

INVESTIGATING AND PROSECUTING TERRORISM: THE COUNTER-TERRORISM LEGISLATION AND THE LAW OF EVIDENCE

ANDREW PALMER*

I INTRODUCTION

This article discusses the evidential aspects of the Commonwealth's counter-terrorism legislation,¹ and the legislation proposed to deal with classified and sensitive national security information.² Its focus is on those aspects of the legislation which impinge on or affect the way in which evidence is gathered, and the way in which evidence is used at trial.³ The first part of the article examines the evidential implications of the new investigative powers conferred on the Australian Security Intelligence Organisation ('ASIO') by the *Australian Security Intelligence Organisation Legislation Amendment Act 2003* (Cth); while the second part of the paper focuses on a Bill currently before the Commonwealth Parliament, together with the Australian Law Reform Commission's ('ALRC') proposals for trials involving the use of 'secret' evidence. Elsewhere in this issue, some or all of these proposals are considered from the point of view of constitutional law, international law, human rights law and so on; the aim in this article is to analyse them purely from the perspective of the law of evidence.

* Barrister at Law, Victoria; Associate Professor, Law School, University of Melbourne. The writing of this article was enormously helped by the able research assistance of Lucie O'Brien. I also benefited from the helpful comments of Brian Walters SC and Dr Jeremy Gans, my colleagues respectively at the Bar and at the Law School. Finally, the article was reviewed by three anonymous referees, each of whom made a number of important suggestions for improvement, many of which I adopted outright. Of course, responsibility for any errors, oversights or misconceptions remains mine and mine alone.

1 In particular the *Australian Security Intelligence Organisation Act 1979* (Cth), as amended by the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2002* (Cth), and the *Australian Security Intelligence Organisation Legislation Amendment Act 2003* (Cth).

2 Including the National Security Information (Criminal Proceedings) Bill 2004 (Cth), which is largely based on proposals contained in Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, Discussion Paper No 67 (2004).

3 I will not be discussing the non-forensic uses that may be made of information gathered through this process. Cf, eg, Brian Walters, 'The War on Terror: Labor's Capitulation to the ASIO Legislation' (2003) 12 *Dissent* 48, 50, discussing the possibility that information which a person was compelled to give might be used to identify targets for extra-judicial killing.

II THE EVIDENTIAL ASPECTS OF ASIO'S NEW INVESTIGATIVE POWERS

Among the most significant of the 2003 amendments to the *Australian Security Intelligence Organisation Act 1979* (Cth) ('ASIO Act') is the introduction of a new div 3 ('Special Powers Relating to Terrorism Offences') into pt III ('Functions and Powers of Organisation'). The most important of the new powers conferred on ASIO is the power to compulsorily question people, and if necessary to detain them for that purpose. The main point of these provisions is no doubt to assist ASIO in the gathering of intelligence; but the information so gathered could also conceivably be used as evidence in a trial. Accordingly, this part of the article focuses on two main aspects of the provisions: first, any modifications to the law of evidence that the new investigative regime makes; and secondly, the question of whether information obtained through the use of these new powers could be used as evidence in a trial. I focus on the regime as it applies to adults, rather than the special provisions applying to children.⁴ I start by setting out the framework of the new regime, as a necessary preliminary to subsequent analysis.

A Outline of the New Investigative Regime

1 *The Issuing of a Warrant*

The most significant feature of the new investigative regime is the fact that ASIO may be granted warrants to question and detain people. There are a number of different persons involved in this process of seeking and then executing a warrant:

- the person in respect of whom a warrant is being sought ('the subject');
- the Director-General of ASIO ('the Director-General');
- the Minister responsible for ASIO ('the Minister');
- the 'issuing authority', namely a Federal Magistrate or a Judge, appointed by the Minister under s 34AB, for the purposes of issuing warrants;
- the 'prescribed authority', normally a former judge of a superior court, appointed by the Minister under s 34B, before whom persons to be questioned under warrant are questioned; and
- persons exercising authority under the warrant.

