas, the accused may face problems in adducing evidence, particularly from witnesses who may not wish to be identified and who may live thousands of miles away. If the accused cannot produce such witness – or any other cogent evidence – then the accused him or herself may be forced to give evidence, raising real issues about an accused’s right to silence. The effect of placing the evidential burden on the accused is that the Crown is excused from having to prove an element of the offence where the accused cannot point to evidence sufficient to raise a reasonable possibility that he or she was not reckless.<sup>212</sup> On the basis of this reasoning, Emerton concludes that

*by permitting conviction even though no evidence has been led that the accused had any criminal aims, no evidence has been led that the organisation with which he or she was involved had any criminal aims, and no evidence has been led that the accused knew, or was reckless as to the possibility that, involvement with the organisation was a criminal offence, the law clearly permits arbitrary imprisonment.*<sup>213</sup>

This argument may only have theoretical significance. It is hard to imagine a case where a person would innocently train with a specified terrorist organisation, given the notoriety of the organisations that are listed and the purposes for which they exist.

### 3.3.4 Extraterritorial operation of the terrorist organisation provisions

The extraterritorial operation of the terrorist organisation provisions can also give rise to difficult cases. Take for instance the offence of making funds available to a terrorist organisation where the person knows the organisation is a terrorist organisation (s 102.6(1) – note that there is no requirement that the terrorist organisation be a *specified* organisation). Hamas is an extremist terrorist organisation that is primarily active in Israel. Few people would dispute that Hamas (which is Arabic for “zeal” and an acronym for the Islamic Resistance Movement that grew out of the Intifada in 1987<sup>214</sup>) falls within the popular notion of what would constitute a terrorist organisation. Hamas’ military wing, the al-Qassam Brigades, is a terrorist organisation that has been specified by the Governor-General.<sup>215</sup> However it has been suggested that “much of the budget of Hamas (estimated in 1995 at \$70 million) [is spent] for legitimate religious and social purposes,”<sup>216</sup> such as “social

---

<sup>211</sup> *Criminal Code Regulations 2002* (Cth). Section 100.1 of the *Criminal Code Act 1995* (Cth) provides that an organisation means a body corporate or unincorporated body, whether or not the body is based outside of Australia, consists of persons who are not Australian citizens, or is part of a larger organisation.

<sup>212</sup> *Criminal Code Act 1995* (Cth), s 13.3(6).

<sup>213</sup> Emerton, “Paving the Way” at 13.

<sup>214</sup> I. J Bickerton and C. L. Klausner, *A Concise History of the Arab-Israeli Conflict*, 4<sup>th</sup> Ed, Prentice Hall, New Jersey, 2002 (hereafter *History of the Arab-Israeli Conflict*), p. 362.

<sup>215</sup> *Criminal Code Regulations 2002* (Cth), s 4U.

<sup>216</sup> Bickerton and Klausner, *History of the Arab-Israeli Conflict*, p. 289.

services, free schools and clinics”<sup>217</sup> for Palestinians. This does not change the fact that Hamas routinely employs terrorist tactics, nor that its institutions are “sometimes a cover and recruiting ground for young terrorists,”<sup>218</sup> but it does raise some problems in relation to the application of the terrorist organisation provisions. Suppose that a Palestinian woman and her children flee from Israel to Australia hoping to start a new life. Suppose that whilst still in Israel, the woman’s children attended a free school run by Hamas, and that they received a legitimate education there. If, just prior to leaving, the woman gave a donation to the organisation running the school (i.e. Hamas, an organisation that she knows is involved in terrorist acts, amongst other things) in gratitude for educating her children, then it is possible that on settling in Australia she will be convicted of making funds available to a terrorist organisation and sentenced to 25 years in prison. Moreover, her and her children might be sentenced to 3 years in prison for associating with the teachers at their former school (who happened to be members of Hamas). Even worse, the woman’s eldest son might be sentenced to 25 years imprisonment for training with a terrorist organisation, because even though he had no desire to be a terrorist, it was a condition of his education in later years that he attend certain training exercises. It can be seen from the above that the extraterritorial application of the terrorist organisation provisions could have wide and unexpected consequences.

### **3.4 Harming Australians**

Division 115 of the *Criminal Code* (Cth) (“Harming Australians”) is not in its terms directed specifically against terrorists. Nevertheless, the second reading speech to the *Criminal Code Amendment (Offences Against Australians) Bill 2002* (Cth) (which inserted Division 115), delivered on 12 November 2002 in the House of Representatives, makes it abundantly clear that the terrorist threat was the prime motivation for the provisions. The Minister’s speech (at p. 8797) began as follows:

*The terrorist attacks of September 11 in the United States marked a fundamental shift in the world’s security environment. The tragic events in Bali brought the reality of this threat closer to home in a direct and horrific way.*

*Australia is committed to the war against terrorism...*

After some further remarks in a similar vein, the Minister continued (at p. 8798):

*In response to the Bali attacks the Howard Government is reviewing current arrangements to identify any possible action to strengthen our counter-terrorism capabilities still further.*

*As a result of that review the government announced that it would enact, as a matter of urgency, new legislation outlawing the murder of Australians abroad.*

---

<sup>217</sup> Ibid, p. 319.

<sup>218</sup> Ibid, p. 289.

Division 115 creates offences against murdering,<sup>219</sup> manslaughtering,<sup>220</sup> intentionally causing serious harm,<sup>221</sup> or recklessly causing serious harm<sup>222</sup> to an Australian citizen or permanent resident who is outside Australia. The offences are punishable by life, 25 years, 20 years and 15 years imprisonment, respectively. In essence, these provisions could be described as catch-all offences designed to cover situations that fall through the cracks of the specific terrorism provisions.

### **3.5 Hoaxes and Other Offences Using Postal or Carriage Services**

The *Criminal Code Amendment (Anti-hoax and Other Measures) Act 2002* (Cth) and the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No 2) 2004* (Cth) inserted anti-hoax provisions into the *Criminal Code* (Cth). The Acts created the following offences:

- It is now punishable by up to 10 years imprisonment to make bomb hoaxes<sup>223</sup> and threats<sup>224</sup> through a postal service (which includes, inter alia, a courier service<sup>225</sup>) or a telecommunications carriage service;
- It is an offence punishable by 2 years imprisonment (in the case of a postal service) or 3 years imprisonment (in the case of a carriage service) to use a postal service or a carriage service in a way that would be regarded by reasonable persons as being menacing, harassing or offensive;<sup>226</sup>
- It is an offence (punishable by 10 years imprisonment) to cause an explosive to be carried by post;<sup>227</sup> and
- It is also an offence for a person to cause an article to be carried by a postal or similar service in a way that gives rise to a danger of death or serious harm to another person, where the first-mentioned person is reckless as to the danger of death or serious harm (10 years imprisonment).<sup>228</sup>

In relation to the last offence mentioned above, conduct giving rise to a danger of death or serious harm is conduct that is ordinarily capable of creating a real and not merely a theoretical danger of death or serious harm, regardless of any statistical calculation of the degree of risk involved.<sup>229</sup> Such a danger will also be taken to arise if the conduct exposes a person to the risk of catching a disease that may give rise to death or serious harm. It is not necessary to show that a person was actually placed in danger of death or serious harm to make out the offence.<sup>230</sup>

---

<sup>219</sup> *Criminal Code* (Cth), s 115.1.

<sup>220</sup> *Criminal Code* (Cth), s 115.2.

<sup>221</sup> *Criminal Code* (Cth), s 115.3.

<sup>222</sup> *Criminal Code* (Cth), s 115.4.

<sup>223</sup> *Criminal Code* (Cth), s 471.10 (postal service) and s 474.16 (carriage service).

<sup>224</sup> *Criminal Code* (Cth), s 471.11 (postal service) and s 474.15 (carriage service).

<sup>225</sup> *Criminal Code* (Cth), s 470.1.

<sup>226</sup> *Criminal Code* (Cth), s 471.12 (Postal service) and s 474.17 (carriage service).

<sup>227</sup> *Criminal Code* (Cth), s 471.15(1). That section also makes it an offence to post a dangerous or harmful substance or thing proscribed by the regulations.

<sup>228</sup> *Criminal Code* (Cth), s 471.13(1).

<sup>229</sup> *Criminal Code* (Cth), s 471.13(3)-(4).

<sup>230</sup> *Criminal Code* (Cth), s 471.13(5).



### **3.6 International Terrorism**

Division 72 of the *Criminal Code* (Cth) (“International terrorist activities using explosive or lethal devices”) was inserted by the *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* (Cth). Section 72.1 recites that the Division was enacted to give effect to the *International Convention for the Suppression of Terrorist Bombings* (done at New York, 15 December 1997).<sup>231</sup> For the Division to apply, the acts in question must have an Australian *and* an international link;<sup>232</sup> the Division has no operation where the alleged offences are exclusively internal to Australia.<sup>233</sup> The Division sets out two offences punishable by imprisonment for life. Section 72.3(1) provides that

*a person commits an offence if:*

*(a) the person intentionally delivers, places, discharges or detonates a device; and*

*(b) the device is an explosive or other lethal device and the person is reckless as to that fact; and*

*(c) the device is delivered, placed, discharged, or detonated, to, in, into or against:*

*(i) a place of public use; or*

*(ii) a government facility; or*

*(iii) a public transportation system; or*

*(iv) an infrastructure facility; and*

*(d) the person intends to cause death or serious harm.*

Section 72.3(2) is in precisely the same terms until subs (d). From (d) onwards, s 72.3(2) reads:

*(d) the person intends to cause extensive destruction to the place, facility or system; and*

*(e) the person is reckless as to whether that intended destruction results in or is likely to result in major economic loss.*

### **3.7 Financing Terrorism: Freezable Assets**

The *Suppression of the Financing of Terrorism Act 2002* (Cth) inserted provisions creating terrorism offences into the *Charter of the United Nations Act 1945* (Cth)

---

<sup>231</sup> *Criminal Code* (Cth), s 72.1.

<sup>232</sup> *Criminal Code* (Cth), s 72.4(1).

<sup>233</sup> *Criminal Code* (Cth), s 72.4. Note that the *Crimes (Hostages) Act 1989* (Cth) has a provision to the similar effect (s 9(2) and s 9(4)).

("Part 4 – Offences to give effect to Security Council decisions"). Unless authorised under s 22, it is an offence punishable by 5 years imprisonment to directly or indirectly make an asset available to a proscribed person or entity (i.e. the Taliban, Osama bin Laden, a member of al-Qaeda, or a person or entity named in the list of the Committee established under para 6 of UN Resolution 1267).<sup>234</sup> A freezable asset is defined as an asset that:

(a) is owned or controlled by a proscribed person or entity; or,

(b) is a listed asset; or

(c) is derived or generated from assets mentioned in paragraph (a) or (b).<sup>235</sup>

The Minister may list an asset or class of asset if the Minister is satisfied that the asset is owned or controlled by persons:

- "who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts," or
- by entities owned or controlled directly or indirectly by such persons, or by persons and entities acting on their behalf, or
- at the direction, of such persons or entities.<sup>236</sup>

Unless authorised under s 22, it is an offence punishable by 5 years imprisonment for a person to hold a freezable asset that the person uses, deals with, allows to be used or dealt with, or facilitates the using or dealing with that asset.<sup>237</sup> An owner of an asset that is wrongly frozen is entitled to compensation for any loss caused thereby,<sup>238</sup> and a person who freezes an asset will not be liable for doing so if the asset was frozen in good faith and without negligence.<sup>239</sup> An injunction may be granted restraining conduct involving a contravention of Pt 4.<sup>240</sup>

### **3.8 Espionage and Related Activities**

Division 91 of the *Criminal Code* (Cth) ("Offences relating to espionage and related activities") was inserted in 2002.<sup>241</sup> Like the offences of treason and sedition in Division 80 of the *Criminal Code* (Cth), as well as the offences of treachery and sabotage under ss 24AA and 24AB of the *Crimes Act 1914*, espionage offences under Div 91 (and related offences under s 79 of the *Crimes Act 1914* (Cth)) are not triable summarily.<sup>242</sup>

The offences under s 91.1 of Div 91 involve information that is:

---

<sup>234</sup> *Charter of the United Nations Act 1945* (Cth), s 21; *Charter of the United Nations (Terrorism and Dealings with Assets) Regulations 2002* (Cth), reg 6A.

<sup>235</sup> *Charter of the United Nations Act 1945* (Cth), s 14.

<sup>236</sup> *Charter of the United Nations Act 1945* (Cth), s 15; *Charter of the United Nations (Terrorism and Dealings with Assets) Regulations 2002* (Cth), reg 6.

<sup>237</sup> *Charter of the United Nations Act 1945* (Cth), s 20.

<sup>238</sup> *Charter of the United Nations Act 1945* (Cth), s 25.

<sup>239</sup> *Charter of the United Nations Act 1945* (Cth), s 24.

<sup>240</sup> *Charter of the United Nations Act 1945* (Cth), s 26.

<sup>241</sup> *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth).

<sup>242</sup> *Crimes Act 1914* (Cth), s 4J(7).

(i) *information concerning the Commonwealth's security or defence; or*

(ii) *information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth.*<sup>243</sup>

It is an offence punishable by 25 years imprisonment for a person to communicate or make available such information where:

- the person intends to prejudice the Commonwealth's security or defence; or
- the person does so without lawful authority and intends to give an advantage to another country's security or defence; and

the act results in, or is likely to result in, the information being communicated or made available to another country or foreign organisation or a person acting on their behalf.<sup>244</sup>

It is also an offence punishable by 25 years imprisonment for a person to make, obtain or copy a record (in any form) of such information where:

- the person intends to prejudice the Commonwealth's security or defence; or
- the person does so without lawful authority and intends to give an advantage to another country's security or defence; and

the person does so intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on their behalf (even if the person does not have a particular country, foreign organisation or person in mind at the time).<sup>245</sup>

It is a defence to any offence under s 91.1 if the information has already been communicated or made available to the public with the authority of the Commonwealth.<sup>246</sup>

If the person presiding over proceedings for an offence under s 91.1 is satisfied that it is in the interests of the security or defence of the Commonwealth, he or she may make orders providing for a hearing in camera, restricted access to documents etc.<sup>247</sup> It is an offence to contravene such an order.<sup>248</sup>

### **3.9 Offences Relating to Foreign Travel Documents**

---

<sup>243</sup> See, eg, *Criminal Code* (Cth), s 91.1(1)(a).

<sup>244</sup> *Criminal Code* (Cth), ss 91.1(1) and (2).

<sup>245</sup> *Criminal Code* (Cth), ss 91.1(3), (4) and (5).

<sup>246</sup> *Criminal Code* (Cth), s 91.2.

<sup>247</sup> *Criminal Code* (Cth), s 93.2(2).

<sup>248</sup> *Criminal Code* (Cth), s 93.2(3). Punishable by 2 years imprisonment.

New offences have been inserted into the *Passports Act 1938* (Cth) by the *Anti-Terrorism Act (No 3) 2004* (Cth). Several offences, each punishable by 10 years imprisonment or 1,000 penalty units or both, have been created in relation to foreign travel documents.<sup>249</sup> The offences relate to:

- making false or misleading statements, giving false or misleading information or producing false or misleading documents in connection with an application for a “foreign travel document”<sup>250</sup> (which includes a foreign passport),<sup>251</sup>
- misuse of a foreign travel document;<sup>252</sup> and
- possessing, controlling, making or providing a false foreign travel document.<sup>253</sup>

New provisions in the *Passports Act 1938* (Cth) also provide for the Minister to demand that a person surrender their foreign travel documents in certain circumstances.<sup>254</sup>

### **3.10 Aviation Offences**

The *Aviation Transport Security Act 2004* (Cth) was enacted primarily to provide “a regulatory framework to safeguard against unlawful interference with aviation.”<sup>255</sup> The Act is predominantly directed at “aviation industry participants” (which includes aircraft operators, airport operators, and the like<sup>256</sup>) but it does create some offences that apply to the public generally. The most significant of these offences relate to the possession of weapons and prohibited items (a prohibited item is an item that could be used for unlawful interference with aviation and that is prescribed by the regulations<sup>257</sup>). It is an offence for an unauthorised person to:

- Possess a weapon in an airside area or a landside security area in a security controlled airport;<sup>258</sup> or
- Possess a prohibited item in an airside area or a landside security area in a security controlled airport.<sup>259</sup>

Security controlled airports are declared by the Secretary of the Department by notice published in the *Gazette*.<sup>260</sup> Such a notice must establish an airside area within the airport (the purpose of which is to control access to operational areas).<sup>261</sup> Landside areas are any areas within the airport that are not airside areas.<sup>262</sup> Landside security areas can be established by the Secretary giving a written notice

---

<sup>249</sup> *Passports Act 1938* (Cth), Pt 3.

<sup>250</sup> *Passports Act 1938* (Cth), ss 18-20.

<sup>251</sup> *Passports Act 1938* (Cth), s 5(1).

<sup>252</sup> *Passports Act 1938* (Cth), s 21.

<sup>253</sup> *Passports Act 1938* (Cth), s 22.

<sup>254</sup> *Passports Act 1938* (Cth), Pt 2.

<sup>255</sup> *Aviation Transport Security Act 2004* (Cth), s 3(1).

<sup>256</sup> *Aviation Transport Security Act 2004* (Cth), s 9.

<sup>257</sup> *Aviation Transport Security Act 2004* (Cth), s 9.

<sup>258</sup> *Aviation Transport Security Act 2004* (Cth), s 46.

<sup>259</sup> *Aviation Transport Security Act 2004* (Cth), s 54.

<sup>260</sup> *Aviation Transport Security Act 2004* (Cth), s 28.

<sup>261</sup> *Aviation Transport Security Act 2004* (Cth), s 29.

<sup>262</sup> *Aviation Transport Security Act 2004* (Cth), s 29(3).

to the operator of a security controlled airport.<sup>263</sup> The purpose of such an area is to allow stricter controls than in landside areas generally.<sup>264</sup>

It is also an offence to:

- Carry a weapon<sup>265</sup> or prohibited item<sup>266</sup> through a screening point; or
- Carry a weapon or prohibited item on an aircraft, or otherwise have possession of a weapon or prohibited item that is located in a place that is accessible.<sup>267</sup>

All of the offences detailed above may be charged as either a standard offence or as a strict liability offence. Strict liability offences are punishable by 100 penalty units where the offence involves a weapon, or 20 units where the offence involves a prohibited item. Standard offences are subject to a maximum penalty of 7 years imprisonment for weapons offences, or 2 years for prohibited item offences.

### **3.11 Sedition**

The Commonwealth recently enacted new offences in relation to sedition. These provisions were inserted into the *Criminal Code* (Cth) by the *Anti-terrorism Act (No 2) 2005* (Cth), and commenced on the eleventh of January this year. Several offences are created, each punishable by 7 years imprisonment. It is an offence to:

- urge another person to overthrow by force or violence the Constitution, a Commonwealth, State or Territory government, or a lawful authority of the government of the Commonwealth;<sup>268</sup>
- urge interference by force or violence in the lawful processes of an election;<sup>269</sup>
- urge a person to assist an organisation or country at war with the Commonwealth or that is specified by proclamation to be at war with the Commonwealth;<sup>270</sup> and
- urge a person to engage in conduct that assists an organisation or country that is engaged in armed hostilities against the Australian Defence Force.<sup>271</sup>

Section 80.2(5) is slightly different. It provides that:

*(5) A person commits an offence if:*

---

<sup>263</sup> *Aviation Transport Security Act 2004* (Cth), ss 32(1)-(2).

<sup>264</sup> *Aviation Transport Security Act 2004* (Cth), s 32(3).

<sup>265</sup> *Aviation Transport Security Act 2004* (Cth), 47.

<sup>266</sup> *Aviation Transport Security Act 2004* (Cth), s 55.

<sup>267</sup> *Aviation Transport Security Act 2004* (Cth), ss 48, 49, 56, 57.

<sup>268</sup> *Criminal Code* (Cth), s 80.2(1).

<sup>269</sup> *Criminal Code* (Cth), s 80.2(3).

<sup>270</sup> *Criminal Code* (Cth), s 80.2(7).

<sup>271</sup> *Criminal Code* (Cth), s 80.2(8).

*(a) the person urges a group or groups (whether distinguished by race, religion, nationality or political opinion) to use force or violence against another group or other groups (as so distinguished); and*

*(b) the use of the force or violence would threaten the peace, order or good government of the Commonwealth...*

*(6) Recklessness applies to the element of the offence under subsection (5) that it is a group or groups that are distinguished by race, religion, nationality or political opinion that the first-mentioned person urges the other person to use force or violence against.*

Sections 80.1(2) and (4) contain similar recklessness provisions in relation to the offences of urging the overthrow of the Constitution (etc) and urging interference in elections. It should be noted that the terms of s 80.2(5) may make it possible for speeches made by extremist religious leaders to be interpreted as a criminal offence. Since the offence is a category D offence, it might also apply to visiting public figures who have made inflammatory speeches in other countries. However, potentially seditious acts that are done in good faith may attract the defence in s 80.3.

## Chapter 4: Terrorist Offences and the Criminal Charge and Trial Process

### **4.1 Detention after Arrest**

Both the Commonwealth and NSW have enacted legislation that authorises the detention of a person who is under arrest so that an investigating official can question them.<sup>272</sup> A person may only be so detained for 4 hours,<sup>273</sup> unless a detention warrant is obtained from an “authorised officer” under the NSW Act (see above) or a “judicial officer” (i.e. a magistrate, a bail justice or a justice of the peace<sup>274</sup>) under the Commonwealth Act. Such an officer may issue a warrant extending the investigation period by up to 8 hours.<sup>275</sup> Under the NSW Act, an authorised officer must not issue a detention warrant unless satisfied that:

- (a) the investigation is being conducted diligently and without delay, and*
- (b) a further period of detention of the person...is reasonably necessary to complete the investigation, and*
- (c) there is no reasonable alternative means of completing the investigation otherwise than by the continued detention of the person, and*
- (d) circumstances exist in the matter that make it impracticable for the investigation to be completed within the 4-hour period.<sup>276</sup>*

The Commonwealth Act provides that a judicial officer may issue a detention warrant if satisfied that:

- (a) the offence is a serious offence [i.e. punishable by 12 months or more in prison<sup>277</sup>]; and*
- (b) further detention of the person is necessary to preserve or obtain evidence or to complete the investigation into the offence or into another serious offence; and*
- (c) the investigation into the offence is being conducted properly and without delay; and*

---

<sup>272</sup> Crimes Act 1914 (Cth), Pt IC, Div 2; Law Enforcement (Powers and Responsibilities) Act 2002 (NSW), Pt 9.

<sup>273</sup> Crimes Act 1914 (Cth), s 23C(4) (2 hours in the case of Aboriginals or Torres Strait Islanders); Law Enforcement (Powers and Responsibilities) Act 2002 (NSW), s 115.

<sup>274</sup> Crimes Act 1914 (Cth), s 23D(2).

<sup>275</sup> Crimes Act 1914 (Cth), s 23D(5); Law Enforcement (Powers and Responsibilities) Act 2002 (NSW), s 118(3).

<sup>276</sup> Law Enforcement (Powers and Responsibilities) Act 2002 (NSW), s 118(5).

<sup>277</sup> Crimes Act 1914 (Cth), s 23D(6).

*(d) the person, or his or her legal representative, has been given the opportunity to make representations about the application.*<sup>278</sup>

#### **4.1.1 Detention Warrants in respect of Terrorist Offences – Commonwealth**

Since 2004, the *Crimes Act 1914* (Cth) has made a distinction between detention warrants issued in respect of terrorism offences and those issued in respect of all other offences.<sup>279</sup> When a person is arrested for a terrorism offence<sup>280</sup> the investigation period is 4 hours, which commences when the person is arrested.<sup>281</sup> This is the same as for normal crimes. What is different to the case of other offences is how those 4 hours are calculated.

#### **4.1.2 Calculation of the Detention Period – Commonwealth Detention Warrants**

Section 23CA(8) sets out a list of times that are to be disregarded when calculating the investigation period. It is the same in every respect to the times to be disregarded for other offences, except for subsection (m), which has no equivalent.

**Subsection (m)** provides that any reasonable time in which the questioning is reasonably suspended or delayed and that is within the period specified in s 23CB is not to be regarded when calculating the investigation period.

**Section 23CB** provides that an investigating official may apply for a period to be specified by a judicial officer (see above) for the purpose of s 23CA(8)(m) at or before the end of the investigation period.<sup>282</sup> The application must include, inter alia, the reasons why the official believes the period should be specified, and how long the official believes that period should be.<sup>283</sup> The “judicial officer” may, by instrument, specify a period if satisfied that:

*(a) it is appropriate having regard to:*

*(i) the application; and*

*(ii) the representation (if any) made by the person, or his or her legal representative, about the application; and*

*(iii) any other relevant matters; and*

*(b) the offence is a terrorism offence; and*

*(c) detention of the person is necessary to preserve or obtain evidence or to complete the investigation into the offence or into another terrorism offence; and*

---

<sup>278</sup> *Crimes Act 1914* (Cth), s 23D(4).

<sup>279</sup> *Anti-terrorism Act (No 1) 2004* (Cth).

<sup>280</sup> I.e. an offence against Div 72 or Pt 5.3 of the *Criminal Code* (Cth): *Crimes Act 1914* (Cth), s 3.

<sup>281</sup> *Crimes Act 1914* (Cth), s 23CA(4).

<sup>282</sup> *Crimes Act 1914* (Cth), s 23CB(2).

<sup>283</sup> *Crimes Act 1914* (Cth), s 23CB(5).



(d) the investigation of the offence is being conducted properly and without delay; and

(e) the person, or his or her legal representative, has been given the opportunity to make representations about the application.<sup>284</sup>

The instrument must specify the period as a number of hours, set out the time and date when it was signed, as well as set out the reasons for specifying the period.<sup>285</sup> Somewhat remarkably, there is no precise limit to how long a specified period may be. The only limit appears to be that of reasonableness.<sup>286</sup>

### 4.1.3 Issuing Commonwealth Detention Warrants

A detention warrant may extend the investigation period by up to 20 hours in respect of a terrorist offence<sup>287</sup> (as opposed to 8 hours for a normal offence). A judicial officer (i.e. a magistrate, a bail justice or a justice of the peace<sup>288</sup>) may issue such a warrant if satisfied of the same matters that must be satisfied for a non-terrorism offence, except that references to a “serious offence” in s 23D(4) are instead references to a “terrorism offence” in s 23DA(4). Just as is the case for applications for detention warrants in relation to conventional offences, applications for detention warrants in relation to terrorist offences must be made to a magistrate unless the application cannot be made at a time when a magistrate is available. If the application is made at such a time, it must be made to either a bail justice or to a justice of the peace employed in a State or Territory court. If none of the above-mentioned judicial officers are available, then the application may be made to a justice of the peace.<sup>289</sup>

### 4.2 Bail and Non-parole Periods

For terrorist offences there have been two crucial changes to the conventional bail process:

- The *Anti-terrorism Act 2004* (Cth) inserts provisions into the *Crimes Act 1914* (Cth) that prevent a bail authority from granting bail to a person charged with or convicted of an offence against Div 72 or Pt 5.3 of the *Criminal Code* (Cth) (other than an offence against s 102.8<sup>290</sup>) or other offences related to terrorism such as treason and treachery<sup>291</sup> unless the authority is satisfied that “exceptional circumstances exist to justify the bail;” and
- The *Bail Act 1978* (NSW) has also been amended so that there is a presumption against bail with respect to offences

<sup>284</sup> *Crimes Act 1914* (Cth), s 23CB(7).

<sup>285</sup> *Crimes Act 1914* (Cth), s 23CB(8).

<sup>286</sup> See *Crimes Act 1914* (Cth), s 23CA(8)(m).

<sup>287</sup> *Crimes Act 1914* (Cth), s 23DA(7).

<sup>288</sup> *Crimes Act 1914* (Cth), s 23DA(2).

<sup>289</sup> *Crimes Act 1914* (Cth), ss 23D(2) and 23DA(2).

<sup>290</sup> This exception was inserted by the *Anti-terrorism Act (No 2) 2004* (Cth).

<sup>291</sup> See *Crimes Act 1914* (Cth), s 15AA(2)(c) and (d).

against Divisions 101, 102 and 103 of the *Criminal Code* (Cth).

The *Anti-terrorism Act 2004* (Cth) contains provisions relating to a person who is convicted of a terrorism offence, an offence against s 24AA of the *Crimes Act 1914* (Cth) or an offence against Divs 80 or 91 of the *Criminal Code* (Cth). In such a case, the court must fix a single non-parole period of at least three-quarters of:

(a) *the sentence for the minimum non-parole offence; or*

(b) *if two or more sentences have been imposed on the person for minimum non-parole offences – the aggregate of those sentences.*

*The non-parole period is in respect of all federal sentences the person is to serve or complete.*<sup>292</sup>

### **4.3 Disclosure of National Security Information**

#### **4.3.1 Enactment and Objectives**

The *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) came into force on the eleventh of January this year. The effect of the Act is to “permit the prosecution and conviction of individuals on the basis of information which, for reasons of national security, is not itself tendered in evidence against them at trial.”<sup>293</sup> The object of the Act (which a Court is required to take into account when exercising powers and functions under the Act<sup>294</sup>) is stated in s 3 as being “to prevent the disclosure of information in federal criminal proceedings and civil proceedings where the disclosure is likely to prejudice national security, except to the extent that preventing the disclosure would seriously interfere with the administration of justice.”<sup>295</sup>

#### **4.3.2 Definitions**

“**National security**” is defined to mean “Australia’s defence, security, international relations or law enforcement interests.”<sup>296</sup> Relevantly, “security” is defined in the *ASIO Act 1979* (Cth) to mean:

(a) *the protection of, and of the people of, the Commonwealth and the several States and Territories from:*

(i) *espionage;*

(ii) *sabotage;*

<sup>292</sup> *Crimes Act 1914* (Cth), s 19AG(2).

<sup>293</sup> Emerton, “Paving the Way” at 15.

<sup>294</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 3(2).

<sup>295</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 3(1).

<sup>296</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 8.

- (iii) *politically motivated violence;*
- (iv) *promotion of communal violence;*
- (v) *attacks on Australia’s defence system; or*
- (vi) *acts of foreign interference;*

*whether directed from, or committed within, Australia or not; and*

- (b) *the carrying out of Australia’s responsibilities to any foreign country in relation to a matter mentioned in any of the [above subparagraphs].*<sup>297</sup>

“**Politically motivated violence**” is defined to include “acts that are terrorism offences”<sup>298</sup> (i.e. offences against Div 72 or Pt 5.3 of the *Criminal Code* (Cth)).

The provisions in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) that deal with civil proceedings were inserted by the *National Security Information Legislation Amendment Act 2005* (Cth). Those provisions are outside the scope of this paper. Here we will only deal with those aspects of the Act that deal with crime. The only criminal proceedings to which the Act applies are “federal criminal proceedings.”

A “**federal criminal proceeding**” is a proceeding in relation to the *Extradition Act 1988* (Cth), or “a criminal proceeding in any court exercising federal jurisdiction, where the offence or any of the offences concerned are against a law of the Commonwealth.”<sup>299</sup>

A “**criminal proceeding**” includes (inter alia) bail, committal, discovery, sentencing, appeal and certain judicial review proceedings.<sup>300</sup>

#### 4.3.3 Alteration to Criminal Procedure

If in a federal criminal proceeding the prosecutor or defendant knows or believes that he or she will disclose, or that one of their intended witnesses (either in giving evidence or by his or her mere presence) will disclose information and:

- the information relates to national security; or
- the disclosure may affect national security,

then the prosecutor or defendant must as soon as practicable give the Attorney-General notice of such knowledge or belief,<sup>301</sup> and advise the court that such notice has been given.<sup>302</sup> Where a witness is asked a question in federal criminal proceedings and the prosecutor or defendant knows or believes that the answer will

<sup>297</sup> *ASIO Act 1979* (Cth), s 4.

<sup>298</sup> *ASIO Act 1979* (Cth), s 4.

<sup>299</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 14.

<sup>300</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 13.

<sup>301</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 24(1).

<sup>302</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 24(3)

include information of the sort described above, then **the following steps should occur:**

- The prosecutor or defendant must advise the court of such knowledge or belief.<sup>303</sup>
- The court must then adjourn the proceeding and hold a closed hearing where the witness must give a written answer to the court.<sup>304</sup>
- The answer must be shown to the prosecutor,<sup>305</sup> who must give notice to the court and the Attorney-General if he or she knows or believes that the answer would contain information of the sort described above if given in evidence in the proceedings.<sup>306</sup>

In any case where the Attorney-General is notified, the court must adjourn the proceedings to await his or her response.<sup>307</sup> The Attorney-General may issue a “criminal non-disclosure certificate” or a “witness exclusion certificate” (or may refuse to issue a certificate at all, in which case he or she must advise the court of the decision<sup>308</sup>). When either a criminal non-disclosure certificate or a witness exclusion certificate has been issued the court must hold a closed hearing so as to make an order under s 31.<sup>309</sup>

#### 4.3.4 Disclosure certificates

##### 4.3.4.1 Documentary and other evidence

Where notice has been given to the Attorney-General, or the Attorney-General for any reason expects that information of the sort described above will be disclosed in a federal criminal proceeding,<sup>310</sup> a criminal non-disclosure certificate may be issued, but only if the disclosure is not constituted by the mere presence of a witness (in which case a witness exclusion certificate may be appropriate) and the disclosure is likely to prejudice national security.<sup>311</sup>

A disclosure is “likely to prejudice national security” if there is “a real, and not merely a remote, possibility that the disclosure will prejudice national security.”<sup>312</sup> Where the information is in the form of a document, the Attorney-General may give each potential discloser of the document a copy of the document with:

- the information deleted; or
- the information deleted and a summary attached; or

---

<sup>303</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 25(1)-(2).

<sup>304</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 25(3)-(5).

<sup>305</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 25(5).

<sup>306</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 25(6).

<sup>307</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 24(4) and s 25(7).

<sup>308</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 26(7) and s 28(10).

<sup>309</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 27 and s 28(5).

<sup>310</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 26(1)(a).

<sup>311</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 26(1)(b)-(c).

<sup>312</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 17.

- the information deleted and a statement of the facts that the information would or would be likely to prove attached;

together with a certificate that describes the information and states that the potential discloser may not disclose the information but may disclose the copy, statement and/or summary.<sup>313</sup>

Alternatively, the Attorney-General may give a certificate that describes the information and states that the potential discloser must not disclose the information except in permitted circumstances.<sup>314</sup>

The court must be given the certificate as well as any source document, copy, summary or statement.<sup>315</sup> Where the information is not a document, similar provisions apply.<sup>316</sup>

#### 4.3.4.2 Witness exclusion certificates

A witness exclusion certificate may be issued where notice has been given to the Attorney-General, or the Attorney-General for any reason believes, that information of the sort described above will be disclosed by the mere presence of a witness, and that such disclosure is likely to prejudice national security.<sup>317</sup> In such a case the Attorney-General may give a certificate to the prosecutor or the defendant stating that a witness must not be called.<sup>318</sup>

#### 4.3.5 Closed hearings

The Attorney-General may intervene in a closed hearing.<sup>319</sup> It is important not to misunderstand the nature of such a hearing. It

*is not concerned essentially with the admission or exclusion of evidence. It is concerned only with disclosure and the identification of material that may be later adduced in the trial. Questions as to the admissibility of the evidence and the manner of giving evidence remain for the determination of the trial judge in the ordinary way.*<sup>320</sup>

In a closed hearing under the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) the defendant and/or their lawyer (if the lawyer has not been given a security clearance at the “level considered appropriate by the Secretary” of the Attorney-General’s Department) may be ordered to leave the court for national security reasons while the prosecutor or the Attorney-General gives details of the sensitive information, or argues why it should not be disclosed or why a witness should not be called.<sup>321</sup> The defendant or their lawyer must be given the

<sup>313</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 26(2)(a).

<sup>314</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 26(2)(b).

<sup>315</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 16(4).

<sup>316</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 26(3).

<sup>317</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 28(1).

<sup>318</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 28(2).

<sup>319</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 30.

<sup>320</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 7 February 2006) (Whealy J) at [96].

<sup>321</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 29(3).

opportunity to make submissions about any such argument.<sup>322</sup> After a hearing, the court must make an order under s 31.

Under s 31, the court may make any order with respect to the disclosure of documents or information that the Attorney-General could have made, regardless of the type of disclosure that is in fact permitted in the Attorney-General's certificate.<sup>323</sup> The court may also decline to give effect to the Attorney-General's certificate at all by ordering that the information can be disclosed without alteration or that the witness can be called.<sup>324</sup> In such a case, the information will only be admissible in evidence if it would otherwise be admissible.<sup>325</sup>

In deciding what order to make under s 31, the court must consider:

- (a) *whether, having regard to the Attorney-General's certificate, there would be a risk of prejudice to national security if:*
  - (i) *...the information were disclosed in contravention of the certificate; or*
  - (ii) *...the witness were called;*
- (c) *whether any such order would have a substantial adverse effect on the defendant's right to receive a fair hearing, including in particular on the conduct of his or her defence;*
- (c) *any other matter the court considers relevant.*<sup>326</sup>

Subsection 31(8) provides that in making its decision the court must give the most weight to the matters in (a) above. In *R v Faheem Khalid Lodhi* (unreported, NSWSC, 7 February 2006, Whealy J) it was suggested in argument that the discretion under s 31 is a "sham" discretion and that the effect of ss 31(7) and (8) is to make the Attorney-General's certificate conclusive. Whealy J rejected this suggestion, stating that there were no grounds for supposing that in an appropriate case the court will not make orders that differ from the Attorney-General's certificate.<sup>327</sup> His Honour stated (at [108]) that "the legislation does no more than to give the Court guidance as to the comparative weight it is to give one factor when considering it alongside a number of other facts."

#### **4.3.6 Breach of a non-disclosure order or certificate, or a failure to notify the Attorney-General**

Division 1 of Part 5 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) creates a number of offences, punishable by 2 years

---

<sup>322</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 29(4).

<sup>323</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 31.

<sup>324</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), ss 31(5) and 31(6)(b).

<sup>325</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 31(5).

<sup>326</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 31(7).

<sup>327</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 7 February 2006) (Whealy J) at [108].

imprisonment, that will apply in the event of a breach of a non-disclosure order or certificate, or a failure to notify the Attorney-General in accordance with ss 24 or 25.

#### 4.3.7 Criticism and interpretation of the national security information provisions

It is important to point out that even after an order has been made under s 31, the court is not prevented “from later ordering that the federal criminal proceeding be stayed on a ground involving the same matter, including that an order made under s 31 would have a substantial adverse effect on a defendant’s right to receive a fair hearing.”<sup>328</sup> As the Attorney-General’s Department noted in their submissions to the Senate Legal and Constitutional Legislation Committee:

*Having decided that a particular document can be admitted with certain amendments, in making those amendments the right of the accused to a fair trial is not as significant as protecting the security of the information if it is extremely sensitive. But having made that decision, there is subsequently when the trial resumes a question of whether the trial proceeds.*<sup>329</sup>

In *R v Faheem Khalid Lodhi* (unreported, NSWSC, 7 February 2006), Whealy J noted (at [85]) that Part 3 of the Act does not impinge

*in any fundamental way upon the ordinary process of the establishment of guilt or innocence by judge and jury. The onus of proof does not alter. The rules of evidence are not changed. The discretions as to the exclusion of evidence in the trial remain untouched. The traditional protections given to an accused person are not put aside by the legislation.*

Whealy J also said that although the Act has the potential to cause significant delay in a trial, in a worst case scenario “the court would retain the right to bring the trial to an end either by discharge or, in the case of vexation or abuse of process by way of a stay.”<sup>330</sup> In the same case the Act survived what may be the first of many challenges on constitutional grounds. It was argued on behalf of various media interests that Pt 3 of the Act was constitutionally unsound because, inter alia, it breached the implied freedom of political communication, and required the NSW Supreme Court to exercise Commonwealth judicial power in a manner inconsistent with its fundamental attributes or character. In the course of rejecting these arguments, it was noted that powers of a (somewhat) similar nature that are conferred by the *Crimes Act 1914* (s 85B) and the *Criminal Code* (s 93.2) have not been criticised on constitutional grounds.<sup>331</sup> It was also pointed out that many of the procedural aspects of Pt 3 to which objection was taken – such as the delay caused by the mandatory adjournments required by the Part – could be avoided through the use of the pre-trial conferencing mechanism (s 21) combined with appropriate orders under s 22.<sup>332</sup>

---

<sup>328</sup> *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), s 19(2).

<sup>329</sup> Quoted in: Emerton, “Paving the Way” at 31.

<sup>330</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 7 February 2006) (Whealy J) at [88].

<sup>331</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 7 February 2006) (Whealy J) at [120].

<sup>332</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 7 February 2006) (Whealy J) at [84].

### 4.3.8 Special Advocates

In *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006), Whealy J considered an application by the accused for the appointment of a special advocate for the purposes of a forthcoming closed hearing. The Act does not make specific provision for the appointment of a special advocate, but legislation such as the *Special Immigration Appeals Commission Act 1997* (UK) allows for the appointment of such representatives in certain UK proceedings. Whealy J quotes a passage of Lord Woolf CJ in *M v The Secretary of State* (2004) 2 All ER 863 which summarises the nature and function of a special advocate under that Act:

*The involvement of a special advocate is intended to reduce (it cannot wholly eliminate) the unfairness, which follows from the fact that an appellant will be unaware at least as to part of the case against him. Unlike the appellant's own lawyers, the special advocate is under no duty to inform the appellant of secret information. That is why he can be provided with closed material and attend closed hearings...[A] special advocate can play an important role in protecting an appellant's interests before SIAC [the Security Information Appeals Commission]. He can seek further information. He can ensure that evidence before the SIAC is tested on behalf of the appellant. He can object to evidence and other information being unnecessarily kept from the appellant. He can make submissions to SIAC as to why the statutory requirements have not been complied with. In other words he can look after the interests of the appellant, in so far as it is possible for this to be done without informing the appellant of the case against him and without taking direct instructions from the appellant.*<sup>333</sup>

In the case before Whealy J, the defendant was seeking the appointment of an advocate of a similar nature to the one described above. The defendant argued that the inherent power of the Supreme Court to control its own proceedings (which is preserved, subject to any express provision to the contrary, by s 19(1) of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth)) was wide enough to allow the court to appoint a special advocate.<sup>334</sup> The Attorney-General opposed the application, arguing that s 29(2)(e) – which allows “any legal representative of the defendant” to be present at a closed hearing unless the court orders otherwise on national security grounds – could not be construed as referring to a representative in the nature of a special advocate.<sup>335</sup> In the result Whealy J found that the Supreme Court had the power to appoint a special advocate, and that the provisions of the Act were not inconsistent with such an appointment.<sup>336</sup> Indeed, in many respects such an appointment would reflect the object of the Act as set out in s 3<sup>337</sup> (see above). His Honour held that a special advocate would only be appointed “if the Court is satisfied that no other course will adequately meet the overriding requirements of fairness to the defendant (*R v McKeown* [(2004) NICA 41]).”<sup>338</sup> Even so, it was noted that English cases such as *Regina (Roberts) v The*

<sup>333</sup> Quoted in *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [16].