There are four distinct steps required before a warrant can be issued. The first is that the Director-General seeks the Minister's consent to a request for the issue of a warrant.⁵ In making this request, the Director-General must provide the Minister with a draft of the warrant, and a statement of the facts and other grounds on which the Director-General considers it necessary that the warrant

4 See *Australian Security Intelligence Organisation Act 1979* (Cth) s 34NA, which prohibits the questioning of persons under 16 years of age, and creates special rules for persons between the ages of 16 and 18.

5 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34C(1).

should be issued. The second step is that the Minister consents to the making of the request.⁶ The Minister may only consent if he or she is satisfied that:

- (a) there are reasonable grounds for believing that issuing the warrant will substantially assist the collection of intelligence that is important in relation to a 'terrorism offence';⁷ and
- (b) that relying on other methods of collecting that intelligence would be ineffective; and
- (c) if the warrant is to authorise immediate custody and detention, that there are reasonable grounds for believing that if the subject is not immediately taken into custody and detained that the subject:
 - (i) may alert a person involved in a terrorism offence that the offence is being investigated; or
 - (ii) may not appear before the prescribed authority; or
 - (iii) may destroy, damage or alter a record or thing the person may be requested to produce under the warrant.

Once the Minister has consented, the Director-General may take the third step, which is to request an issuing authority to issue a warrant.⁸ The fourth step is the issuing of the warrant by the issuing authority.⁹ The issuing authority may only issue the warrant if 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. This is the same test as was applied by the Minister in deciding whether or not to consent to the making of the request. The vagueness and imprecision of the test is likely to render it all but immune to judicial challenge.¹⁰

A noteworthy absence from the tests to be applied by the Minister or the issuing authority is any requirement that there be reasonable grounds, or indeed any grounds at all, to suspect the subject of having committed, or of being about to commit, an offence. The subject may be entirely innocent of any wrongdoing, and ASIO may know this: the subject may nevertheless be detained, if there are grounds to believe that their detention will assist in the gathering of intelligence in relation to a terrorism offence. As Walters points out:

It is enough if you have been dining at a restaurant at the next table to some suspected terrorists, and it is believed that you may have overheard something. It is enough if you have come from the home village in another country of a suspected terrorist, and it is believed you may be able to provide some background on the person. It is enough if you are a relative of a suspected terrorist, and may have some idea of where they might be. It is enough to be a journalist who has interviewed one of these suspected people.¹¹

6 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34C(3).

7 A 'terrorism offence' is defined in s 4 of the *ASIO Act* as an offence against div 72 (International Terrorist Activities Using Explosive or Lethal Devices) or pt 5.3 (Terrorism) of the *Criminal Code* (Cth).

8 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34C(4).

9 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34D(1).

10 See Walters, above n 3, 50.

11 *Ibid* 51.

2 *What a Warrant May Authorise*

All warrants must authorise ASIO, subject to any restrictions or conditions, to question the subject by requesting the subject to do either or both of the following: give information that is or may be relevant to intelligence in relation to a terrorism offence; and produce records or things that are or may be relevant to intelligence in relation to a terrorism offence.¹² Beyond this common core, there are two main types of warrants: those that authorise the subject to be taken into immediate custody and to be detained and those that do not.¹³ Both types of warrant, however, require the subject to be brought before (where custody was authorised), or to appear before (where custody was not authorised), a prescribed authority for questioning under the warrant.