<sup>334</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [17].

<sup>335</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [21].

<sup>336</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [28]-[32].

<sup>337</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [32].

<sup>338</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [45].



*Parole Board & Anor* (2005) 3 WLR 152 show that “in some situations, even the appointment of special counsel will not be enough to save a suggested procedure from resulting in unfairness, abuse of process and a denial of natural justice.”<sup>339</sup>

Ultimately, Whealy J declined to make the order sought by the defendant on the basis that the application was somewhat premature.<sup>340</sup> His Honour adjourned the matter to the day of the closed hearing, making recommendations to the effect that a special advocate should be got ready in case he or she should subsequently be required.<sup>341</sup>

#### **4.4 Video Link Evidence in Terrorism Related Proceedings**

The traditional approach to the giving of evidence in criminal trials is stated in *R v McHardie & Danielson* (1983) 2 NSWLR 733 at 739:

*The general rule is that a normal criminal jury trial provides for the presentation of the Crown case in the presence and hearing of the accused and this procedure is correctly described as a ‘right.’*<sup>342</sup>

The enactment of the *Evidence (Audio and Audio Visual Links) Act 1998* (NSW) provides a significant exception to this “right.” Indeed, there has been a general trend in the use of audio visual facilities both locally and abroad that has made the use of evidence given via such facilities much more accepted than it once was.<sup>343</sup>

Part IAE of the *Crimes Act 1914* (Cth) (“Video link evidence in proceedings for terrorism and related offences etc”) was inserted by the *Law and Justice Legislation Amendment (Video Link Evidence and Other Measures) Act 2005* (Cth). The purpose of the Part, as the Attorney-General stated during the second reading speech in the House of Representatives on 14 September 2005 (at p. 8), is to “ensure that, in terrorism cases, so long as the defendant’s right to a fair trial is not infringed, important evidence from overseas witnesses can be put before the court using video link technology.”

Part IAE applies to most of the terrorist offences that have been set out in this paper, including offences against Division 72 and Part 5.3 of the *Criminal Code* (Cth).<sup>344</sup> In such proceedings, the prosecutor or the defendant may apply for a witness (who is not the defendant) to give evidence by video link.<sup>345</sup> So long as:

- the witness is available or will reasonably be available to give video link evidence; and
- the required facilities are available or will reasonably be available; and
- the court is satisfied that the applicant gave the court reasonable notice of his or her intention to make an application for evidence to be given by video link;

<sup>339</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [39].

<sup>340</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [44].

<sup>341</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 21 February 2006) (Whealy J) at [46]-[48].

<sup>342</sup> Quoted in *R v Faheem Khalid Lodhi* (unreported, NSWSC, 27 February 2006) (Whealy J) at [25].

<sup>343</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 27 February 2006) (Whealy J) at [37]-[46].

<sup>344</sup> *Crimes Act 1914* (Cth), s 15YU.

<sup>345</sup> *Crimes Act 1914* (Cth), s 15YV.

then the court “must” direct or by order allow the witness to give evidence by video link unless:

- where the applicant is the prosecutor, the court is satisfied that the direction or order “would have a substantial adverse effect on the right of a defendant in the proceeding to receive a fair hearing”<sup>346</sup> (“substantial adverse effect” is defined to mean “an effect that is adverse and not insubstantial, insignificant or trivial”<sup>347</sup>); or
- where the applicant is the defendant, the court is satisfied that “it would be inconsistent with the interests of justice for the evidence to be given by video link.”<sup>348</sup>

The court may when making the order or direction,<sup>349</sup> or at any time afterwards,<sup>350</sup> require that an appropriate and independent observer<sup>351</sup> be physically present at the place where the witness gives their evidence, and the court may direct or allow such an observer to give the court a report.<sup>352</sup> The court may use the report in determining whether or not evidence by the witness should be admitted as evidence in the proceedings.

In relation to an application made by a prosecutor, Whealy J has said that “properly construed, the expression ‘substantial adverse effect’ does not mean that a heavy burden is placed on the accused.”<sup>353</sup> Nevertheless, the burden would not appear to be one that is easily discharged. Since it is up to the accused to show that the prosecutor’s application should be refused, the prosecutor does not need to show a good reason why the evidence should be given by video link.<sup>354</sup> Moreover, where the use of video link facilities has the potential to have a substantial adverse effect on the accused’s right to receive a fair hearing, the court will consider whether this can be ameliorated by requiring the presence of an observer.<sup>355</sup> A fair trial is not to be equated with a perfect trial, and the determination of what is fair in any given case will require the balancing of different interests.<sup>356</sup>

Once a determination has been made, the court must adjourn on the request of a party who is opposed to the court’s decision to grant or refuse an application in order to allow that party to decide whether or not to appeal the decision or (in the case of the prosecutor) withdraw the proceedings, or so as to allow the party to make the appeal or to withdraw the proceedings.<sup>357</sup>

---

<sup>346</sup> *Crimes Act 1914* (Cth), s 15YV(1).

<sup>347</sup> *Crimes Act 1914* (Cth), s 15YV(3).

<sup>348</sup> *Crimes Act 1914* (Cth), s 15YV(2).

<sup>349</sup> *Crimes Act 1914* (Cth), s 15YW(1).

<sup>350</sup> *Crimes Act 1914* (Cth), s 15YW(2).

<sup>351</sup> *Crimes Act 1914* (Cth), s 15YW(5).

<sup>352</sup> *Crimes Act 1914* (Cth), s 15YW(7).

<sup>353</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 27 February 2006) (Whealy J) at [51].

<sup>354</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 27 February 2006) (Whealy J) at [61].

<sup>355</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 27 February 2006) (Whealy J) at [69]-[71].

<sup>356</sup> *R v Faheem Khalid Lodhi* (unreported, NSWSC, 27 February 2006) (Whealy J) at [52]-[57].

<sup>357</sup> *Crimes Act 1914* (Cth), s 15YX.

Where the proceedings involve a jury and the video link evidence is admissible, “the judge must give such directions as the judge thinks necessary to ensure that the jury gives the same weight to the evidence as if it had been given by the witness in the courtroom or other place where the court is sitting.”<sup>358</sup>

---

<sup>358</sup> *Crimes Act 1914* (Cth), s 15YZ.

## Chapter 5: Warrants and Orders: Conventional Powers

### **5.1 Introduction**

The threat of terrorism raises some fundamental questions about law enforcement in NSW. This is particularly evident in relation to warrants or orders authorising the detention without charge of non-suspects in relation to terrorist acts. At the heart of the debate is the fear that “in the name of national defence, we would sanction the subversion of one of the liberties that makes the defence of the nation worthwhile.”<sup>359</sup> The rest of this paper analyses the powers and duties of members of the judiciary who may issue the various warrants and orders available under the law.

As Lord Wilberforce said in *R v Inland Revenue Commissioner; Ex parte Rossminster Ltd* [1980] AC 952 at 1000:

*There is no mystery about the word “warrant”: it simply means a document issued by a person in authority under power conferred in that behalf authorising the doing of an act which would otherwise be illegal.*

In NSW alone, there are at least 102 different pieces of legislation that confer a power to issue a search warrant.<sup>360</sup> A unanimous High Court held in *George v Rockett* (1990) 93 ALR 483 at 487:

*...in construing and applying such statutes, it needs to be kept in mind that they authorise the invasion of interests which the common law has always valued highly and which, through the writ of trespass, it went to great lengths to protect. Against that background, the enactment of conditions which must be fulfilled before a search warrant can be lawfully issued and executed is to be seen as a reflection of the legislature’s concern to give a measure of protection to these interests. To insist on strict compliance with the statutory conditions governing the issue of search warrants is simply to give effect to the purpose of the legislation.*

It may be accepted that this statement applies with equal force to the various other kinds of warrants that are available to law enforcement agencies (subject, of course, to the language of the statute in question).<sup>361</sup> Such warrants may interfere with rights other than property rights, such as a person’s right to be brought before a magistrate at the earliest opportunity in the case of detention warrants. Others, such as listening device warrants or interception warrants, may interfere with a person’s privacy. Although there is no strict legal “right” to privacy, the NSW Law Reform Commission has said that “it is reasonable to regard privacy as a basic human right.”<sup>362</sup>

### **5.2. Search Warrants**

---

<sup>359</sup> US Supreme Court, quoted in: Barker, “Human rights” at 280.

<sup>360</sup> See *Law Enforcement (Powers and Responsibilities) Act 2002*, Sch 2.

<sup>361</sup> See *R v Nicholas* [2000] VSCA 49.

<sup>362</sup> NSWLRC, *Surveillance: an interim report*, Report 98, 2001 (hereafter *Surveillance*) at [1.8].

“A search warrant...authorises an invasion of premises without the consent of persons in lawful possession or occupation thereof.”<sup>363</sup> The *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) commenced operation on the 1st of December, 2005. Part 5 of that Act deals with search warrants and largely replicates provisions that used to be found in the *Search Warrants Act 1985* (NSW) and the *Crimes Act 1900* (NSW).

### 5.2.1 Authorised officers and applications for search warrants

Under s 47(1) of Pt 5:

*A police officer may apply to an authorised officer for a search warrant if the police officer believes on reasonable grounds that there is or, within 72 hours will be, in or on any premises:*

- (a) a thing connected with a particular indictable offence, or*
- (b) a thing connected with a particular firearms offence, or*
- (c) a thing connected with a particular prohibited weapons offence, or*
- (d) a thing connected with a particular narcotics offence, or*
- (e) a thing connected with a particular child pornography offence, or*
- (f) a thing stolen or otherwise unlawfully obtained.*<sup>364</sup>

Obviously, only (a)-(c) and perhaps (f) will be relevant in respect of most ‘terrorist’ acts. An indictable offence is defined to include any act or omission that would be an indictable offence if done or omitted to be done in NSW,<sup>365</sup> and s 47(3) explicitly states that an application may be made in respect of an act or omission that is an indictable offence “even though the act or omission occurred outside New South Wales and was not an offence against the law of New South Wales.”<sup>366</sup> Except in the case of telephone warrants, a search warrant must not be issued unless the application is made in person and is verified before the authorised officer on oath or affirmation or by affidavit.<sup>367</sup>

An “**authorised officer**” is defined to mean

- (a) a Magistrate or a Children’s Magistrate, or*
- (b) a clerk of a Local Court, or*
- (c) an employee of the Attorney-General’s Department authorised by the Attorney-General as an authorised officer for the purposes of this Act either*

<sup>363</sup> *George v Rockett* (1990) 93 ALR 483 at 486 per curiam.

<sup>364</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 47(1).

<sup>365</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 47(4).

<sup>366</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 47(3).

<sup>367</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 60.

*personally or as the holder of a specified office.*<sup>368</sup>

Section 48 provides that:

*An authorised officer to whom an application for a search warrant is made may, if satisfied that there are reasonable grounds for doing so, issue a search warrant authorising any police officer:*

*(a) to enter the premises; and*

*(b) to search the premises for things of a kind referred to in section 47(1).*

### **5.2.2 Reasonable grounds**

Section 62(2) gives an authorised officer some guidance as to what constitutes reasonable grounds. It states that:

*An authorised officer, when determining whether there are reasonable grounds to issue a warrant, is to consider (but is not limited to considering) the following matters:*

*(a) the reliability of the information on which the application is based, including the nature of the source of the information,*

*(b) if the warrant is required to search for a thing in relation to an alleged offence – whether there is sufficient connection between the thing sought and the offence.*

Applying the test used by Sully J in *Rohozynsky v Holder* [2005] NSWSC 868 at [56], before issuing a search warrant an authorised officer must be satisfied that, “assuming that the application [is] prima facie justified in terms of the [s 47] requirements, it [is] reasonable, having proper regard to the requirements of [s 62(2)], and having regard to all other relevant considerations, to issue the Warrant.”<sup>369</sup> That is,

*The duty, which the [authorised officer] must perform in respect of an information, is not some quaint ritual of the law, requiring a perfunctory scanning of the right formal phrases, perceived but not considered, and followed by simply an inevitable signature. What is required by the law is that the [authorised officer] should stand between the police and the citizen, to give real attention to the question whether the information proffered by the police does justify the intrusion they desire to make into the privacy of the*

---

<sup>368</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 3(1).

<sup>369</sup> Note that since this was a case under the *Search Warrant Act 1985* (NSW) (which is not materially different to the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) with respect to the provisions in question), I have replaced the section numbers used by Sully J with the corresponding section numbers in the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW).

*citizen and the inviolate security of his personal and business affairs.*<sup>370</sup>

It is clear from the terms of s 47 that before applying for a search warrant a police officer *must* believe on reasonable grounds that the relevant circumstances exist. An authorised officer, on the other hand, only has to be satisfied that there are reasonable grounds for issuing the warrant, which entails that the authorised officer needs to be reasonably satisfied that there are reasonable grounds for the police officer's belief. The authorised officer him or herself does not have to entertain that belief.<sup>371</sup> This is because "[w]hen a statute prescribes that there must be "reasonable grounds" for a state of mind – including suspicion and belief – it requires the existence of facts which are sufficient to induce that state of mind in a reasonable person."<sup>372</sup> Part 5 of the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) refers to belief on reasonable grounds. In *George v Rockett* (1990) 93 ALR 483 at 491, the High Court held that

*The objective circumstances sufficient to show a reason to believe something need to point more clearly to the subject matter of the belief [than the objective circumstances sufficient to show a reason to suspect something], but that is not to say that the objective circumstances must establish on the balance of probabilities that the subject matter in fact occurred or exists: the assent of belief is given on more slender evidence than proof. Belief is an inclination of the mind towards assenting to, rather than rejecting, a proposition and the grounds which can reasonably induce that inclination of the mind may, depending on the circumstances, leave something to surmise or conjecture.*

If there is insufficient information in an application for a search warrant to provide reasonable grounds for issuing the search warrant, then any warrant issued on the basis of such information will be invalid.<sup>373</sup> Section 62(1) of the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) states that:

*An authorised officer must not issue a warrant unless the application for the warrant includes the following information:*

- (a) details of the authority of the applicant to make the application for the warrant,*
- (b) the grounds on which the warrant is being sought,*
- (c) the address or other description of the premises the subject of the application,*
- (d) if the warrant is required to search for a particular thing a full description of that thing and, if known, its location,*

---

<sup>370</sup> *Parker v Churchill* (1985) 9 FCR 316 at 333 per Burchett J, quoted with approval by the High Court in *George v Rockett* (1990) 93 ALR 483 at 487-488. References to "Justice of the Peace" have been omitted and replaced with the words "authorised officer."

<sup>371</sup> See *George v Rockett* (1990) 93 ALR 483 at 488 per curiam.

<sup>372</sup> *George v Rockett* (1990) 93 ALR 483 at 488 per curiam.

<sup>373</sup> *George v Rockett* (1990) 93 ALR 483 at 489 per curiam.

- (e) if a previous application for the same warrant was refused details of the refusal and any additional information required by section 64,
- (f) any other information required by the regulations.

Section 64 provides that an application for the same warrant may not be made unless it is an application to a magistrate following an unsuccessful application to an authorised officer who is not a magistrate, or unless there is “additional information that justifies the making of the further application.”<sup>374</sup> In any case, the applicant must provide “such further information as the authorised officer requires concerning the grounds on which the warrant is being sought”<sup>375</sup> (although an applicant is not required to disclose the identity of a source if do so might jeopardise their safety<sup>376</sup>). The *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW) sets out the form that is to be used in an application for, inter alia, a Pt 5 warrant.<sup>377</sup> As well as the above information, the form specifies that the offence in respect of which a thing is reasonably believed to be connected (see s 47) is also to be set out in the application.<sup>378</sup>

Once an authorised officer is satisfied that there are reasonable grounds for issuing a warrant, he or she may issue a search warrant. If an authorised officer issues a warrant, he or she must make a record of “all relevant particulars of the grounds the authorised officer has relied on to justify the issue of the warrant.”<sup>379</sup> In *Carroll v Mijovich* (1991) 25 NSWLR 444, the majority held that failure to comply with this requirement will result in the invalidity of a warrant. The *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW) specifies the form that such a record must take,<sup>380</sup> the documents that must be kept in connection with the issue of a warrant, as well as how, when and if they can be inspected.<sup>381</sup>

### 5.2.3 Terms of a search warrant

A warrant must be in the form prescribed by the regulations.<sup>382</sup> Essentially, what is required is:

1. *The precise identification of the premises, the searching of which the warrant authorises;*
2. *The precise identification of who exactly it is who will be entitled to enter and search, and if appropriate seize, under the authority of the warrant;*

---

<sup>374</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 64.

<sup>375</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 62(3).

<sup>376</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 62(4).

<sup>377</sup> *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW), s 4.

<sup>378</sup> *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW), Sch 1, Form 1, Part 1.

<sup>379</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 65(1).

<sup>380</sup> *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW), Sch 1, Form 1, Part 2.

<sup>381</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 65(2); *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW), ss 10-11.

<sup>382</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 66. See *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW), Sch 1, Form 9.



3. *What it is for which any such person may search; and what it is which, if found, may thereupon be seized under the authority of the warrant;*
4. *What alleged offence(s) persuaded the authorising Justice to issue the warrant.*<sup>383</sup>

What is to be avoided is a general warrant; that is, a warrant “of the kind the law decisively rejected in the eighteenth century.”<sup>384</sup> The warrant must not, for instance, purport to authorise a search for a thing that is of too wide and general a description, or fail to specify at all<sup>385</sup> the offence in respect of which the warrant is issued. In this regard, Burchett J has said that the offence may not need to be described with exactitude in every case. His Honour states that:

*The question should not be answered by the bare application of a verbal formula, but in accordance with the principle that the warrant should disclose the nature of the offence so as to indicate the area of search. The precision required in a given case, in any particular respect, may vary with the nature of the offence, the other circumstances revealed, the particularity achieved in other respects, and what is disclosed by the warrant, read as a whole, and taking account of its recitals.*<sup>386</sup>

Nevertheless, where it is possible a search warrant should:

- “refer to a particular offence and authorise seizure by reference to that offence;”<sup>387</sup>
- include the approximate time and date of the offence if possible; and
- identify the alleged offender where possible. This is not required by the legislation but by doing so “greater precision is lent to the warrant.”<sup>388</sup> Note that precise information given in one respect may make up for a lack of particularity in some other respect.<sup>389</sup>

A search warrant must:

- specify the time the warrant is to expire (which is 72 hours after the warrant is issued unless the authorised officer is satisfied that the warrant cannot be executed within 72 hours),<sup>390</sup> and

<sup>383</sup> *Rohozynsky v Holder* [2005] NSWSC 868 at [25] (Sully J).

<sup>384</sup> *Beneficial Finance Corporation Ltd v Commissioner of Australian Federal Police* (1991) 103 ALR 167 at 178 per Burchett J.

<sup>385</sup> In such a case, the warrant will be invalid even if it complies “precisely and completely with the prescribed form authorised by the statute.” *Douglas v Blackler* [2001] NSWSC 901 at [12] (Taylor AJ). See also *Warner v Elder* (unreported, NSWSC, 23 April 1997, confirmed on appeal).

<sup>386</sup> *Beneficial Finance Corporation Ltd v Commissioner of Australian Federal Police* (1991) 103 ALR 167 at 188.

<sup>387</sup> *R v Tillet; Ex parte Newton* (1969) 14 FLR 101 at 113.

<sup>388</sup> Toohey J in the unreported case of *Quartermaine v Netto* (14 December 1984), quoted in *Beneficial Finance Corporation Ltd v Commissioner of Australian Federal Police* (1991) 103 ALR 167 at 188.

<sup>389</sup> *Ryder v Morley* (1986) 12 FCR 438 at 443 per Toohey J.

<sup>390</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 73(2)-(5).

- specify whether or not the warrant may be executed by night.<sup>391</sup> Execution by night may only be authorised when there are reasonable grounds for doing so, which grounds might include the safety of any person, or the likelihood that a thing might be on the premises at a given time.<sup>392</sup>

Any defect in a search warrant will not invalidate the warrant unless “the defect affects the substance of [the] warrant in a material particular.”<sup>393</sup>

#### 5.2.4 Extension of a search warrant

On an application before the expiry of a search warrant, the authorised officer who issued the warrant may extend the warrant by up to 72 hours if satisfied that the warrant cannot be executed within the first 72 hours.<sup>394</sup>

#### 5.2.5 Occupier’s notices

When a warrant is issued, the authorised officer must prepare an occupier’s notice and give it to the person to whom the warrant is issued.<sup>395</sup> The form of the notice is set out in the *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW).<sup>396</sup> As well as containing a summary of the nature of the warrant and the powers conferred thereby,<sup>397</sup> the notice must specify:

- (i) *the name of the person who applied for the warrant,*
- (ii) *the name of the authorised officer who issued the warrant,*
- (iii) *the date and time when the warrant was issued,*
- (iv) *the address or other description of the premises the subject of the warrant.*<sup>398</sup>

#### 5.2.6 Issue of a search warrant by telephone

An authorised officer may issue a warrant following an application by telephone if satisfied that the warrant is required urgently and that it is not practicable for the application to be made in person.<sup>399</sup> Such an application is to be made by fax if the facilities are readily available.<sup>400</sup> Gleeson CJ noted in *Commissioner of Police v Atkinson* (1991) 23 NSWLR 495 at 499 that a telephone warrant

*is not to be regarded as merely an alternative method of obtaining a search*

<sup>391</sup> *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW), Sch 1, Form 9.

<sup>392</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 72(2).

<sup>393</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 76.

<sup>394</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 73A.

<sup>395</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 67.

<sup>396</sup> Sch 1, Form 17.

<sup>397</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 67(2)(c).

<sup>398</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 67(2)(b).

<sup>399</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 61(1)-(2).

<sup>400</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 61(4).

*warrant which may be employed to suit the convenience of the applicant for the warrant. Because it is not accompanied by the protections contained in the ordinary method, and also by reason of the language of [s 61] itself, it is to be regarded as an exceptional method of obtaining a search warrant, and it may be employed only in cases where, in the terms of the statute, the authorised [officer] is satisfied that the warrant is required urgently and that it is not practicable for the application to be made in person.*

In that case a telephone warrant was held invalid because at the time it was issued there was no evidence before the issuing magistrate as to when the decision to search the premises had been made by the applicant. In the circumstances of the case, it was held that it was not possible for the magistrate to “properly or adequately” consider the issues raised by s 12(3) of the *Search Warrants Act 1985* (NSW) (now s 61(2) of the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW)) in relation to urgency and practicality.<sup>401</sup> An authorised officer need not record the reasons why he or she is or is not satisfied with respect to the urgency and practicality of the application, but must state whether or not he or she is or is not so satisfied.<sup>402</sup>

An authorised officer who issues a telephone warrant must:

- (a) complete and sign the warrant, and*
- (b) furnish the warrant to the person who made the application or inform that person of the terms of the warrant and of the date and time when it was signed, and*
- (c) in the case of a search warrant, prepare and furnish an occupier’s notice to the person who made the application or inform the person of the terms of the occupier’s notice.<sup>403</sup>*

A telephone search warrant will expire 24 hours after being issued if it has not been executed in that time<sup>404</sup> and it cannot be extended.<sup>405</sup>

## **5.2.7 Search warrants under the Commonwealth legislation**

The principles that apply to the issuing of search warrants under the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) also apply to search warrants issued under the *Crimes Act 1914* (Cth). These two regimes are similar in many respects, so that it is only necessary here to point out some of the most salient differences between them. In contrast to the NSW Act, which refers to reasonable grounds for believing that a thing(s) connected with certain offences are or will be (within 72 hours) on premises, the Commonwealth Act requires an issuing officer to be satisfied “that there are reasonable grounds for *suspecting* that there is or will be

---

<sup>401</sup> *Commissioner of Police v Atkinson* (1991) 23 NSWLR 495 at 506 per Gleeson CJ.

<sup>402</sup> *Law Enforcement (Powers and Responsibilities) Regulation 2005* (NSW), Sch 1, Form 1; *Commissioner of Police v Atkinson* (1991) 23 NSWLR 495 at 503 per Gleeson CJ.

<sup>403</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 61(5).

<sup>404</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 73(1)(b).

<sup>405</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 73A(3).

within the next 72 hours, any *evidential material* at the premises”<sup>406</sup> (emphasis added) before he or she issues a search warrant. As to what constitutes reasonable grounds for suspecting, see 5.3.5 below. “Evidential material” is “a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form.”<sup>407</sup>

Notably, where data is held in, or is accessible from, a computer on premises in respect of which a warrant has been issued, an officer executing the warrant may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonably necessary to allow the officer to access, copy and/or convert the data into documentary form.<sup>408</sup> The magistrate may grant the order if satisfied that:

(a) *there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and*

(b) *the specified person is:*

(i) *reasonably suspected of having committed the offence stated in the relevant warrant; or*

(ii) *the owner or lessee of the computer; or*

(iii) *an employee of the owner or lessee of the computer; and*

(c) *the specified person has relevant knowledge of:*

(i) *the computer or a computer network of which the computer forms a part; or*

(ii) *measures applied to protect data held in, or accessible from, the computer.*<sup>409</sup>

It is an offence punishable by six months imprisonment to fail to comply with such an order.<sup>410</sup>

## **5.3 Listening Device Warrants**

### **5.3.1 Introduction**

In his book titled *Investigating Corruption and Misconduct in Public Office*,<sup>411</sup> Justice Hall lists some of the benefits of electronic surveillance that were identified by the

---

<sup>406</sup> *Crimes Act 1914* (Cth), s 3E(1).

<sup>407</sup> *Crimes Act 1914* (Cth), s 3C.

<sup>408</sup> *Crimes Act 1914* (Cth), s 3LA

<sup>409</sup> *Crimes Act 1914* (Cth), s 3LA(2).

<sup>410</sup> *Crimes Act 1914* (Cth), s 3LA(3).

<sup>411</sup> Hall, P. M., *Investigating Corruption and Misconduct in Public Office: Commissions of Inquiry – Powers and Procedure*, Lawbook Co, Sydney, 2004 (hereafter *Investigating Corruption*). Note that much of this section is based on the “Electronic Surveillance and Telecommunications Interception” chapter of Mr. Justice Hall’s book.

Wood Royal Commission. Two of those benefits stand out as particularly relevant to terrorist offences. These benefits are

- 1) “the possible opportunity to effect an arrest while a crime is in the planning stage, thereby lessening the risk to lives and property;”<sup>412</sup> and
- 2) the achievement of “overall efficiencies in the investigation of...forms of criminality that are covert, sophisticated, and difficult to detect by conventional methods, particularly where those involved are aware of policing methods, are conscious of visual surveillance, and employ counter-surveillance techniques.”<sup>413</sup>

Although they have utility, listening device warrants do authorise a substantial interference with the privacy of an individual. Article 17 of the *International Covenant on Civil and Political Rights* (“the ICCPR”) provides that

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence...*
2. *Everyone has the right to the protection of the law against such interference...*

Because of the importance of privacy many of the principles that are applicable to search warrants are also applicable, or at least relevant, to listening device warrants. One must, however, be cautious when applying such principles,<sup>414</sup> especially considering that search warrants are intended to be produced to the person affected by the search for their inspection, whereas listening device warrants are necessarily covert.<sup>415</sup> In this sense listening device warrants are more analogous to interception warrants than search warrants.<sup>416</sup>

In its interim report on surveillance, the NSWLRC succinctly summarised the operation of the *Listening Devices Act 1984* (NSW) (referred to in the report as “the LDA”) as follows [note: the NSWLRC’s original footnotes have been inserted into the text in square brackets; my own footnotes are in the usual form]:

5.6 ...[T]he LDA prohibits covert surveillance unless it is carried out in accordance with that Act and has been authorised by warrant. Part 4 of the LDA contains the relevant provisions pertaining to warrants.

5.7 There is no restriction on who may apply for authorisation to use a listening device. In order to succeed on an application for a warrant, “a person” (the applicant) must satisfy an “eligible Judge” of the Supreme Court that there are reasonable grounds to believe that a “prescribed” offence has been, is about to be or is likely to be committed, and that the use of a listening device is necessary to investigate that offence, or obtain evidence of the

---

<sup>412</sup> Ibid at p. 422.

<sup>413</sup> Ibid at p. 423.

<sup>414</sup> *Ousley v The Queen* (1997) 192 CLR 69 at 118 per Gummow J.

<sup>415</sup> Hall, *Investigating Corruption*, pp. 454-455 p. 461.

<sup>416</sup> *Ousley v The Queen* (1997) 192 CLR 69 at 119 per Gummow J.

offender or of the commission of the offence [s 16(1)]. An “eligible Judge” is one whom the Attorney General has declared, with that judge’s consent, to be eligible for the purposes of the LDA [s 3A. The regulations may provide that, in certain prescribed circumstances, the functions of an eligible judge may be exercised by an eligible judicial officer]. A “prescribed offence”<sup>417</sup> is an indictable offence or is prescribed for the purposes of Part 4, whether indictable or not [s 15].

5.8 Pursuant to section 16(2), in determining whether a warrant should be granted, the judge is to have regard to: the nature of the offence; the likely impact on privacy; alternative means of obtaining the evidence or information; the evidentiary value of the evidence; and any previous warrant sought or granted in connection with the offence.

5.9 Section 16(3) provides that, in authorising the installation of a listening device on premises, the Court must authorise and require the retrieval of the listening device and authorise entry onto the premises for that purpose.

5.10 Section 16(4) prescribes that a warrant must specify a number of matters, in default of which the warrant will not be valid [*Hayes v Attorney General (NSW)* (Unreported, NSWSC, 9 February 1996)]. These matters are as follows:

- the prescribed offence in respect of which the warrant is granted;
- where practicable, the name of any person whose private conversation may be recorded or listened to;
- the period during which the warrant is in force;
- the name of any person who may use the listening device, or who may use it on that person’s behalf;
- where practicable, the premises on which the device is to be installed, or the place at which it is to be used;
- any conditions applying to entry onto premises or use of the listening device; and
- the time within which the surveillance user must report to an eligible judge and the Attorney General.

5.11 An applicant for a warrant must also serve on the Attorney General notice of the particulars required by section 16(4), as well as particulars of: the type of listening device intended to be used; details of any previous warrant sought or granted; any other alternative means of obtaining the information or evidence; and the results of any attempt to use alternative means [s 17(1)]. The Attorney General must have an opportunity of being heard in relation to the granting of the warrant [s 17(2)].

5.12 A warrant may be issued for a period not exceeding 21 days [s 16(4)(c)], but can be revoked before its expiry [s 16(5)]. Further warrants can be granted in respect of the same offence [s 16(6)].

---

<sup>417</sup> A prescribed offence includes an indictable offence under a law of the Commonwealth or of another State or Territory: *Listening Devices Act 1984* (NSW), s 15.

5.13 Under section 18, in urgent situations, a member of the police force can apply for a warrant by telephone [s 18; application can also be by radio or any other communication device: s 18(1)], providing the eligible judge is satisfied that “the immediate use of a listening device is necessary” and that it is not practicable to grant a warrant in the normal way pursuant to section 16 [ss 18(2)(b) and 18(3)]. A warrant granted under section 18 cannot be in force for longer than 24 hours [s 18(8)]. In all other respects, the provisions of section 16 (2)-(6) apply to section 18 warrants [s 18(8)].

5.14 A person to whom a warrant was granted, whether pursuant to section 16 or section 18, must satisfy the reporting requirements set out in section 19. Briefly, an eligible judge and the Attorney General must be given particulars in writing concerning the name, if known, of any person subjected to surveillance, the period during which, and the place at which, the device was used, or the premises on which it was installed, the use made of the surveillance material and particulars of any previous use of a listening device in respect of the subject offence [s 19(1)].

5.15 After reporting the results of surveillance conducted under warrant, an eligible judge may form the view that, having regard to the evidence or information obtained, or any other relevant matter, the use of the listening device was not justified and was an unnecessary interference with privacy. In that case, the eligible judge may make a direction that the subject of the surveillance be informed of the surveillance [s 20].

### 5.3.2 Recent changes to Listening Device Warrant Provisions

It is important to note that there has been a significant change in the *Listening Devices Act 1984* (NSW) since the NSWLRC’s report was written. Ordinarily, warrants last for a period not exceeding 21 days<sup>418</sup> or 24 hours in the case of telephone warrants.<sup>419</sup> The *Terrorism Legislation Amendment (Warrants) Act 2005* (NSW) has altered this position so that warrants granted in respect of “terrorist offences”<sup>420</sup> last for up to 90 days.<sup>421</sup> Remarkably, it appears that this is so whether or not the warrant is issued to an applicant in person or over the telephone.

### 5.3.3 Definitions

A **listening device** is “any instrument, apparatus, equipment or device capable of being used to record or listen to a private conversation simultaneously with its taking place.”<sup>422</sup> Devices capable of visual imaging and recording, as well as tracking devices, are not of themselves subject to the *Listening Devices Act 1984* (NSW), but a device is not precluded from being a listening device merely because it has such

---

<sup>418</sup> *Listening Devices Act 1984* (NSW), s 16(4)(c).

<sup>419</sup> *Listening Devices Act 1984* (NSW), s 18(8).

<sup>420</sup> Defined in s 16(8) as “an offence under Part B of the *Crimes Act 1900* or an offence against section 101.1, 101.2, 101.4, 101.5, 101.6, 102.2, 102.3, 102.4, 102.5, 102.6, 102.7 or 103.1” of the *Criminal Code* (Cth).

<sup>421</sup> *Listening Devices Act 1984* (NSW), combined effect of ss 16(4)(c) and 18(8).

<sup>422</sup> *Listening Devices Act 1984* (NSW), s 3(1).

capabilities.<sup>423</sup> Warrants have been granted in respect of devices that have tracking capabilities, but that were primarily to be used as listening devices.<sup>424</sup>

### 5.3.4 Grounds for the Issue of a Listening Device Warrant

The test for issuing a listening device warrant is set out in ss 16(1)-(2) and is as follows:

*(1) Upon application made by a person that the person suspects or believes:*

*(a) that a prescribed offence has been, is about to be or is likely to be committed, and*

*(b) that, for the purpose of an investigation into that offence or of enabling evidence to be obtained of the commission of the offence or the identity of the offender, the use of a listening device is necessary,*

*an eligible Judge may, if satisfied that there are reasonable grounds for that suspicion or belief, authorise, by warrant, the use of the listening device.*

*(2) In determining whether a warrant should be granted under this section, the eligible Judge shall have regard to:*

*(a) the nature of the prescribed offence in respect of which the warrant is sought,*

*(b) the extent to which the privacy of any person is likely to be affected,*

*(c) alternative means of obtaining the evidence or information sought to be obtained,*

*(d) the evidentiary value of any evidence sought to be obtained, and*

*(e) any previous warrant sought or granted under this Part in connection with the same prescribed offence.*

### 5.3.5 Interpretation of Grounds for the Issue of a Listening Device Warrant

I have considered above the concept of reasonable grounds for belief in relation to search warrants. The test in relation to listening device warrants is reasonable grounds for *suspicion* or belief. What may constitute reasonable grounds for

---

<sup>423</sup> *Listening Devices Act 1984 (NSW)*, s 3(1A).

<sup>424</sup> Hall, *Investigating Corruption*, p. 429 (n 31).



suspicion is something less than reasonable grounds for belief. The High Court considered the matter in *George v Rockett* (1990) 93 ALR 483 and said (at 490-491) that:

*Suspicion, as Lord Devlin said in Hussien v Chong Fook Kam [1970] AC 942 at 948, "in its ordinary meaning is a state of conjecture or surmise where proof is lacking: 'I suspect but I cannot prove.'" The facts which can reasonably ground a suspicion may be quite insufficient reasonably to ground a belief, yet some factual basis for the suspicion must be shown. In Queensland Bacon Pty Ltd v Rees (1966) 115 CLR 266...Kitto J said (at 303):*

*"A suspicion that something exists is more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to a 'slight opinion, but without sufficient evidence'..."*

In coming to a conclusion as to the admissibility of evidence obtained under a listening device warrant, "a court must determine merely whether the warrant was regularly granted by the eligible judge. It does not inquire into the sufficiency of the material which satisfied the eligible judge of the matters to which he or she must have regard."<sup>425</sup>

### 5.3.6 Validity of Listening Device Warrants and Admissibility of Evidence

As the NSWLRC notes, a warrant will be invalid if it fails to specify the matters listed in s 16(4) of the *Listening Devices Act 1984* (NSW). This will be the case if it **fails** to:

- specify the matter at all<sup>426</sup> or
- specify the matter with sufficient precision.<sup>427</sup>

A warrant that authorises the installation of a listening device on any premises will be invalid if it fails to require the retrieval of the listening device.<sup>428</sup>

Even if a listening device warrant is held to be invalid, evidence obtained in reliance on it may still be admissible. This will depend, firstly, upon whether s 13 – which concerns the admissibility of evidence of private conversations that is unlawfully obtained - applies. In *Amalgamated Television Services Pty Ltd v Marsden* [2000] NSWCA 167 the Court<sup>429</sup> said

*the section [i.e. s 13] does not apply where 'the person called to give evidence' is a 'principal party' to the private conversation. The conversation could not be said to 'come to the knowledge' of such a party. He had knowledge of the private conversation directly and contemporaneously as a*

<sup>425</sup> NSWLRC, *Surveillance*, at [5.36]. See *Murphy v The Queen* (1989) 167 CLR 94; see also Hall, *Investigating Corruption*, p. 454.

<sup>426</sup> *Hayes v Attorney General (NSW)* (Unreported, NSWSC, 9 February 1996).

<sup>427</sup> *Lawrence v NSW Police Service* [2004] NSWSC 59 (lack of precision in specification of offence).

<sup>428</sup> *Bayeh v Taylor* (unreported, NSWSC, Grove J, 4 February 1998).

<sup>429</sup> *Priestley and Powell JJA, and Foster AJA*; quoted with approval by Kirby J in *R v W J Eade* [2000] NSWCCA 369 at [56].

*participant in it. The person contemplated by the section is one who acquires knowledge of it other than as a participant in it.*

If s 13 does not apply, then the evidence may be given (subject, of course, to the usual exclusionary discretions, particularly s 138 of the *Evidence Act 1995* (NSW)). If s 13 does apply, then the evidence is inadmissible unless it falls into one of the exceptions in s 13(2). In relation to terrorist offences – which often attract substantial maximum sentences – the most relevant exception is contained in s 13(2)(d)(i), which provides that evidence obtained in contravention of s 5 (which includes evidence obtained under an invalid warrant) will not be rendered inadmissible under s 13(1) if it is evidence in proceedings for “an offence punishable by imprisonment for life or for 20 years or more.” In determining whether to admit such evidence, the court shall refer to the matters in s 13(3), which are similar (though different in terms) to the considerations guiding an exercise of discretion under s 138 of the *Evidence Act 1995* (NSW).<sup>430</sup> There is also an exception to the prohibition on the use of a listening device without warrant where it is to gather evidence or information in connection with “an imminent threat of serious violence to persons or of substantial damage to property” and “it is necessary to use the device immediately to obtain that evidence or information.”<sup>431</sup> Again, the use of such evidence will be subject to the usual exclusionary discretions.

Even when a warrant *is* validly issued, evidence obtained under it may still be inadmissible. An interesting example is in relation to an accused who is in custody or a suspect who is at large. In such cases, due regard must be had to the subject’s right to maintain their silence.<sup>432</sup> Where an accused in custody or a suspect at large has made it clear that they do not wish to answer questions, subsequent use of a police operative or informer equipped with a listening device may result in the evidence so obtained being excluded.<sup>433</sup> In *R v KS* [2003] VSC 418 the 15 year old accused (who had refused to comment during the record of interview) made admissions to an inmate who had been placed in the accused’s cell in order to stimulate conversation about the alleged offence (murder). The admissions were recorded by a listening device authorised by a valid warrant. The issue was whether the evidence should be excluded. In the course of his judgment (at [41]), Coldrey J quoted himself in *R v Heaney and Welsh* (1998) 4 VR 636 when he said:

*Putting aside the issue of voluntariness, the current approach of the majority of the High Court to the exclusory discretions seems to be as follows. The fairness discretion encompasses considerations of the effect of the conduct of law enforcement officers upon the reliability of the impugned material. The term 'law enforcement officers' may be regarded as including persons acting as their agents. The fairness discretion will also come into play where some impropriety by law enforcement officers or their agent has eroded the procedural rights of the accused, occasioning some forensic disadvantage. Those procedural rights include the right to choose whether or not to speak to the police. Importantly, the method of eliciting the admission or confession will clearly be relevant in determining whether or not it would be unfair to an*

<sup>430</sup> *R v W J Eade* [2000] NSWCCA 369 at [25] per Greg James J.

<sup>431</sup> *Listening Devices Act 1984* (NSW), s 5(2)(c)(i).

<sup>432</sup> *R v Swaffield* (1997) 192 CLR 159.

<sup>433</sup> *R v O'Neill* (1995) 81 A Crim R 458.

*accused to admit it into evidence. The discretion to exclude evidence on the grounds of public policy may be enlivened where no unfairness to the accused is occasioned, but nonetheless, the method by which the confessional evidence has been elicited is unacceptable in the light of prevailing community standards. This broad discretion will involve a balancing exercise.*

Because of the subversion of the accused's procedural rights and the forensic disadvantage occasioned thereby, the evidence was excluded.<sup>434</sup> In the South Australian case of *R v Smith* (1994) 75 A Crim R 327 evidence was excluded because at the time the listening device evidence was obtained, the police already had enough evidence to charge the suspect and so he should have been informed of his right to silence before he was recorded.<sup>435</sup> On the other hand, there are cases such as *R v Suckling* [1999] NSWCCA 36 where recordings made by a police informer of a suspect were not excluded. *Suckling* was a case where the informer was a friend and former cell-mate of the suspect who had approached the police of his own accord. The suspect had made voluntary statements to the informer and other people on prior occasions which indicated that there was a likelihood that he might voluntarily make further disclosures. In light of these facts, and considering the seriousness of the crime and the fact that the informer's conversations with the suspect were not in the nature of interrogations, the evidence was admitted.<sup>436</sup>

## **5.4 Surveillance Device Warrants**

### **5.4.1 Definition**

The Commonwealth Parliament recently enacted the *Surveillance Devices Act 2004* (Cth). This Act covers a wider range of surveillance devices than the *Listening Devices Act 1984* (NSW). A **surveillance device** is defined to mean:

*(a) a data surveillance device, a listening device, an optical surveillance device or a tracking device; or*

*(b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a); or*

*(c) a device of a kind prescribed by the regulations.<sup>437</sup>*

Each of the devices mentioned in para (a) are separately defined in s 6 of the Act as follows:

- *"data surveillance device" means any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device;*

---

<sup>434</sup> *R v KS* [2003] VSC 418 at [42]-[45].