Where custody and detention are authorised, the warrant will authorise the subject to be detained for a ‘questioning period’ as determined by s 34D(3). The questioning period commences when the subject is first brought before the prescribed authority and ends as soon as one of the following happens: a person exercising authority under the warrant informs the prescribed authority that they have no further requests to make of the subject; s 34HB prohibits any further questioning (I return to s 34HB below); or 168 hours (seven days) elapses. Section 34HC confirms that the maximum continuous period for which a subject may be detained is 168 hours. Even if the warrant did not authorise detention, the prescribed authority may still order it, provided that the Minister approves in writing, and the prescribed authority is satisfied that there are reasonable grounds for believing that if the subject is not detained they may alert another person involved in a terrorism offence to the fact that the offence is being investigated; or may fail to appear again; or may destroy, damage or alter a record or thing that they have been, or may be requested to produce.¹⁴ Such a direction must not result in the subject being detained after the end of the questioning period as determined by s 34D(3).¹⁵

The time limits under the *ASIO Act* can be contrasted with those imposed by the *Crimes Act 1914* (Cth), which applies when someone is arrested for a Commonwealth offence. Section 23C provides that a person who is arrested for a non-terrorism offence may not be detained for investigative purposes for more than four hours (or two hours if the person is under 18 or is an Aboriginal or Torres Strait Islander). This investigation period can be extended by order of a magistrate, but can only be extended by up to eight hours, and can only be extended once.¹⁶ In respect of terrorism offences, the *Anti-terrorism Act 2004* (Cth) inserted new ss 23CA and 23DA into the *Crimes Act 1914* (Cth). These impose the same initial time limits for detention for the investigation of Commonwealth terrorism offences as apply to non-terrorism offences; that is, two hours if the suspect is under 18 or is an Aboriginal or Torres Strait Islander, and four hours in all other cases. These time limits can, however, be extended by

12 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34D(5)(a).

13 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34D(2)(a)–(b).

14 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34F(1)–(3).

15 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34F(4)(a).

16 *Crimes Act 1914* (Cth) s 23D.

an additional 20 hours, rather than the eight which applies in respect of non-terrorism offences. The effect of the provisions then is to allow a maximum 24 hour investigation period for the investigation of Commonwealth terrorism offences.¹⁷ If a maximum of 12 hours detention is adequate for investigating non-terrorism offences, and a maximum of 24 hours is adequate for investigating terrorism offences, why is ASIO permitted to detain people for up to 168 hours?

3 *Further Warrants*

If a warrant has previously been issued in relation to the subject, there are additional steps that must be taken before a further warrant can be issued. First, the Director-General's request to the Minister must also include details about the outcomes of all previous requests for warrants (for example, were they issued or not); and a statement of the period for which the subject was questioned and/or detained under those warrants.¹⁸

Secondly, if the subject has already been detained under earlier warrants and the proposed request is for a warrant authorising further detention, the Minister must take this into account in deciding whether or not to consent to the making of the request; and may only consent to the making of the request if satisfied that the issuing of the warrant is justified by information that is additional to or materially different from that known to the Director-General at the time that the Director-General sought the Minister's consent to the last of the earlier warrants.¹⁹

Thirdly, if the subject has previously been detained and the request is for a warrant authorising further detention, these same restrictions also apply to the issuing authority in deciding whether or not to issue the warrant.²⁰ In addition, the issuing authority must be satisfied that the subject is not currently being detained under one of the earlier warrants.²¹ This limitation is obviously designed to prevent the use of overlapping or rolling warrants.

A major concern is whether the additional or materially different information which would justify the issue of a further warrant might be information obtained from the subject him or herself;²² certainly, there is nothing in the legislation that says that it could not be information obtained from the subject. If it could be, this obviously raises the spectre of a series of warrants being granted, each justified by the information gathered in the exercise of the previous warrant.

4 *Protections for the Subject*

17 Or 22 hours where the suspect is under 18 or is an Aboriginal or Torres Strait Islander: which rather suggests that any special protection offered these groups is effectively obliterated by the possible extension time of 20 hours.

18 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34C(2)(c)-(d).

19 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34C(3D).

20 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34D(1A).

21 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34D(1A)(b)(ii).

22 See Duncan Kerr, 'Australia's Legislative Response to Terrorism' (Speech delivered at the Criminal Bar Association of Victoria, Melbourne, 26 August 2003) 4, 11, referring to the letter from the Law Council of Australia to Prime Minister John Howard, 25 June 2003.