<sup>435</sup> This summary is taken from Hall, *Investigating Corruption*, p. 433 (n 46).

<sup>436</sup> Again, this summary relies to a large extent on: *Ibid*, pp. 467-468.

<sup>437</sup> *Surveillance Devices Act 2004* (Cth), s 6(1).

- *"listening device" means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear;*
- *"optical surveillance device" means any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment;*
- *"tracking device" means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.*

The Act creates two types of warrants: surveillance device warrants and retrieval warrants.<sup>438</sup> Here we will only consider the former type of warrants.

#### **5.4.2 Issuing Authority**

An "eligible Judge" is a Judge of a court created by the Federal Parliament who has given their written consent and who is declared by the Minister to be an eligible Judge.<sup>439</sup> An "eligible Judge" or a "nominated AAT member" may issue a surveillance device warrant following an application by a law enforcement officer. A law enforcement officer may apply for a warrant in respect of (inter alia<sup>440</sup>) a "relevant offence."<sup>441</sup> Such an offence includes a federal offence or a State offence with a federal aspect that is punishable by a maximum term of at least 3 years imprisonment,<sup>442</sup> unless the applicant is a State or Territory law enforcement officer. Oddly, it would seem that State or Territory law enforcement officers can only apply for a warrant in respect of relevant federal offences; they cannot apply in respect of State offences with a federal aspect.<sup>443</sup>

#### **5.4.3 Grounds for application and issue of a surveillance device warrant**

Before applying, the applicant (or a person on their behalf) must suspect on reasonable grounds that:

- one or more relevant offences have been, are being or will be committed;
- an investigation into those offences is being, will be, or is likely to be conducted; and
- that the use of the surveillance device is necessary in order to obtain evidence of the commission of the offences or the identity or location of the offenders.<sup>444</sup>

<sup>438</sup> *Surveillance Devices Act 2004* (Cth), s 10(1).

<sup>439</sup> *Surveillance Devices Act 2004* (Cth), s 12.

<sup>440</sup> See *Surveillance Devices Act 2004* (Cth), s 14(3).

<sup>441</sup> *Surveillance Devices Act 2004* (Cth), s 14(1)(a).

<sup>442</sup> *Surveillance Devices Act 2004* (Cth), s 6(1).

<sup>443</sup> *Surveillance Devices Act 2004* (Cth), s 14(2). Section 14(2) that "if the application is being made by or on behalf of a State or Territory law enforcement officer, the reference in subsection (1) to a relevant offence does not include a reference to a State offence that has a federal aspect."

<sup>444</sup> *Surveillance Devices Act 2004* (Cth), s 14(1)

The application must:

- include the name of the applicant and the nature and duration of the warrant sought,<sup>445</sup> and
- be supported by an affidavit except in specified circumstances of urgency and impracticality.<sup>446</sup>

Applications may be made by telephone, fax, e-mail “or any other means of communication.”<sup>447</sup>

An eligible Judge or nominated AAT member may issue a warrant if, having regard to certain prescribed matters,<sup>448</sup> he or she is satisfied that (in the case of a warrant sought in relation to a relevant offence) “there are reasonable grounds for the suspicion founding the application for the warrant.”<sup>449</sup> Where the application is unsworn and/or made by telephone etc, the issuing officer must be satisfied that it would have been impracticable to have applied in the regular way.<sup>450</sup> The legislation sets out a long and very specific list of what a warrant “must” contain in s 17.

#### **5.4.4 Emergency authorisations**

In certain circumstances, a law enforcement officer can apply to an “appropriate issuing authority” for an emergency authorisation to use a surveillance device. An “appropriate authorising officer” is, in the case of the AFP, the AFP Commissioner, Deputy Commissioner or the Commissioner’s proper delegate.<sup>451</sup> In the case of a state police force, an “appropriate authorising officer” is a Commissioner, Assistant Commissioner, or Superintendent (or relevant equivalent).<sup>452</sup> Under s 28(1), a law enforcement officer can apply for an emergency authorisation if, in the course of an investigation of a relevant offence, he or she reasonably suspects that:

*(a) an imminent risk of serious violence to a person or substantial damage to property exists; and*

*(b) the use of a surveillance device is immediately necessary for the purpose of dealing with that risk; and*

*(c) the circumstances are so serious and the matter is of such urgency that the use of a surveillance device is warranted; and*

*(d) it is not practicable in the circumstances to apply for a surveillance device warrant.*

---

<sup>445</sup> *Surveillance Devices Act 2004* (Cth), s 14(5).

<sup>446</sup> *Surveillance Devices Act 2004* (Cth), s 14(6).

<sup>447</sup> *Surveillance Devices Act 2004* (Cth), s 15(1).

<sup>448</sup> *Surveillance Devices Act 2004* (Cth), s 16(2).

<sup>449</sup> *Surveillance Devices Act 2004* (Cth), s 16(1)(a).

<sup>450</sup> *Surveillance Devices Act 2004* (Cth), s 16(1)(c)-(d).

<sup>451</sup> *Surveillance Devices Act 2004* (Cth), s 6.

<sup>452</sup> *Surveillance Devices Act 2004* (Cth), s 6.

If the appropriate authorising officer is satisfied that there “are reasonable grounds for the suspicion founding the application,” he or she may give the authorisation.<sup>453</sup> Note that state law enforcement officers can only apply in respect of a relevant offence that is a Commonwealth offence.<sup>454</sup>

Section 29 deals with emergency authorisations in respect of recovery orders and is similar in operation to s 28. Recovery orders are orders made under the *Family Law Act 1975* (Cth) and consequently are outside the scope of this paper.

Under s 30(1), a law enforcement officer conducting an investigation into an offence against, inter alia, Pt IIIA of the *Crimes Act 1914* (Cth) or against Divs 72, 80, 101, 102, 103, 270 or ss 73.2 or 91.1 of the *Criminal Code* (Cth), who reasonably suspects that:

- the use of the surveillance device is immediately necessary to prevent the loss of any evidence relevant to that investigation; and
- the circumstances are so serious and the matter is of such urgency that the use of the surveillance device is warranted; and
- it is not practicable in the circumstances to apply for a surveillance device warrant

may apply to an appropriate authorising officer for an authorisation.<sup>455</sup> The appropriate authorising officer may give the authorisation if satisfied that an investigation is being conducted into the offence and that there “are reasonable grounds for the suspicion” entertained by the law enforcement officer.<sup>456</sup>

Applications under ss 28-30 “may be made orally, in writing or by telephone, fax, e-mail or any other means of communication.” A record of the authorisation must be made by the appropriate authorising officer.<sup>457</sup> An emergency authorisation may authorise anything that a surveillance device warrant may authorise.<sup>458</sup>

Within 48 hours of giving an authorisation the appropriate authorising officer must apply to have the authorisation approved by an eligible Judge or nominated AAT member.<sup>459</sup> The application:

*(a) must specify:*

*(i) the name of the applicant for the approval; and*

*(ii) the kind or kinds of surveillance device to which the emergency authorisation relates and, if a warrant is sought, the nature and duration of the warrant; and*

---

<sup>453</sup> *Surveillance Devices Act 2004* (Cth), s 28(4).

<sup>454</sup> *Surveillance Devices Act 2004* (Cth), s 28(3).

<sup>455</sup> *Surveillance Devices Act 2004* (Cth), s 30(1).

<sup>456</sup> *Surveillance Devices Act 2004* (Cth), s 30(3).

<sup>457</sup> *Surveillance Devices Act 2004* (Cth), s 31.

<sup>458</sup> *Surveillance Devices Act 2004* (Cth), s 32(2).

<sup>459</sup> *Surveillance Devices Act 2004* (Cth), s 33(1).

*(b) must be supported by an affidavit setting out the grounds on which the approval (and warrant, if any) is sought; and*

*(c) must be accompanied by a copy of the written record made under section 31 in relation to the emergency authorisation.<sup>460</sup>*

The eligible Judge or nominated AAT member may require further information before considering the application.<sup>461</sup>

Different matters must be considered by the eligible Judge or nominated AAT member depending on which section the authorisation was given under.

Where the authorisation was issued under s 28, the eligible Judge or nominated AAT member may approve the authorisation if satisfied that there were reasonable grounds to suspect that:

*(a) there was a risk of serious violence to a person or substantial damage to property; and*

*(b) using a surveillance device may have helped reduce the risk; and*

*(c) it was not practicable in the circumstances to apply for a surveillance device warrant.<sup>462</sup>*

In deciding this issue, the eligible Judge or nominated AAT member must, being mindful of the intrusive nature of a surveillance device, consider the following:

*(a) the nature of the risk of serious violence to a person or substantial damage to property;*

*(b) the extent to which issuing a surveillance device warrant would have helped reduce or avoid the risk;*

*(c) the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk;*

*(d) how much the use of alternative methods of investigation could have helped reduce or avoid the risk;*

*(e) how much the use of alternative methods of investigation would have prejudiced the safety of the person or property because of delay or for another reason;*

*(f) whether or not it was practicable in the circumstances to apply for a surveillance device warrant.<sup>463</sup>*

---

<sup>460</sup> Surveillance Devices Act 2004 (Cth), s 33(2).

<sup>461</sup> Surveillance Devices Act 2004 (Cth), s 33(3).

<sup>462</sup> Surveillance Devices Act 2004 (Cth), s 35(1).

<sup>463</sup> Surveillance Devices Act 2004 (Cth), s 34(1).

On the other hand, where the authorisation was issued under s 30, the eligible Judge or nominated AAT member may approve the authorisation if satisfied that:

- (a) *there were reasonable grounds to suspect that:*
  - (i) *there was a risk of loss of evidence; and*
  - (ii) *using the surveillance device may have helped reduce the risk; and*
- (b) *it was not practicable in the circumstances to apply for a surveillance device warrant.*<sup>464</sup>

In deciding this issue, the eligible Judge or nominated AAT member must, being mindful of the intrusive nature of a surveillance device, consider the following:

- (a) *the nature of the risk of the loss of evidence;*
- (b) *the extent to which issuing a surveillance device warrant would have helped reduce or avoid the risk;*
- (c) *the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk;*
- (d) *how much the use of alternative methods of investigation could have helped reduce or avoid the risk;*
- (e) *whether or not it was practicable in the circumstances to apply for a surveillance device warrant.*<sup>465</sup>

Where the eligible Judge or nominated AAT member approves the authorisation (regardless of what section it was issued under), he or she may issue a warrant for the continued use of the device as if the application for the approval was an application for a surveillance device warrant, or – if satisfied that since the authorisation the activity that required surveillance has ceased – order that use of the device cease.<sup>466</sup> Where the eligible Judge or nominated AAT member declines to approve the authorisation, he or she may order that use of the device cease, or – if satisfied that a surveillance device warrant is now justified even if it was not justified when the authorisation was given – issue a surveillance device warrant.<sup>467</sup>

#### **5.4.5 Surveillance Devices in NSW**

Surveillance device warrants, as such, are only available under Commonwealth law. The closest equivalent in NSW is the *Workplace Surveillance Act 2005* (NSW). That Act, however, exists primarily to regulate surveillance of employees at work and so is not immediately relevant to terrorism. Given that almost all specific terrorism offences exist under Commonwealth statutes, the *Surveillance Devices Act 2004*

---

<sup>464</sup> *Surveillance Devices Act 2004* (Cth), s 35(3).

<sup>465</sup> *Surveillance Devices Act 2004* (Cth), s 34(3).

<sup>466</sup> *Surveillance Devices Act 2004* (Cth), s 35(4).

<sup>467</sup> *Surveillance Devices Act 2004* (Cth), s 35(5).



(Cth) will be available for use by state law enforcement officers in relation to most of these offences. Where, however, the state law enforcement officer wishes to use a surveillance device in relation to a state offence, he or she will have to apply under the *Listening Devices Act 1984* (NSW) – which may or may not apply to the surveillance device in question (see above). Notably, s 3(1A) of the *Listening Devices Act 1984* (NSW) provides that:

*A thing is not precluded from being a listening device within the meaning of this Act merely because it is also capable of:*

*(a) recording or transmitting visual images (for example a video camera), or*

*(b) recording or transmitting its own position.*

## **5.5 Interception Warrants**

The *Telecommunications (Interception) Act 1979* (Cth) prohibits the interception of communications passing over a telecommunications system,<sup>468</sup> unless (inter alia) the interception is done pursuant to a warrant.<sup>469</sup>

### **5.5.1 Interpretation**

For the purposes of the *Telecommunications (Interception) Act 1979* (Cth),

*interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.*<sup>470</sup>

This has been interpreted to mean that the Act does not apply unless the interception occurs somewhere in a telecommunications system between the microphone in the handset of a telephone and the loudspeaker in the handset of another telephone.<sup>471</sup> This will include interceptions made by devices attached to the microphone or loudspeaker itself,<sup>472</sup> but not interceptions that are made by devices (such as tape recorders) that record the communication after it has left the loudspeaker.<sup>473</sup> These latter “interceptions” would be covered instead by the various listening device regimes.

It is important to remember that unlike the other warrants that have been examined so far in this paper, interception warrants typically do not authorise a trespass

---

<sup>468</sup> *Telecommunications (Interception) Act 1979* (Cth), s 7

<sup>469</sup> *Telecommunications (Interception) Act 1979* (Cth), s 7(2)(b).

<sup>470</sup> *Telecommunications (Interception) Act 1979* (Cth), s 6(1).

<sup>471</sup> *R v Giaccio* (1997) 93 A Crim R 462 at 468 per Cox J.

<sup>472</sup> *R v Migliorini* (1981) 38 ALR 356.

<sup>473</sup> *R v Giaccio* (1997) 93 A Crim R 462.

(although they may in some cases). For this reason, and in light of the language and structure of the *Telecommunications (Interceptions) Act 1979* (Cth), interception warrants have been construed less strictly than search warrants and listening device warrants. In *McCleary v DPP* (1998) 157 ALR 301, for instance, it was held that a failure to record on the warrant the date on which it was issued was not sufficient to invalidate the warrant. Moreover, as Justice Hall notes:

*It has been stated that the “decision” to issue [an interception] warrant is, for all practical purposes, an unreviewable in camera exercise of executive power to authorise a future clandestine gathering of information: Grollo v Palmer (1995) 184 CLR 348, at 367. In that case, Brennan CJ, Deane, Dawson and Toohey JJ pointed out that because of the secrecy necessarily involved in applying for and obtaining the issue of an interception warrant under the [Telecommunications (Interception) Act 1979 (Cth)], no records are kept which would permit judicial review of the judge’s “decision” to issue the warrant nor the reasons given for such a decision: at 367.<sup>474</sup>*

### 5.5.2 Application for an Interception Warrant

Part VI of the Act concerns warrants that authorise “agencies” to intercept telecommunications. An “agency” includes the AFP and the Australian Crime Commission,<sup>475</sup> as well as State agencies such as the NSW Police Force for whom declarations under s 34 are in force. An agency may apply to an “eligible Judge” or a “nominated AAT member” for a warrant in respect of a telecommunications service or a warrant in respect of a named person.<sup>476</sup> An “eligible Judge” is a Judge of a court created by the Commonwealth Parliament who has consented in writing and who the Minister has declared to be an eligible Judge.<sup>477</sup> Where the applicant is the chief officer of an agency, or someone authorised by the chief officer under s 40(3), they may apply for the warrant by telephone if necessary due to urgent circumstances.<sup>478</sup> Otherwise, the application must be in writing.<sup>479</sup>

A written application must:

- set out the name of the agency and of the applicant,<sup>480</sup>
- be accompanied by an affidavit setting out the facts and grounds upon which the application is based; and
- set out the period for which the warrant is sought and the reasons why such a period is necessary.<sup>481</sup>

The affidavit must also include:

---

<sup>474</sup> Hall, *Investigating Corruption*, p. 504.

<sup>475</sup> *Telecommunications (Interception) Act 1979* (Cth), s 5.

<sup>476</sup> *Telecommunications (Interception) Act 1979* (Cth), s 39(1).

<sup>477</sup> *Telecommunications (Interception) Act 1979* (Cth), s 6D.

<sup>478</sup> *Telecommunications (Interception) Act 1979* (Cth), s 40(2). If the information supplied in a telephone application is not subsequently sworn in an affidavit and given to the eligible Judge or nominated AAT member, the eligible Judge or nominated AAT member may revoke the warrant: *Telecommunications (Interception) Act 1979* (Cth), ss 51-52.

<sup>479</sup> *Telecommunications (Interception) Act 1979* (Cth), s 40(1).

<sup>480</sup> *Telecommunications (Interception) Act 1979* (Cth), s 41.

<sup>481</sup> *Telecommunications (Interception) Act 1979* (Cth), s 42(2)-(3).

- information about the number of warrants previously sought and issued in relation to the same subject;
- particulars of the use made by the agency of the interceptions made under those warrants;<sup>482</sup> and
- (if the application is for a named person warrant, as opposed to a telecommunications service warrant) - the name of the person and details (to the extent they are known by the chief officer) sufficient to identify the telecommunications services the person is using or is likely to use.<sup>483</sup>

The information that must be given in a telephone application is set out in s 43. The eligible Judge or nominated AAT member may require further information to be given in connection with either a written or a telephone application.<sup>484</sup>

### 5.5.3 Grounds for the Issue of an Interception Warrant

The matters of which an eligible Judge or nominated AAT member must be satisfied before issuing an interception warrant differ according to the type of offence in respect of which the warrant is sought. Interception warrants may be sought in relation to either class 1 or class 2 offences. Class 1 offences are particularly relevant to terrorist activities. Section 5(1) defines a class 1 offence to mean:

*(a) murder, or an offence of a kind equivalent to murder; or*

*(b) a kidnapping, or an offence of a kind equivalent to kidnapping; or*

...

*(ca) an offence constituted by conduct involving an act or acts of terrorism; or*

*(cb) an offence against Division 72, 101, 102 or 103 of the Criminal Code [i.e. most terrorism offences]; or*

*(d) an offence constituted by:*

*(i) aiding, abetting, counselling or procuring the commission of;*

*(ii) being, by act or omission, in any way, directly or indirectly, knowingly concerned in, or party to, the commission of; or*

*(iii) conspiring to commit;*

*an offence of the kind referred to in paragraph (a), (b), (c), (ca) or (cb); or*

*(e) an offence constituted by receiving or assisting a person who is, to the offender's knowledge, guilty of an offence of a kind referred to in paragraph*

<sup>482</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 42(4)(a)-(c) and ss 42(4A)(c)-(e).

<sup>483</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 42(4A)(a)-(b).

<sup>484</sup> *Telecommunications (Interception) Act 1979* (Cth), s 44.

(a), (b), (c), (ca) or (cb), in order to enable the person to escape punishment or to dispose of the proceeds of the offence.

Note that subs (ca) and (cb) above were inserted by the *Telecommunications Interception Legislation Amendment Act 2002* (Cth) and the *Telecommunications (Interception) Amendment Act 2004* (Cth), respectively. Class 2 offences include, amongst other offences, certain offences that are punishable by at least 7 years imprisonment, including specified types of offences that involve substantial planning and organisation.<sup>485</sup>

Telecommunications service warrants and named person warrants in relation to **class 1 offences** may be issued if the eligible Judge or nominated AAT member is satisfied, “on the basis of the information given to [them] under [Part VI] in connection with the application,”<sup>486</sup> that:

- 1) the application complies with the requirements set out above; and
- 2) in the case of a telephone application – it was necessary to make the application by telephone because of urgent circumstances; and
- 3) there are reasonable grounds for suspecting that a particular person is using, or is likely to use:
  - the service, in the case of a telecommunications service warrant; or
  - more than one service, in the case of a named person warrant; and
- 4) information that would be likely to be obtained by intercepting under a warrant communications made to or from:
  - the service; or
  - any service that the person is using or is likely to use;(as the case may be) would be likely to assist in connection with the investigation by the agency of a class 1 offence(s) in which the person is involved; and
- 5) some or all of the information referred to in the last point cannot appropriately be obtained by other methods, having regard to the use and availability of such methods, their effectiveness and whether they are likely to prejudice the investigation through delay or some other reason.<sup>487</sup>

Where the warrant is a telecommunications service warrant, it may be issued in relation to communications made to or from the particular service. Where the warrant is a named person warrant, it may be issued in relation to communications made to or from any telecommunications service that the person is using or is likely to use.

Where a warrant is sought in relation to a **class 2 offence**, the warrant may be issued if the eligible Judge or nominated AAT member is satisfied of the matters in points 1) to 4) above (except that references to class 1 offences should be read as

---

<sup>485</sup> *Telecommunications (Interception) Act 1979* (Cth), s 5D.

<sup>486</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 45 and 45A.

<sup>487</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 45(a)-(e) and 45A(a)-(e).

references to class 2 offences).<sup>488</sup> In addition, however, the eligible Judge or nominated AAT member must be satisfied that, having regard to the matters in s 46(2) or s 46A(2) (as the case may be) and to no other matters, they should authorise the communications to be intercepted.<sup>489</sup> The relevant matters to which the eligible judge or nominated AAT member must have regard are:

- how much the privacy of any person will be interfered with;
- the gravity of the conduct constituting the offence(s);
- how much the information likely to be obtained would assist in the investigation of the offence(s);
- the use and availability of other methods for obtaining the information, their effectiveness and whether they are likely to prejudice the investigation through delay or some other reason.<sup>490</sup>

None of the interception warrants considered above authorise the interception of any communications unless the Managing Director of the telecommunications carrier has been notified of the warrant under s 60(1), and unless the interception takes place as the result of the actions of an employee of the carrier and certain persons associated with the AFP.<sup>491</sup>

Where an agency can seek a telecommunications service warrant in relation to either a class 1 or a class 2 offence, the agency may instead apply for a warrant under s 48 which also authorises entry onto specified premises. In such a case, the affidavit accompanying the application (as well as containing the matters required by ss 45 or 46) must state why entry is necessary, as well as the number of s 48 warrants that have been applied for and issued in relation to the same premises. An eligible Judge or nominated AAT member may only issue such a warrant if the application includes these further matters, and only if the warrant would otherwise have been issuable under the telecommunications service warrant provisions (i.e. ss 45 and 46). Further, the warrant may not be issued unless the eligible Judge or nominated AAT member is satisfied on the basis of information given in connection with the application that:

*(i) for technical reasons connected with the nature or operation of the service or of a telecommunications system of which the service forms a part; or*

*(ii) ...execution of the warrant as a result of action taken by the employees of [a telecommunications] carrier might jeopardise security of the investigation by the agency of a serious offence in which a person to whom the application relates is involved;*

*it would be impracticable or inappropriate to intercept communications under a warrant in respect of the service otherwise than by use of equipment or a line installed on those premises.*<sup>492</sup>

---

<sup>488</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 46(1)(a)-(d) and ss 46A(1)(a)-(d).

<sup>489</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 46(1)(e) and ss 46A(1)(e).

<sup>490</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 46(2)(a)-(f) and ss 46A(2)(a)-(f).

<sup>491</sup> *Telecommunications (Interception) Act 1979* (Cth), s 47.

<sup>492</sup> *Telecommunications (Interception) Act 1979* (Cth), s 48(d).

If issued, such a warrant will authorise entry on the specified premises to install, maintain, use or recover the equipment or line, as well as the interception of communications by use of that equipment or line.<sup>493</sup>

Any interception warrant may specify conditions or restrictions relating to interceptions under the warrant.<sup>494</sup> The warrant must:

- be signed and set out in the form prescribed by the regulations,<sup>495</sup>
- set out the period for which it is to be in force, which may not exceed 90 days,<sup>496</sup> and
- include “short particulars of each serious offence [i.e. class 1 or class 2 offence, as the case may be] in relation to which the Judge or nominated AAT member issuing the warrant was satisfied” in accordance with the relevant section.<sup>497</sup>

A warrant authorising entry onto premises must state whether the entry is authorised to be effected at any time, or only during specified hours, and may authorise measures that the Judge or nominated AAT member is satisfied are necessary and reasonable for the purpose of effecting entry.<sup>498</sup>

#### **5.5.4 Interceptions that are not authorised by an eligible Judge or AAT member**

Pt V of the Act allows a member of a police force to request an employee of a telecommunications carrier to intercept a communication for the purposes of tracing the location of a caller. A police officer may make such a request where he or she is of the opinion that tracing the location of the caller “is likely to assist” in dealing with a prescribed type of emergency.<sup>499</sup> The police officer is only entitled to form such an opinion if he or she is a party to the communication, or has been informed by a party to the communication, and the party to the communication has formed an honest belief (based on information supplied by the caller and any other matter) that either of the following emergencies exist:

*(i) another person (whether or not the caller) is dying, is being seriously injured or has been seriously injured; [or]*

*(ii) another person (whether or not the caller) is likely to die or be seriously injured.<sup>500</sup>*

The request may only be made where the party to the communication does not know the location of the caller.<sup>501</sup>

---

<sup>493</sup> *Telecommunications (Interception) Act 1979* (Cth), s 48(4).

<sup>494</sup> *Telecommunications (Interception) Act 1979* (Cth), s 49(2).

<sup>495</sup> *Telecommunications (Interception) Act 1979* (Cth), s 49(1).

<sup>496</sup> *Telecommunications (Interception) Act 1979* (Cth), s 49(3).

<sup>497</sup> *Telecommunications (Interception) Act 1979* (Cth), s 49(7).

<sup>498</sup> *Telecommunications (Interception) Act 1979* (Cth), s 48(5).

<sup>499</sup> *Telecommunications (Interception) Act 1979* (Cth), s 30(2).

<sup>500</sup> *Telecommunications (Interception) Act 1979* (Cth), s 30(1)(b)(i)-(ii).

<sup>501</sup> *Telecommunications (Interception) Act 1979* (Cth), s 30(1)(c).

Part III of the Act deals with warrants sought by ASIO. Where, upon the request of the Director-General of Security, the Attorney-General is satisfied that a person is engaged in, is reasonably suspected by the Director-General to be engaged in, or is likely to engage in, activities prejudicial to security (“security” is given the same meaning as it has in the *ASIO Act 1979* (Cth) (see above)), then the Attorney-General may issue a telecommunications service warrant if satisfied that the person is using, or is likely to use, a telecommunications service and that the interception will, or is likely to, assist ASIO in “carrying out its function of obtaining intelligence relating to security.”<sup>502</sup> Where the Attorney-General is satisfied that relying on a telecommunications service warrant would be ineffective to obtain the intelligence, he or she may instead issue a named person warrant.<sup>503</sup> Both types of warrant may authorise entry onto premises for the purposes of “installing, maintaining, using or recovering any equipment used to intercept such communications”<sup>504</sup> and remain in force for up to 6 months<sup>505</sup> (note that warrants issued by eligible Judges or nominated AAT members only remain in force for up to 90 days<sup>506</sup>). The Director-General may issue an emergency warrant (which lasts up to 48 hours<sup>507</sup>) if satisfied that the facts would justify the issue of a warrant by the Attorney-General and that security will be, or is likely to be, seriously prejudiced if the interception does not commence before a warrant can be issued and made available by the Attorney-General.<sup>508</sup>

Part III also provides for warrants relating to foreign intelligence. Where the Director-General gives a notice in writing to the Attorney-General requesting a warrant, the Attorney-General may issue a telecommunications service warrant for the purpose of obtaining foreign intelligence relating to a matter specified in the notice if satisfied on the basis of advice received by the relevant Minister that the collection of the relevant foreign intelligence is important in relation to the defence of the Commonwealth or the conduct of the Commonwealth’s international affairs.<sup>509</sup> Where the Attorney-General is satisfied that relying on a telecommunications service warrant would be ineffective to obtain the intelligence, he or she may issue a named person warrant.<sup>510</sup> Where the Attorney-General is satisfied that relying on a named person warrant would be ineffective to obtain the intelligence, he or she may issue a warrant allowing the interception of *foreign* communications.<sup>511</sup> Warrants relating to foreign intelligence remain in force for up to 6 months.<sup>512</sup>

### 5.5.5 Uses to which intercepted evidence may be put

Part VII of the *Telecommunications (Interception) Act 1979* (Cth) deals with the uses to which intercepted evidence may be put. Section 63 states that – subject to exceptions - intercepted information, whether lawfully obtained or not, cannot be

---

<sup>502</sup> *Telecommunications (Interception) Act 1979* (Cth), s 9.

<sup>503</sup> *Telecommunications (Interception) Act 1979* (Cth), s 9A.

<sup>504</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 9(1) and 9(1A).

<sup>505</sup> *Telecommunications (Interception) Act 1979* (Cth), s 9B(3).

<sup>506</sup> *Telecommunications (Interception) Act 1979* (Cth), s 49(3).

<sup>507</sup> *Telecommunications (Interception) Act 1979* (Cth), s 10(3).

<sup>508</sup> *Telecommunications (Interception) Act 1979* (Cth), s 10(1)(d).

<sup>509</sup> *Telecommunications (Interception) Act 1979* (Cth), s 11A(1).

<sup>510</sup> *Telecommunications (Interception) Act 1979* (Cth), s 11B(1)(b)(iii).

<sup>511</sup> *Telecommunications (Interception) Act 1979* (Cth), s 11C(1)(b)(iii).

<sup>512</sup> *Telecommunications (Interception) Act 1979* (Cth), s 11D(2).

given in evidence. Evidence lawfully obtained under a warrant may be given in evidence in exempt proceedings,<sup>513</sup> which includes proceedings by way of a prosecution for a class 1 or class 2 offence.<sup>514</sup> Note that the list of exempt proceedings in s 5B is quite substantial. Where a communication has been intercepted by an agency under a warrant that is subject to an irregularity, information thereby obtained may be given in evidence if the court is satisfied that in all the circumstances the irregularity should be disregarded.<sup>515</sup> An irregularity is defined to mean:

*a defect or irregularity (other than a substantial defect or irregularity):*

*(a) in, or in connection with the issue of, a document purporting to be a warrant; or*

*(b) in connection with the execution of a warrant, or the purported execution of a document purporting to be a warrant.<sup>516</sup>*

Evidence that is inadmissible remains inadmissible notwithstanding Pt VII.<sup>517</sup>

---

<sup>513</sup> *Telecommunications (Interception) Act 1979* (Cth), s 74.

<sup>514</sup> *Telecommunications (Interception) Act 1979* (Cth), ss 5 and 5B.

<sup>515</sup> *Telecommunications (Interception) Act 1979* (Cth), s 75(1). The section also requires the court to be satisfied that but for the irregularity the interception would not have contravened s 7(1).

<sup>516</sup> *Telecommunications (Interception) Act 1979* (Cth), s 75(2).

<sup>517</sup> *Telecommunications (Interception) Act 1979* (Cth), s 78.



Table 2: Summary of Judicial Anti-terror Powers

Type of warrant/order	Contained in	Effect	Grounds/Test	Issuing authority
<b>Commonwealth</b>				
Detention Warrants	<i>Crimes Act 1914</i> , Pt IC, Div 2 (inserted by <i>Anti-terrorism Act 2004</i> ).	Allows investigation period to be extended up to 20 hours in respect of persons arrested for a terrorism offence	s 23DA.	Magistrate, bail justice, justice of the peace
Control Orders	<i>Criminal Code Act 1995</i> , Div 104 (inserted by <i>Anti-terrorism Act (No 2) 2005</i> )	Allows imposition of obligations, prohibitions and restrictions for the purpose of protecting the public from a terrorist act	s 104.4	Federal Court, Family Court, Federal Magistrates Court
Continued Preventative Detention Orders	<i>Criminal Code Act 1995</i> , Div 105 (inserted by <i>Anti-terrorism Act (No 2) 2005</i> )	Preventative detention up to 48 hours: <ul style="list-style-type: none"> <li>- prevent imminent terrorist act; or</li> <li>- preserve evidence of recent terrorist act.</li> </ul>	s 105.4	Eligible: Federal or Supreme Court judges, retired superior court judges with 5 years experience, Federal Magistrates, President/Deputy President of AAT
Prohibited Contact Orders	<i>Criminal Code Act 1995</i> , ss 105.14A-105.16 (inserted by <i>Anti-terrorism Act (No 2) 2005</i> )	Prohibits contact by person subject to continued preventative detention order with a specified person	s 105.14A	As above
Detention and Questioning Warrants	<i>ASIO Act 1979</i> , Pt III, Div 3 (inserted by <i>ASIO Legislation Amendment (Terrorism) Act 2003</i> )	Allows questioning of a person in order to obtain intelligence relating to a terrorist offence; and allows detention and questioning of a person if the person may alert others involved, may not appear, or may damage evidence	s 34C s 34D	Eligible Federal Judges or Federal Magistrates, and persons specified by the regulations as issuing authorities

<b>NSW</b>				
Covert search warrants	<i>Terrorism (Police Powers) Act 2002, Pt 3 (inserted by Terrorism Legislation Amendment (Warrants) Act 2005)</i>	Search warrant in respect of a terrorist act without notice to occupier/suspect	s 27C s 27K	Eligible Supreme Court Judges
Preventative Detention Orders	<i>Terrorism (Police Powers) Act 2002, Pt 2A (inserted by Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005)</i>	Preventative detention up to 14 days to: <ul style="list-style-type: none"> <li>- prevent imminent terrorist act; or</li> <li>- preserve evidence relating to recent terrorist act</li> </ul>	s 26D s 26I	The Supreme Court
Prohibited Contact Order	<i>Terrorism (Police Powers) Act 2002, s 26N (inserted by Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005)</i>	Prohibits contact by person subject to preventative detention order with a specified person	s 26N	The Supreme Court

## Chapter 6: Commonwealth Warrants and Orders: New Anti-terror Powers

### **6.1 Summary**

New judicial 'anti-terror' powers with regard to warrants and orders under Commonwealth legislation have been created by:

- the *ASIO Legislation Amendment (Terrorism) Act 2003* (Cth);
- the *Anti-terrorism Act 2004* (Cth);
- the *Anti-terrorism Act (No 2) 2005* (Cth);

The powers created by these Acts have been inserted into:

- the *Crimes Act 1914* (Cth);
- the *Criminal Code* (Cth); and
- the *ASIO Act 1979* (Cth).

### **6.2 Control Orders - Commonwealth**

The *Anti-terrorism Act (No 2) 2005* (Cth) inserts Division 104 into the *Criminal Code* (Cth), the object of which "is to allow obligations, prohibitions and restrictions to be imposed on a person by a control order for the purpose of protecting the public from a terrorist act."<sup>518</sup> It is important at this point to note that there is no NSW legislation that contains equivalent provisions. NSW courts and judges will not be asked to issue control orders.

Under Div 104, an "issuing court" (i.e. the Federal Court, the Family Court, or the Federal Magistrates Court<sup>519</sup>) may make interim control orders. Except when the case is urgent,<sup>520</sup> such an order may only be made on the request of a senior AFP member who has sought and obtained the Attorney-General's consent to the request.<sup>521</sup> Before making an order, the court may seek such further information as it requires.<sup>522</sup>

#### **6.2.1 Obligations, prohibitions and restrictions that a control order may impose – Commonwealth**

---

<sup>518</sup> *Criminal Code* (Cth), s 104.1.

<sup>519</sup> *Criminal Code* (Cth), s 100.1.

<sup>520</sup> See *Criminal Code* (Cth), Division 104, Subdivision C.

<sup>521</sup> *Criminal Code* (Cth), s 104.4(1)(a).

<sup>522</sup> *Criminal Code* (Cth), s 104.4(1)(b).

The obligations, prohibitions and restrictions that may be imposed on the subject of an order are wide and varied. They are:<sup>523</sup>

- (a) a prohibition or restriction on the person being at specified areas or places;*
- (b) a prohibition or restriction on the person leaving Australia;*
- (c) a requirement that the person remain at specified premises between specified times each day, or on specified days;*
- (d) a requirement that the person wear a tracking device;*
- (e) a prohibition or restriction on the person communicating or associating with specified individuals;*
- (f) a prohibition or restriction on the person accessing or using specified forms of telecommunication or other technology (including the Internet);*
- (g) a prohibition or restriction on the person possessing or using specified articles or substances;*
- (h) a prohibition or restriction on the person carrying out specified activities (including in respect of his or her work or occupation);*
- (i) a requirement that the person report to specified persons at specified times and places;*
- (j) a requirement that the person allow himself or herself to be photographed;*
- (k) a requirement that the person allow impressions of his or her fingerprints to be taken;*
- (l) a requirement that the person participate in specified counselling or education [but only if the person agrees to participate: s 104.5(6)].*

### **6.2.2 Grounds for the issue of an interim control order - Commonwealth**

The court may issue an interim order if satisfied on the balance of probabilities that:

- the making of the order would substantially assist in preventing a terrorist act (s 104.4(1)(c)(i)); or that the subject of the order has provided training to, or received training from, a terrorist organisation that has been specified by the Governor-General as a terrorist organisation (s 104.4(1)(c)(ii)); and
- each of the obligations, prohibitions and restrictions to be imposed on the person by the order is reasonably necessary, and reasonably appropriate and adapted, for the purpose of protecting the public from a terrorist act (s 104.4(1)(d)). In determining this latter requirement, the court must take into

---

<sup>523</sup> *Criminal Code (Cth)*, s 104.5(3).

account the impact of the obligation on the person's circumstances, including their financial and personal circumstances.<sup>524</sup> An obligation that does not meet this requirement may be excluded from any subsequent order.<sup>525</sup>

### 6.2.3 Terms of an interim control order - Commonwealth

An interim control order must state:

- the court's satisfaction as to the matters in ss 104.4(1)(c)-(d);
- the name of the subject;
- all of the obligations that are to be imposed;
- that the order is not in force until served personally on the subject;
- the period during which the order is in force (which must be no longer than 12 months after it is made); and
- that the person's lawyer may attend a specified place in order to obtain a copy of the order.<sup>526</sup>

In addition, the order must set out a summary of the grounds on which it is made,<sup>527</sup> and it must:

*specify a day on which the person may attend the court for the court to:*

*(i) confirm (with or without variation) the interim control order; or*

*(ii) declare the interim control order to be valid; or*

*(iii) revoke the interim control order.<sup>528</sup>*

This day must be as soon as practicable but not less than 72 hours after the order is made.<sup>529</sup>

### 6.2.4 Confirmation of an interim control order - Commonwealth

Once an interim control order has been issued, the following is to occur::

- At least 48 hours before the specified day, the senior AFP officer who made the request for the interim order may elect to confirm the interim order.<sup>530</sup>
- If the senior AFP member elects not to confirm the order, the interim order ceases to have effect.<sup>531</sup>

---

<sup>524</sup> *Criminal Code* (Cth), s 104.4(2).

<sup>525</sup> *Criminal Code* (Cth), s 104.4(3).

<sup>526</sup> *Criminal Code* (Cth), s 104.5(1)

<sup>527</sup> *Criminal Code* (Cth), s 104.5(1)(h).

<sup>528</sup> *Criminal Code* (Cth), s 104.5(1)(e).

<sup>529</sup> *Criminal Code* (Cth), s 104.5(1A).

<sup>530</sup> *Criminal Code* (Cth), s 104.12A.

<sup>531</sup> *Criminal Code* (Cth), s 104.12A(4).

- If an election to confirm is made, the matter proceeds to court on the specified day.
- The subject or their representative(s), as well as the senior AFP member and one or more other AFP members, may adduce evidence or make submissions in relation to the confirmation of the order.<sup>532</sup>
- In addition to such evidence or submissions, the court must consider the original request for an interim control order before taking any action in relation to the confirmation of the order.<sup>533</sup>
- **If the subject or their representative attend court on the specified day, the court may:**
  - declare the order void if satisfied that there were no grounds for making the interim order at the time it was made;
  - revoke the order if not satisfied as to the matters in s 104.4(1)(c);
  - confirm the order if satisfied as to the matters in ss 104.4(1)(c) and (d); or
  - confirm and vary the order if satisfied as to the matters in s 104.4(1)(c) but not as to the matters in s 104.4(1)(d).<sup>534</sup>
- If the subject or their representative do not attend court on the specified day, then the court may confirm the order without variation if satisfied on the balance of probabilities that the order was properly served on the subject of the order.<sup>535</sup>
- **When an interim order is confirmed, the court must make a corresponding order that states the court's satisfaction as to:**
  - the matters in ss 104.4(1)(c) and (d);
  - the name of the subject;
  - the obligations (etc) that are imposed by the order;
  - the period in which the order is in force (which can be no longer than 12 months after the day on which the interim order was made); and
  - that the person's lawyer may attend a specified place in order to obtain a copy of the confirmed order.<sup>536</sup>

Note that an order in respect of someone aged 16 to 18 cannot remain in force for more than 3 months after the initial control order is made.<sup>537</sup> The Commissioner of the AFP may apply to an issuing court to vary a confirmed control order by adding

---

<sup>532</sup> *Criminal Code* (Cth), s 104.14(1)

<sup>533</sup> *Criminal Code* (Cth), s 104.14(3)

<sup>534</sup> *Criminal Code* (Cth), ss 104.14(5)-(6).

<sup>535</sup> *Criminal Code* (Cth), s 104.14(4).

<sup>536</sup> *Criminal Code* (Cth), s 104.16(1).

<sup>537</sup> *Criminal Code* (Cth), s 104.28(2).

further obligations, prohibitions and restrictions.<sup>538</sup> It is an offence punishable by 5 years imprisonment to contravene a control order.<sup>539</sup>

### **6.3 Detention and Questioning Warrants: Warrants for the Purpose of Interrogation by ASIO - Commonwealth**

#### **6.3.1 Introduction**

The availability of detention and questioning warrants is perhaps the most controversial aspect of the new terrorism laws. These warrants allow for the detention without charge of certain persons to allow ASIO to interrogate them. These types of powers raise fundamental questions about Australian society. In an article titled "Terrorism and the Democratic Response 2004," Justice Michael Kirby quotes Stevens J of the US Supreme Court in *Padilla v Rumsfeld*:<sup>540</sup>

*Unrestrained Executive detention for the purpose of investigating and preventing subversive activity is the hallmark of the Star Chamber...[I]f this nation is to remain true to its ideals symbolised by its flag, it must not wield the tools of tyrants even to resist an assault by the forces of tyranny.*<sup>541</sup>

Article 9(1) of the *International Covenant on Civil and Political Rights* states that "no one shall be subjected to arbitrary arrest and detention." The UN Human Rights Committee has said that "'arbitrariness' is not to be equated with 'against the law,' but must be interpreted more broadly to include elements of inappropriateness, injustice and lack of predictability."<sup>542</sup> Whether justified or not, these are all criticisms that have been levelled at the legislation.