There are a number of provisions that offer some measure of protection for the subject. The subject has the right to request an interpreter, and this request must be met, unless the prescribed authority believes on reasonable grounds that the subject has an adequate knowledge of English.²³ There are rules about the conduct of strip searches.²⁴ The subject must be ‘treated with humanity and with respect for human dignity, and must not be subjected to cruel, inhuman or degrading treatment’.²⁵ It is an offence to contravene these and other safeguards, such as preventing the subject from contacting someone the warrant says they may contact.²⁶

Even though it is backed with an offence, a requirement of humane treatment is clearly vague and hard to enforce in anything other than the clearest examples (such as the abuse of Iraqi prisoners by American defence personnel at Abu Ghraib prison). Of more practical significance may be the standards set out in a protocol tabled by the Government in Parliament on 11 August 2003.²⁷ The protocol establishes guidelines for the treatment of detainees, such as ensuring that detainees are permitted a minimum of eight hours undisturbed sleep in every 24 hour period, are not continuously questioned for more than four hours without being offered a break, are provided with three meals a day, are to be given a separate room or cell in which to sleep,²⁸ and so on. Breach of the guidelines contained in the protocol might lead to the detention and questioning being regarded as illegal or improper, which could have implications for the admissibility of any evidence gathered.²⁹

5 Time Limits on Questioning under a Warrant

At first sight, s 34HB(1) appears to limit questioning under a warrant to a total of eight hours. However, s 34HB(1) and (4) actually give the prescribed authority power to permit further questioning if satisfied of two things: first, that there are reasonable grounds for believing that permitting the continuation will substantially assist the collection of intelligence that is important in relation to a terrorism offence; and second, that the previous questioning was conducted properly and without delay. Similarly, s 34HB(2) appears to limit questioning to a total of 16 hours; but the prescribed authority again has the power to permit further questioning. The actual limit on questioning is imposed by s 34HB(6), which limits the questioning to a total of 24 hours. The prescribed authority has no power to permit further questioning once that limit is reached.

Once the 24 hour limit is reached, or the eight or 16 hour limits are reached without the prescribed authority having permitted a continuation of questioning, further questioning is prohibited and the subject must be immediately released

23 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34HAA.

24 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 34L–M.

25 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34J(2).

26 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34NB.

27 Kerr, above n 22, 8.

28 While the protocol seems to assume that a separate cell is a positive, this could equally be described as mandatory solitary confinement.

29 See discussion below in Part II(C)(2).

from detention.³⁰ Despite the fact that a continuation of questioning from eight to 16 and from 16 to 24 hours can only be granted if the prescribed authority is satisfied that the previous questioning was conducted without delay, the legislation clearly contemplates a certain amount of delay given that detention can last for up to 168 hours. Even allowing for breaks and sleep, it is hard to see how someone could be detained for 168 hours but only questioned for 24, without there being significant periods during which they could be being questioned, but are not questioned. That they have been detained but are not being questioned might be due to the fact that a large number of persons have been detained for questioning; or it could be because ASIO wishes to question detainees in a particular sequence. The issue for the prescribed authority will be whether, when there is 'delay' for such a reason, it can be said that the questioning of a particular subject has been conducted without delay.

6 *Obligations during Questioning*

Where a subject is being questioned before a prescribed authority, they can not refuse to give information, or to produce a record or thing, on the grounds that the information or production might tend to incriminate them, or make them liable to a penalty.³¹ In other words, the privilege against self-incrimination is expressly abolished.³² Moreover, it is an offence to fail to give any information requested in accordance with the warrant, to make a statement that the subject knows to be false or misleading in a material particular, and to fail to produce a record or thing that the subject is requested to produce.³³ All of these offences are punishable by five years imprisonment. The abolition of the privilege against self-incrimination, and the creation of offences for failing to answer questions or for providing misleading information, are not in themselves unusual: the Commonwealth Parliament has not infrequently given statutory authorities such as the Australian Crime Commission or the Australian Securities and Investment Commission the power to compel persons to provide information notwithstanding that it incriminates them to do so,³⁴ while making it an offence not to do so, or to provide false information.