#### **6.3.2 Australian Security Intelligence Organisation Act 1979 (Cth)**

Division 3 of Pt III of the *Australian Security Intelligence Organisation Act 1979* (Cth) ("Special powers relating to terrorism offences") was inserted by the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* (Cth). It is useful here to adopt the analysis of the Parliamentary Joint Committee on ASIO, ASIS and DSD. The Joint Committee briefly describe the operation of Division 3 of Pt III in these terms [note: references to sections in the *ASIO Act 1979* (Cth) have been added in square brackets]:

*1.4 The legislation enables ASIO to obtain a warrant from an 'issuing authority' for the questioning of a person before a 'prescribed authority' in order to obtain intelligence that is important in relation to a terrorism offence [ss 34C(3)(a), 34C(4) and 34D(1)]. A warrant may also provide for a person to be detained for questioning if there are reasonable grounds for believing that the person may alert someone involved in a terrorism offence, may not appear*

<sup>538</sup> *Criminal Code* (Cth), Division 104, Subdivision F.

<sup>539</sup> *Criminal Code* (Cth), s 104.27.

<sup>540</sup> *Padilla v Rumsfeld*, 124 SCt 2711, 2735 (2004).

<sup>541</sup> Quoted in Kirby, "Terrorism" at 236.

<sup>542</sup> *Hugo van Alphen v The Netherlands*, Communication No 305/1988 at [5.8], UN Doc CCPR/C/39/D/305/1988. See Emerton, "Paving the Way" at 2-3.

*before the prescribed authority, or may destroy or damage evidence [ss 34C(3)(c), 34C(4) and 34D(1)].*

*1.5 Warrants for questioning and detention have no effect in relation to persons under 16 years of age [s 34NA(1)] and may only be issued in relation to persons aged between 16 and 18 years if it is likely that the child will commit, is committing, or has committed a terrorism offence [s 34NA(4)].*

*1.6 The subject of a warrant cannot be detained [continuously] for more than 168 hours [s 34HC]. They can be questioned under a warrant for no more than a total of 24 hours [s 34HB(6)] and once they have been questioned for this period of time they must be released [s 34HB(7)(c)] – unless they have used an interpreter, in which case they can be questioned for up to 48 hours [s 34HB(11)]. Questioning can occur in blocks of up to eight hours [s 34HB(1)] – note, however, that on its face the legislation allows continuous questioning for up to 24 hours if the prescribed authority permits] and two hours for persons aged between 16 and 18 years [s 34NA(6)(b)(ii)]. There appears to be some confusion in the Act as to the time limit of 168 hours...and the length of the warrant, which is 28 days [s 34D(6)(b)]...*

*1.7 Questioning is conducted in the presence of a 'prescribed authority' [s 34D(2)]. 'Prescribed authorities' are initially drawn from the ranks of [consenting] former superior court judges. If there are insufficient former judges, then serving [State and Territory] superior court [and District Court] judges can be appointed [as long as they consent, and have served as a judge for at least 5 years]. If there are insufficient serving judges then a President or Deputy President of the Administrative Appeals Tribunal (AAT) can be appointed, so long as that person holds legal qualifications [and consents to the appointment][s 34B]...*

*1.11 ...[T]he ASIO Legislation Amendment Act 2003 also introduced secrecy provisions into the legislation which prohibit [s 34VAA]:*

*(i) while a warrant is in force (up to 28 days), disclosure of the existence of the warrant and any fact relating to the content of the warrant or to the questioning or detention of a person under the warrant; and*

*(ii) while a warrant is in force and during the period of two years after the expiry of the warrant, disclosure of any ASIO operational information acquired as a direct result of the issue of a warrant, unless the disclosure is permitted under another provision.*

*1.12 The penalty for infringing these provisions is a maximum of 5 years imprisonment.<sup>543</sup>*

---

<sup>543</sup> Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD), *ASIO's Questioning and Detention Powers: Review of the operation, effectiveness and implications of Division 3 of Part III in the Australian Security Intelligence Organisation Act 1979*, Canberra, 2005 (hereafter *ASIO's Questioning and Detention Powers*), pp. 2-3.



A “terrorism offence” is an offence against Div 72 or Pt 5.3 of the *Criminal Code* (Cth). Operational information is information that ASIO has or had, a source of information that ASIO has or had, or an operational capability, method or plan of ASIO.<sup>544</sup> One commentator has pointed out that the disclosure offences can be made out even where the warrant under which a person is questioned/detained is invalid or improperly executed.<sup>545</sup> Moreover, the disclosure offences prevent a person who has been the subject of a warrant from defending themselves in the media in the face of leaks from ASIO itself.<sup>546</sup>

### 6.3.3 Issuing a detention and questioning warrant – Commonwealth

An “issuing authority” is a consenting Federal Magistrate or Federal Judge who has been appointed by the Minister, or a class of persons specified by the regulations.<sup>547</sup>

An issuing authority may issue a warrant where:

*(a) the Director-General has requested it in accordance with subsection 34C(4); and*

*(b) the issuing authority is satisfied that there are reasonable grounds for believing that the warrant will substantially assist the collection of intelligence that is important in relation to a terrorism offence.*<sup>548</sup>

The warrant sought may be a questioning-only warrant or a detention and questioning warrant (which we shall hereafter call an “investigation warrant” to avoid any confusion with “detention warrants” and “preventative detention orders”).

Before a warrant is submitted to an issuing authority by the Director-General, the terms of the warrant must be consented to by the Minister.<sup>549</sup> An issuing authority has no power to alter a warrant, but must either accept or reject it on the terms that it is consented to.<sup>550</sup> The issuing authority’s role is limited. There is

*no requirement that the issuing authority take account of the efficacy of relying on other methods of collecting the intelligence, in respect of a questioning-only or [an investigation] warrant. Nor is there any requirement that the issuing authority be satisfied of the additional grounds necessary to trigger [an investigation warrant].*<sup>551</sup>

The role thus created for the issuing authority has been criticised as being too narrow.<sup>552</sup>

---

<sup>544</sup> *ASIO Act 1979* (Cth), s 34VAA(5).

<sup>545</sup> Hocking, J, “National Security and Democratic Rights: Australian Terror Laws” (2004) 16 *The Sydney Papers* 89 (hereafter “National Security”) at 91.

<sup>546</sup> PJCAAD, *ASIO’s Questioning and Detention Powers*, p. 23.

<sup>547</sup> *ASIO Act 1979* (Cth), s 34AB.

<sup>548</sup> *ASIO Act 1979* (Cth), s 34D.

<sup>549</sup> *ASIO Act 1979* (Cth), s 34C(4).

<sup>550</sup> *ASIO Act 1979* (Cth), ss 34D(2)-(5).

<sup>551</sup> PJCAAD, *ASIO’s Questioning and Detention Powers*, p. 35.

<sup>552</sup> *Ibid*, pp. 35-36.

### 6.3.4 Criticisms of the process for the issue of questioning and detention warrants

Other criticisms of the legislation are not hard to come by. Jenny Hocking, author of *Terror Laws: ASIO, Counter-Terrorism and the Threat to Democracy*, writes that

*Australia remains the only liberal-democratic nation to have proposed the detention and interrogation of non-suspects in this way, and to have introduced such stringent secrecy provisions in relation to public disclosure of its implementation.*<sup>553</sup>

On the other hand, Dennis Richardson, the Director-General of ASIO, argues that in many cases “the capacity to obtain evidence sufficient to meet legal standards [was] beyond reach” before Div 3 of Pt III was inserted, and that it is quite “possible for someone to pose a threat to security without necessarily being in breach of the law.”<sup>554</sup> The debate is a live one, and it will no doubt continue.

It should also be noted that the number of “terrorism offences” in the *Criminal Code* (Cth) has increased since the legislation creating Division 3 of Pt III was introduced into Parliament in 2002. This has arguably given the *ASIO Act 1979* (Cth) a wider scope and operation than was originally envisaged.<sup>555</sup>

### **6.4 Preventative Detention Orders – Commonwealth**

The *Anti-terrorism Act (No 2) 2005* (Cth) sets up a preventative detention scheme under Division 105 of the *Criminal Code* (Cth). The scheme is similar in many respects to Pt 2A of the *Terrorism (Police Powers) Act 2002* (NSW) (see below), but there are some significant differences. These differences were pointed out during the second reading speech of the *Terrorism (Police Powers) Amendment (Preventative Detention) Bill 2005* (NSW) (17 November 2005, from p. 20008), and can be summarised as follows:

- the Commonwealth scheme is administrative (i.e. orders are not made by judges acting as judges – they are initially made by senior AFP members and may be continued by issuing authorities who are acting in a personal capacity), whereas the NSW scheme is judicial;
- the Commonwealth scheme can only operate to detain a person for 48 hours (as opposed to 14 days in NSW); and
- the Commonwealth scheme contains disclosure offences punishable by 5 years imprisonment directed at the subject (s 105.41(1)) or their lawyer (s 105.41(2)) that are designed to keep the preventative detention order a secret.

---

<sup>553</sup> Hocking, “National Security” at 89.

<sup>554</sup> Richardson quoted in: Uhlmann, C, “Containing the threat within” (2005) (23) *About the House* 33 at 34.

<sup>555</sup> PJCAAD, *ASIO’s Questioning and Detention Powers*, p. 33.

#### **6.4.1 Initial preventative detention orders - Commonwealth**

Under the Commonwealth scheme, an AFP member cannot apply for, and an issuing authority cannot issue, a preventative detention order unless the person is satisfied of the matters set out in either s 105.4(4) or s 105.4(6). Subsections 105.4(4)-(6) provide that:

*(4) A person meets the requirements of this subsection if the person is satisfied that:*

*(a) there are reasonable grounds to suspect that the subject:*

*(i) will engage in a terrorist act; or*

*(ii) possesses a thing that is connected with the preparation for, or the engagement of a person in, a terrorist act; or*

*(iii) has done an act in preparation for, or planning, a terrorist act; and*

*(b) making the order would substantially assist in preventing a terrorist act occurring; and*

*(c) detaining the subject for the period for which the person is to be detained under the order is reasonably necessary for the purpose referred to in paragraph (b).*

*(5) A terrorist act referred to in subsection (4):*

*(a) must be one that is imminent; and*

*(b) must be one that is expected to occur, in any event, at some time in the next 14 days.*

*(6) A person meets the requirements of this subsection if the person is satisfied that:*

*(a) a terrorist act has occurred within the last 28 days; and*

*(b) it is necessary to detain the subject to preserve evidence of, or relating to, the terrorist act; and*

*(c) detaining the subject for the period for which the person is to be detained under the order is reasonably necessary for the purpose referred to in paragraph (b).*

These subsections are not materially different to ss 26D(1) and (2) of the *Terrorism (Police Powers) Act 2002* (NSW), which are set out below. An order cannot be made against a person who is under 16.<sup>556</sup>

Where satisfied of the requisite matters, an AFP member may apply for an initial preventative detention order. Senior AFP members (i.e. the Commissioner, Deputy Commissioner, or a member of or above the rank of superintendent) are issuing authorities in relation to initial preventative detention orders.<sup>557</sup> A person may only be detained for up to 24 hours under such an order.<sup>558</sup>

#### **6.4.2 Process for continuing an ‘initial preventative detention order’ – Commonwealth**

An issuing authority in respect of a continued preventative detention order may be appointed by the Minister. The Minister may only appoint:

- (a) *a person who is a judge of a State or Territory Supreme Court; or*
- (b) *a person who is a Judge; or*
- (c) *a person who is a Federal Magistrate; or*
- (d) *a person who:*
  - (i) *has served as a judge in one or more superior courts for a period of 5 years; and*
  - (ii) *no longer holds a commission as a judge of a superior court; or*
- (e) *a person who:*
  - (i) *holds an appointment to the Administrative Appeals Tribunal as President or Deputy President; and*
  - (ii) *is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or Territory; and*
  - (iii) *has been enrolled for at least 5 years, as long as they have consented in writing to the appointment and the consent is in force.*<sup>559</sup>

The Minister can only appoint such a person if they have consented in writing to the appointment and the consent is in force.<sup>560</sup>

The issue of an initial preventative detention order sets the following process in train:

---

<sup>556</sup> *Criminal Code* (Cth), s 105.5(1).

<sup>557</sup> *Criminal Code* (Cth), s 100.1(1).

<sup>558</sup> *Criminal Code* (Cth), s 105.8(5) and s 105.10(5).

<sup>559</sup> *Criminal Code* (Cth), s 105.2(1).

<sup>560</sup> *Criminal Code* (Cth), s 105.2(2).

- An AFP member who is satisfied of the requisite matters may apply for a continued preventative detention order in relation to the subject of the initial preventative detention order in relation to the same terrorist act;<sup>561</sup>
- An application for a continued preventative detention order must be sworn or affirmed<sup>562</sup> and must contain any material that the subject of the initial preventative detention order wishes to put before the issuing authority;<sup>563</sup>
- The application must:

*(a) be made in writing; and*

*(b) set out the facts and other grounds on which the AFP member considers that the order should be made; and*

*(c) specify the period for which the person is to continue to be detained under the order and set out the facts and other grounds on which the AFP member considers that the person should continue to be detained for that period; and*

*(d) set out the information (if any) that the applicant has about the person's age; and...*

*(g) set out a summary of the grounds on which the AFP member considers that the order should be made.<sup>564</sup>*

Subsections (e) and (f) require the application to include information in respect of prior preventative detention order applications, control orders and orders under corresponding State preventative detention laws.

As long as an initial preventative detention order is in force and the subject has been taken into custody under the order,<sup>565</sup> the issuing authority may issue a continued preventative detention order if satisfied of the requisite matters (i.e. the matters in ss 105.4(4) or 105.4(6)).

### **6.4.3 Terms and operation of a preventative detention order - Commonwealth**

The preventative detention order must:

- be in writing;<sup>566</sup>
- set out the name of the subject;
- the date and time when the order is made;
- a summary of the grounds on which the order is made; and
- the period during which the person may be detained under the order.<sup>567</sup>

<sup>561</sup> *Criminal Code (Cth)*, s 105.11(1).

<sup>562</sup> *Criminal Code (Cth)*, s 105.11(4).

<sup>563</sup> *Criminal Code (Cth)*, s 105.11(5).

<sup>564</sup> *Criminal Code (Cth)*, s 105.11(2).

<sup>565</sup> *Criminal Code (Cth)*, s 105.12(1).

<sup>566</sup> *Criminal Code (Cth)*, s 105.12(4).

The period of time beginning when a person is first taken into custody under an initial preventative detention order and finishing at the end of the period specified in a continued preventative detention order may not exceed 48 hours.<sup>568</sup>

#### 6.4.4 Prohibited contact orders - Commonwealth

An AFP member who applies for a preventative detention order may also apply for a prohibited contact order.<sup>569</sup> Where a preventative detention order is in force, any AFP member may apply for a prohibited contact order.<sup>570</sup> The issuing authority to whom the AFP member applies will differ according to what type of preventative detention order (i.e. initial or continued) is being sought or is in force. Before an AFP member applies for, or an issuing authority issues, a prohibited contact order, they must be satisfied that the order is reasonably necessary:

- (a) to avoid a risk to action being taken to prevent a terrorist act occurring; or*
- (b) to prevent serious harm to a person; or*
- (c) to preserve evidence of, or relating to, a terrorist act; or*
- (d) to prevent interference with the gathering of information about:*
  - (i) a terrorist act; or*
  - (ii) the preparation for, or planning of, a terrorist act; or*
- (e) to avoid a risk to:*
  - (i) the arrest of a person who is suspected of having committed an offence against this Part [i.e. Part 5.3]; or*
  - (ii) the taking into custody of a person in relation to whom a preventative detention order is in force, or in relation to whom a preventative detention order is likely to be made; or*
  - (iii) the service on a person of a control order.<sup>571</sup>*

As is the case with preventative detention orders,<sup>572</sup> an issuing authority can refuse to make a prohibited contact order if the applicant does not provide further information that the issuing authority requests.<sup>573</sup>

---

<sup>567</sup> *Criminal Code (Cth)*, s 105.12(6).

<sup>568</sup> *Criminal Code (Cth)*, s 105.12(5).

<sup>569</sup> *Criminal Code (Cth)*, s 105.15(1).

<sup>570</sup> *Criminal Code (Cth)*, s 105.16(1).

<sup>571</sup> *Criminal Code (Cth)*, s 105.14A(4).

<sup>572</sup> *Criminal Code (Cth)*, s 105.4(7).

<sup>573</sup> *Criminal Code (Cth)*, s 105.14A(5).

## Chapter 7: New South Wales Warrants and Orders: New Anti-terror Powers

New judicial ‘anti-terror’ powers with regard to warrants and orders under New South Wales legislation have been created by:

- the *Terrorism (Police Powers) Act 2002* (NSW);
- the *Terrorism Legislation Amendment (Warrants) Act 2005* (NSW); and
- the *Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005* (NSW).

All of the relevant powers have been inserted into the *Terrorism (Police Powers) Act 2002* (NSW).

### **7.1 Special NSW Anti-terror Special Police Outside Judicial Oversight**

Part 2 of the *Terrorism (Police Powers) Act 2002* (NSW) allows police officers to use “special powers” against “authorised” targets. The NSW<sup>574</sup> Commissioner of Police, a Deputy Commissioner of Police or, when they are not available, a police officer above the rank of superintendent, can give an authorisation<sup>575</sup> targeting particular persons, vehicles or areas.<sup>576</sup> Oddly, an authorisation may only be given with the concurrence of the Police Minister (unless he or she cannot be contacted at the time).<sup>577</sup> The police officer giving the authorisation must be satisfied that there are reasonable grounds for believing that a terrorist act (as defined above) has been committed,<sup>578</sup> or that there is an imminent threat of such an act occurring,<sup>579</sup> and that the exercise of the special powers that are enlivened by the authorisation will substantially assist in preventing the terrorist act,<sup>580</sup> or in apprehending the persons responsible.<sup>581</sup> An authorisation in respect of a terrorist act that *has* occurred may not exceed 24 hours (extendable to 48 hours) while an authorisation in respect of a terrorist act that is about to occur may not exceed 7 days (extendable to 14 days).<sup>582</sup> The Act contains a privative clause which purports to protect an authorisation from legal challenge. Section 13(1) provides that:

*An authorisation (and any decision of the Police Minister under this Division with respect to the authorisation) may not be challenged, reviewed, quashed or called into question on any grounds whatsoever before any court, tribunal, body or person in any legal proceedings, or restrained, removed or otherwise*

---

<sup>574</sup> Note that ss 24 and 25 allow the special powers provisions of the *Terrorism (Police Powers) Act 2002* (NSW) to be extended to members of the AFP and the police forces of other States and Territories.

<sup>575</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 8.

<sup>576</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 7.

<sup>577</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 9.

<sup>578</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 6(a).

<sup>579</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 5(a).

<sup>580</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 6(b).

<sup>581</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 5(b).

<sup>582</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 11.

*affected by proceedings in the nature of prohibition or mandamus.*

“Legal proceedings” are defined to include any investigation into police or other conduct under any Act except the *Police Integrity Commission Act 1996* (NSW).<sup>583</sup> Once an authorisation has been given, special police powers include:

- special powers to obtain the disclosure of a person’s identity,<sup>584</sup> and
- special powers of search, entry and seizure.<sup>585</sup>

Where the target is a person of or above the age of 10, that person may be strip searched in certain circumstances.<sup>586</sup>

## **7.2 Covert Search Warrants – NSW**

### **7.2.1 Covert Search Warrants – NSW**

In 2005 a new Part (“Part 3 – Covert search warrants”) was inserted into the *Terrorism (Police Powers) Act 2002* (NSW) by the *Terrorism Legislation Amendment (Warrants) Act 2005* (NSW). The Part allows search warrants in respect of a terrorist act to be issued by an eligible Judge and executed without the knowledge of the occupier. In Part 3, a reference to a terrorist act includes a reference to an offence against s 310J of the *Crimes Act 1900* (NSW) (membership of a terrorist organisation).<sup>587</sup> It does not matter whether or not the act has been, is being, or is likely to be committed in NSW.<sup>588</sup> An eligible Judge is a Judge of the Supreme Court who has given their consent in writing and who the Attorney-General has declared to be an eligible Judge.<sup>589</sup> The Attorney-General may revoke a declaration.<sup>590</sup>

### **7.2.2 Application for a Covert Search Warrant – NSW**

The Commissioner of Police<sup>591</sup> or his or her proper delegate<sup>592</sup> may authorise a police officer to apply for a covert search warrant if they suspect or believe on reasonable grounds:

*(a) that a terrorist act has been, is being, or is likely to be committed, and*

*(b) that the entry to and search of premises will substantially assist in responding to or preventing the terrorist act, and*

*(c) that it is necessary for the entry and search of those premises to be conducted without the knowledge of any occupier of the premises.*<sup>593</sup>

---

<sup>583</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 13(2).

<sup>584</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 16.

<sup>585</sup> *Terrorism (Police Powers) Act 2002* (NSW), ss 17-19 and 20.

<sup>586</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 17 and Sch 1, ss 4, 6 and 7.

<sup>587</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27A.

<sup>588</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 4A.

<sup>589</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27B.

<sup>590</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27B(6).

<sup>591</sup> Or the Crime Commissioner in the case of applications made by his or her staff members: *Terrorism (Police Powers) Act 2002* (NSW), s 27E.

<sup>592</sup> Delegations are regulated by *Terrorism (Police Powers) Act 2002* (NSW), s 27E.

<sup>593</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27C.



A police officer who has received an authorisation may only apply to an “eligible Judge” for a covert search warrant if he or she suspects or believes on reasonable grounds the same things.<sup>594</sup>

There are aspects of the application process for covert search warrants that are the same as for search warrants under the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW). The provisions with respect to applying by person or telephone<sup>595</sup> are not materially different to those contained in that Act. The provisions concerning the making of records are the same except that the *Terrorism (Police Powers) Act 2002* (NSW) requires the eligible judge to record the grounds relied on to justify a refusal to issue a warrant as well as the grounds relied on to justify the issue of a warrant.<sup>596</sup> The *Terrorism (Police Powers) Regulation 2005* (NSW) makes provision as to which documents must be kept after a covert search warrant is issued and how, if and when they can be inspected by the occupiers of the premises.<sup>597</sup> There is also a requirement to prepare and furnish an occupier’s notice, but under the *Terrorism (Police Powers) Act 2002* (NSW) the notice will not be given until after the warrant has been executed.<sup>598</sup> In some cases, a notice might not be furnished for over two years after the execution of the warrant.<sup>599</sup>

**An application for a covert search warrant must include:**

- (a) *the name of the applicant and details of the authorisation...*
- (b) *the address or other description of the subject premises,*
- (c) *particulars of the grounds on which the application is based,*
- (d) *the name of the following persons:*
  - (i) *any person believed to be knowingly concerned in the commission of the terrorist act in respect of which the application is made,*
  - (ii) *if no such person is an occupier of the subject premises any occupier (if known) of those premises,*
- (e) *if it is proposed that premises adjoining or providing access to the subject premises be entered for the purpose of entering the subject premises the address or other description of the premises that adjoin or provide such access and particulars of the grounds on which entry to those premises is required,*
- (f) *the powers that are proposed to be exercised on entry to the subject premises,*

---

<sup>594</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27G.

<sup>595</sup> *Terrorism (Police Powers) Act 2002* (NSW), ss 27H-27I.

<sup>596</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27L.

<sup>597</sup> *Terrorism (Police Powers) Regulation 2005* (NSW), regs 5-6.

<sup>598</sup> *Terrorism (Police Powers) Act 2002* (NSW), ss 27U-27V.

<sup>599</sup> Combined effect of ss 27U(3) and 27(9)(b) of the *Terrorism (Police Powers) Act 2002* (NSW).

*(g) a description of the kinds of things that are proposed to be searched for, seized, placed in substitution for a seized thing, copied, photographed, recorded, operated, printed or tested,*

*(h) if a previous application for the same warrant was refused details of the refusal and any additional information provided as required by section 27M,*

*(i) details of any covert search warrant that has previously been issued in respect of the subject premises,*

*(j) any other information required by the regulations.<sup>600</sup>*

The eligible Judge may require the applicant to provide further information.<sup>601</sup>

### **7.2.3 Grounds for the issue of a Covert Search Warrant – NSW**

Upon application, an eligible Judge may issue a covert search warrant if “satisfied that there are reasonable grounds for doing so.”<sup>602</sup> In determining whether there are reasonable grounds, the eligible Judge is to consider the 8 matters listed in s 27K(2). These are

*(a) the reliability of the information on which the application is based, including the nature of the source of the information,*

*(b) whether there is a connection between the terrorist act in respect of which the application has been made and the kinds of things that are proposed to be searched for, seized, placed in substitution for a seized thing, copied, photographed, recorded, operated, printed or tested,*

*(c) the nature and gravity of the terrorist act,*

*(d) the extent to which the exercise of powers under the warrant would assist in the prevention of, or response to, the terrorist act,*

*(e) alternative means of obtaining the information sought to be obtained,*

*(f) the extent to which the privacy of a person who is not believed to be knowingly concerned in the commission of the terrorist act is likely to be affected if the warrant is issued,*

*(g) if it is proposed that premises adjoining or providing access to the subject premises be entered for the purposes of entering the subject premises:*

*(i) whether this is reasonably necessary in order to enable access to the subject premises, or*

---

<sup>600</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 27J(1).*

<sup>601</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 27J(2).*

<sup>602</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 27K(1).*

*(ii) whether this is reasonably necessary in order to avoid compromising the investigation of the terrorist act,*

*(h) whether any conditions should be imposed by the Judge in relation to the execution of the warrant.*

#### **7.2.4 Terms of a Covert Search Warrant – NSW**

A covert search warrant is to specify the following matters:

- (a) the name of the person who applied for the warrant,*
- (b) the address or other description of the subject premises,*
- (c) the name of the following persons:*
  - (i) any person believed to be knowingly concerned in the commission of the terrorist act in respect of which the warrant is issued,*
  - (ii) if no such person is an occupier of the subject premises any occupier (if known) of those premises,*
- (d) a description of the kinds of things that may be searched for, seized, placed in substitution for a seized thing, copied, photographed, recorded, operated, printed or tested,*
- (e) the date on which the warrant is issued,*
- (f) the date on which the warrant expires (being a date that is not more than 30 days from the date on which the warrant is issued)*
- (g) any conditions imposed in relation to the execution of the warrant,*
- (h) any other matter required by the regulations.<sup>603</sup>*

The sections set out above give some indication of the wide powers that a covert search warrant confers. Some of the things that are authorised by a covert search warrant include:

- impersonating someone for the purposes of executing the warrant,<sup>604</sup>
- seizing any thing connected with a serious indictable offence,<sup>605</sup>
- breaking open receptacles on the subject premises if reasonably necessary for the purpose of searching for a thing described in the warrant.<sup>606</sup>

A covert search warrant *may* authorise, inter alia:

---

<sup>603</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 27N.*

<sup>604</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 27O(1)(b).*

<sup>605</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 27O(1)(h).*

<sup>606</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 27O(1)(f).*

- entry into premises providing access to, or adjoining, the subject premises, for the purpose of entering the subject premises;<sup>607</sup>
- substitution of a thing seized with a thing of that kind;<sup>608</sup>
- the testing of a thing;<sup>609</sup>
- the copying, photographing or recording of a thing;<sup>610</sup> and
- the operation of electronic equipment.<sup>611</sup>

### **7.3 Preventative Detention Orders – NSW**

The *Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005* (NSW), which commenced on the 16<sup>th</sup> of December last year, inserts a new Pt 2A into the *Terrorism (Police Powers) Act 2002* (NSW), the object of which is to allow for preventative detention for a “short period of time” in order to prevent an “imminent terrorist act” or to preserve evidence of or relating to a recent terrorist act.<sup>612</sup> Only the Supreme Court may make a preventative detention order. Such an order may not be made against a person who is under 16 years old.<sup>613</sup>

#### **7.3.1 Interim preventative detention orders – NSW**

A police officer authorised to do so by the Commissioner of police (or a Deputy or Assistant Commissioner) may apply for an order (either interim or final) if satisfied of the requirements under s 26D.<sup>614</sup>

Section 26D, which is the test for both interim and final preventative detention orders, provides that:

*(1) A preventative detention order may be made against a person if:*

*(a) there are reasonable grounds to suspect that the person:*

*(i) will engage in a terrorist act, or*

*(ii) possesses a thing that is connected with the preparation for, or the engagement of a person in, a terrorist act, or*

*(iii) has done an act in preparation for, or planning, a terrorist act, and*

*(b) making the order would substantially assist in preventing a terrorist act occurring, and*

<sup>607</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27O(1)(d).

<sup>608</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 27O(1)(i).

<sup>609</sup> *Terrorism (Police Powers) Act 2002* (NSW), s27O(1)(l)

<sup>610</sup> *Terrorism (Police Powers) Act 2002* (NSW), s27O(1)(j)

<sup>611</sup> *Terrorism (Police Powers) Act 2002* (NSW), s27O(1)(k).

<sup>612</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 26A.

<sup>613</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 26E.

<sup>614</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 26F.

*(c) detaining the person for the period for which the person is to be detained under the order is reasonably necessary for the purpose of substantially assisting in preventing a terrorist act occurring.*

*Any such terrorist act must be imminent and, in any event, be expected to occur at some time in the next 14 days.*

*(2) A preventative detention order may also be made against a person if:*

*(a) a terrorist act has occurred within the last 28 days, and*

*(b) it is necessary to detain the person to preserve evidence in NSW or elsewhere of, or relating to, the terrorist act, and*

*(c) detaining the person for the period for which the person is to be detained is reasonably necessary for the purpose of preserving any such evidence.*

**Note:** *As a consequence of the operation of section 4A, it does not matter whether the location of the terrorist act is in NSW or elsewhere.*

Section 26G(2) relates to interim preventative detention orders. It provides that:

*An application for a preventative detention order that is required urgently may be made by telephone, fax, email or other electronic communication. In that case:*

*(a) the Supreme Court may make an interim preventative detention order if satisfied it is not practicable for the applicant to appear before the Court to make the application, and*

*(b) the terms of the interim order and related directions and other matters may be transmitted to the applicant by telephone, fax, email or other electronic communication, and*

*(c) a written record relating to the application and interim order is to be made as soon as practicable by or at the direction of the Court.*

An interim order may be made – pending the hearing and final determination of the application - if the information provided by the applicant satisfies s 26D and the Court cannot proceed immediately to the hearing and determination of the application.<sup>615</sup> The application must comply with ss 26G(1) and 26G(3) which are set out below. An interim order may be made ex parte and without notice to the subject of the order.<sup>616</sup> It must fix the date and time when the hearing will be resumed, and direct that the subject of the order be given notice of such a time and date.<sup>617</sup> No more than one

<sup>615</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26H(2).*

<sup>616</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26H(3)*

<sup>617</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26H(4).*

interim order can be made in relation to the same terrorist act,<sup>618</sup> but an interim order may be continued if a resumed hearing is adjourned.<sup>619</sup> A terrorist act ceases to be the same act if there is a change in the date on which it is to occur, but not if it is expected to occur at a particular time and there is merely a change in personnel expected to carry out the act or a change in how or where (but not when) the act is expected to occur.<sup>620</sup> An interim order ceases to have effect if the Court has not heard and determined the application in respect of which the order was made within 48 hours of the subject being taken into custody under the interim order.<sup>621</sup>

### 7.3.2 Determination of preventative detention orders by the Court – NSW

After hearing an application for a preventative detention order, the Court must grant or refuse the order.<sup>622</sup> Section 26G sets out the requirements for an application for a preventative detention order (both interim and final). It provides that:

*(1) An application for a preventative detention order must:*

*(a) subject to subsection (2) [subsection (2) is set out above and relates to urgent applications for interim orders], be in writing and sworn, and*

*(b) set out the facts and other grounds on which the police officer considers the order should be made, and*

*(c) specify the period for which the person is to be detained under the order and set out the facts and other grounds on which the police officer considers that the person should be detained for that period, and*

*(d) set out the information (if any) that the applicant has about the person's age, and*

*(e) set out the following:*

*(i) the outcomes and particulars of all previous applications for preventative detention orders made in relation to the person,*

*(ii) the information (if any) that the applicant has about any periods for which the person has been detained under an order made under a corresponding law,*

*(iii) the information (if any) that the applicant has about any control order (including any interim control order) made in relation to the person under Division 104 of the Criminal Code of the Commonwealth.*

---

<sup>618</sup> *Terrorism (Police Powers) Act 2002 (NSW)*, s 26K(5)

<sup>619</sup> *Terrorism (Police Powers) Act 2002 (NSW)*, s 26H(5).

<sup>620</sup> *Terrorism (Police Powers) Act 2002 (NSW)*, s 26K(7).

<sup>621</sup> *Terrorism (Police Powers) Act 2002 (NSW)*, s 26L.

<sup>622</sup> *Terrorism (Police Powers) Act 2002 (NSW)*, s 26I(1).

*The application must also fully disclose all relevant matters of which the applicant is aware, both favourable and adverse to the making of the order.*

(2)...

*(3) The Supreme Court may refuse to make a preventative detention order unless the police officer applying for the order gives the Court any further information that the Court requests concerning the facts and other grounds on which the police officer considers the order should be made.*

Important aspects of the judicial process for making a preventative detention order include the following (the first two points apply for both interim and final orders):

- Proceedings for the making or revoking of preventative detention orders or prohibited contact orders (see below) must be heard in the absence of the public;<sup>623</sup>
- For the purposes of such proceedings, “the Supreme Court may take into account any evidence or information that the Court considers credible or trustworthy and, in that regard, is not bound by principles or rules governing the admission of evidence;”<sup>624</sup>
- At a hearing for a final order, the subject or their legal representative may adduce evidence or make submissions;<sup>625</sup>
- The Court may make a final order *ex parte* if satisfied that the subject was properly notified of the proceedings;<sup>626</sup> and
- A final order may only be made if the Court is satisfied of the requirements under s 26D for the making of an order.<sup>627</sup>

### **7.3.3 Terms and operation of preventative detention orders – NSW**

A final preventative detention order may last up to 14 days,<sup>628</sup> and more than one order may be made in relation to the same terrorist act (whether or not against the same person).<sup>629</sup> An order, whether interim or final, may be revoked by the court on application by the subject of the order or a police officer. In the former case (unless the order is an interim order), the application is to set out information that was not provided to the Court when the order was made.<sup>630</sup>

A preventative detention order (including an interim order<sup>631</sup>) must set out:

*(a) the name of the person authorised to be detained under the order,*

*(b) the period for which the person is authorised to be detained...and*

<sup>623</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26P(2).*

<sup>624</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26O.*

<sup>625</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26I(3)(b)-(c).*

<sup>626</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26I(5).*

<sup>627</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26I(2)*

<sup>628</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26K(2).*

<sup>629</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26K(4).*

<sup>630</sup> *Terrorism (Police Powers) Act 2002 (NSW), s 26M.*

<sup>631</sup> See the definition of “preventative detention order” in s 26B of the *Terrorism (Police Powers) Act 2002 (NSW)*.

(c) the date on which, and the time on which, the order is made, and

(d) the date and time after which the person may not be taken into custody under the order (not exceeding 48 hours after the order is made) [if a person is not apprehended within the specified time the order ceases to have effect<sup>632</sup>], and

(e) a summary of the grounds on which the order is made.<sup>633</sup>

Subsection (e) does not require information that is likely to be prejudicial to national security to be included in the summary. The relevant definition of “national security” is contained in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), which defines national security broadly in s 8 to mean “Australia’s defence, security, international relations or law enforcement interests.”

Divisions 3-6 of Part 2A deal primarily with operational matters such as the carrying out of preventative detention orders and the way a subject is to be treated. The following two provisions are of note:

- contact between the subject and their lawyer may be monitored (although evidence of certain communications will be inadmissible, and it is an offence for a monitor to disclose the information conveyed in such a communication);<sup>634</sup> and
- a subject may not be questioned while in detention except for the narrow purposes set out in s 26ZK.

### 7.3.4 Prohibited contact orders – NSW

A police officer who applies for a preventative detention order may also apply for a prohibited contact order.<sup>635</sup> When a preventative detention order is in force, any police officer may apply for a prohibited contact order.<sup>636</sup> An application must be written and sworn unless urgent, in which case it may be made by telephone etc.<sup>637</sup> Subsection 26N(4) provides that:

*If the Supreme Court is satisfied that making a prohibited contact order is reasonably necessary to achieve the purposes of the preventative detention order, the Court may make a prohibited contact order under this section that the subject is not, while being detained under the preventative detention order, to contact a person specified in the prohibited contact order.*

<sup>632</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 26L(3)

<sup>633</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 26J(1).

<sup>634</sup> *Terrorism (Police Powers) Act 2002* (NSW), ss 26ZI(1), (5) and (6).

<sup>635</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 26N(1).

<sup>636</sup> *Terrorism (Police Powers) Act 2002* (NSW), s 26N(2).

<sup>637</sup> *Terrorism (Police Powers) Act 2002* (NSW), ss 26N(3) and (5).



Once granted, the court may revoke the order on application by the subject or by a police officer.<sup>638</sup> A subject's lawyer may be the subject of a prohibited contact order.<sup>639</sup>

---

<sup>638</sup> *Terrorism (Police Powers) Act 2002 (NSW)*, ss 26N(6)-(7).

<sup>639</sup> *Terrorism (Police Powers) Act 2002 (NSW)*, s 26ZJ

## Appendix 1: Summary of Issuing Authorities for Warrants and Orders Considered in this Paper

Type of Warrant/Order (including a page reference to the relevant part of the paper)	Issuing Authority
Search warrant under the <i>Law Enforcement (Powers and Responsibilities) Act 2002</i> (NSW) (p. 67 ff)	<ul style="list-style-type: none"> <li>- Magistrate or Children's Magistrate</li> <li>- Clerk of a Local Court</li> <li>- Authorised employee of the Attorney-General's Department</li> </ul>
Search warrant under the <i>Crimes Act 1914</i> (Cth) (p. 74 ff)	<ul style="list-style-type: none"> <li>- Magistrate</li> <li>- A Justice of the Peace or other person employed in a court of a State or Territory who is authorised to issue search warrants</li> </ul>
Covert search warrants under the <i>Terrorism (Police Powers) Act 2002</i> (NSW). (p. 111 ff)	A Judge of the Supreme Court who has consented in writing, and who the Attorney-General has declared to be an eligible Judge. The Attorney-General may revoke the declaration (s 27B(6))
Listening device warrants under the <i>Listening Devices Act 1984</i> (NSW) (p. 75 ff)	Supreme Court Judge who has consented in writing, and who is declared by the Attorney-General to be an eligible Judge
Surveillance device warrants under the <i>Surveillance Devices Act 2004</i> (Cth) (p. 82 ff)	<ul style="list-style-type: none"> <li>- A Judge of a Court created by Federal Parliament who has consented in writing, and who is declared by the Minister to be an eligible Judge</li> <li>- A Deputy President, full- or part-time senior member, or member of the AAT who is nominated by the Minister. Such a nomination can be revoked (s 13(3)(b)). The Minister must not nominate a member or part-time senior member unless they are enrolled as a legal practitioner of a federal court (including the High Court) or of a Supreme Court of a State or of the ACT, and have been so enrolled for at least 5 years.</li> </ul>
Approvals of emergency authorisations under the <i>Surveillance Devices Act 2004</i> (Cth) (p. 84 ff)	As above
Interception warrants under Part III of the <i>Telecommunications (Interception) Act 1979</i> (Cth) (p. 93 ff)	<ul style="list-style-type: none"> <li>- The Attorney-General</li> <li>- The Director General of Security may issue "emergency warrants."</li> </ul>

<p>Interception warrants under Part VI of the <i>Telecommunications (Interception) Act 1979</i> (Cth) (p. 88 ff)</p>	<ul style="list-style-type: none"> <li>- A Judge of a Court created by Federal Parliament who has consented in writing, and who is declared by the Minister to be an eligible Judge</li> <li>- A Deputy President, full- or part-time senior member, or member of the AAT who is nominated by the Minister. Such a nomination can be revoked (s 6DA(3)(b)). The Minister must not nominate a member or part-time senior member unless they are enrolled as a legal practitioner of a federal court (including the High Court) or of a Supreme Court of a State or of the ACT, and have been so enrolled for at least 5 years.</li> </ul>
<p>Detention warrants for the purpose of questioning after arrest for an offence (<i>Law Enforcement (Powers and Responsibilities Act 2002</i> (NSW)) (p. 54 ff)</p>	<ul style="list-style-type: none"> <li>- Magistrate or Children’s Magistrate</li> <li>- Clerk of a Local Court</li> <li>- Authorised employee of the Attorney-General’s Department</li> </ul>
<p>Detention warrants for the purpose of questioning after arrest for either a conventional offence (p. 54 ff) or a terrorist offence (p. 55 ff) (<i>Crimes Act 1914</i> (Cth))</p>	<ul style="list-style-type: none"> <li>- Magistrate</li> <li>- Justice of the Peace who is employed in a court of a State or Territory or a bail justice</li> <li>- Justice of the Peace</li> </ul> <p>Note that applications for detention warrants must be made, firstly, to a Magistrate; secondly, to a JP employed in a court or a bail justice, if a Magistrate is not available; thirdly, to a JP if none of the preceding are available</p>
<p>Control orders under the <i>Criminal Code</i> (Cth) (p. 98 ff)</p>	<ul style="list-style-type: none"> <li>- Federal Court</li> <li>- Family Court</li> <li>- Federal Magistrates Court</li> </ul>
<p>Detention and questioning warrants for the purpose of questioning by ASIO (<i>ASIO Act 1979</i> (Cth)) (p. 102 ff)</p>	<ul style="list-style-type: none"> <li>- A Federal Magistrate or a Judge of a Court created by Federal Parliament who has consented in writing, and who is appointed as an issuing authority by the Minister</li> <li>- A class of persons declared by the regulations to be issuing authorities</li> </ul>
<p>Initial preventative detention orders under the <i>Criminal Code</i> (Cth) (p. 106 ff)</p>	<p>Senior AFP member (Commissioner, Deputy Commissioner, member of or above the rank of superintendent)</p>
<p>Prohibited contact orders in respect of initial preventative detention orders under the <i>Criminal Code</i> (Cth) (p. 109 ff)</p>	<p>As above</p>

<p>Continued preventative detention orders under the <i>Criminal Code</i> (Cth) (p. 107 ff)</p>	<p>A person who has consented in writing and who is appointed by the Minister where the person is:</p> <ul style="list-style-type: none"> <li>- A Judge of a State or Territory Supreme Court</li> <li>- A Judge of a Court created by Federal Parliament</li> <li>- A Federal Magistrate</li> <li>- A retired Judge who served for 5 or more years in a superior court</li> <li>- The President or Deputy President of the AAT, as long as he or she has been enrolled for at least 5 years as a legal practitioner of a federal court or a State or Territory Supreme Court</li> </ul>
<p>Prohibited contact orders in respect of continued preventative detention orders under the <i>Criminal Code</i> (Cth) (p. 109 ff)</p>	<p>As above</p>
<p>Preventative detention orders under the <i>Terrorism (Police Powers) Act 2002</i> (NSW) (p. 115 ff)</p>	<p>The Supreme Court</p>
<p>Prohibited contact orders in respect of preventative detention orders issued under the <i>Terrorism (Police Powers) Act 2002</i> (NSW) (p. 119 ff)</p>	<p>The Supreme Court</p>