There are defences to the offences created by s 34G(3) and (6), namely that the subject does not have the information, or does not have possession and control of the record or thing.³⁵ However, the defence carries an evidential burden in relation to leading these defences;³⁶ that is, the defence carries the 'burden of

30 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34HB(7).

31 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34G(8).

32 The significance of this in terms of the admissibility of evidence is discussed at below in Part II(B)(2).

33 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34(3), (5), (6) respectively.

34 See *Australian Crime Commission Act 2002* (Cth) s 30; and *Australian Securities and Investment Commission Act 2001* (Cth) ss 58, 63; and especially 68.

35 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 34G(4), (7), respectively.

36 The imposition of evidential burdens in relation to defence is a feature these offences share with other offences created by the counter-terrorism legislation including *Criminal Code* ss 101.4 ('Possessing Things Connected with Terrorist Acts'), 101.5 ('Collecting or Making Documents Likely to Facilitate Terrorist Acts'), 102.3 ('Membership of a Terrorist Organisation'), 102.6 ('Getting Funds to or from a Terrorist Organisation').

adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist'.³⁷ The evidential burden is distinguished from the legal burden, which is the burden of satisfying the court of the existence or non-existence of a fact, to the requisite standard of proof (in criminal trials, beyond reasonable doubt). It is normal for the accused to carry an evidential burden in relation to a defence that is not simply a denial of the elements of the offence, but involves alleging an additional, exculpatory fact. For example, the defence usually bears an evidential burden in relation to defences such as self-defence or provocation. Moreover, an evidential burden is not necessarily difficult to satisfy: testimony from the subject to the effect that he or she did not have the information, or the record or thing, would presumably satisfy the evidential burden. Once the evidential burden is satisfied, the burden shifts to the prosecution (now as a legal burden) to disprove the defence, beyond reasonable doubt.

What is perhaps unusual about these offences, then, is not that the accused bears an evidential burden in relation to the defences, but that the 'fault' elements of the offences are so minimal. In the case of an offence against the person, for example, such as assault or murder, the accused's evidential burden in relation to self-defence only really becomes an issue once the prosecution have established that the accused did strike or kill another person, as the case may be. In relation to possession offences, the burden of establishing lawfulness only arises once it has been established that the accused was in possession of illicit substances; or as with one of the new 'terrorist' offences, that the accused was found in possession of a thing connected with a terrorist act. Once the fact of possession is proved, the onus is on the defence to lead evidence to show why the possession was not unlawful. The circumstances, it might be said, call for an explanation, and if anyone could give that explanation it would be the accused.

In the case of the offences against s 34G, however, the burden of leading evidence to support a defence arises simply on proof of the fact that the accused was asked to provide information and failed to do so. There may be nothing in the circumstances that make it probable that they would have that information in the first place. The most that may be able to be said is that both the Minister and the issuing authority must have been satisfied that 'there are reasonable grounds for believing that issuing the warrant will substantially assist the collection of intelligence that is important in relation to a terrorism offence';³⁸ but this is not a fact which calls out for explanation by the subject. The situation, then, is that once the warrant has been issued, and the information has been sought, the onus is on the subject to either provide the information, or to lead evidence to show that they do not have it: if they fail to do one of those things, then they are guilty of an offence punishable by five years imprisonment.

7 *Communication with Lawyers*

37 See *Criminal Code* s 13.3.

38 See discussion above in Part II(A)(1).

A detained subject is generally prohibited from communicating with any person.³⁹ However, the regime does confer rights on subjects to communicate with lawyers, albeit that these rights are fairly circumscribed, and can be denied.⁴⁰ Where the Director-General seeks the consent of the Minister to the making of a request for a warrant which would authorise immediate custody and detention, the Minister must ensure that the warrant to be requested would permit the subject to contact a single lawyer of their choice.⁴¹ Similarly, if the issuing authority issues a warrant which authorises custody and detention, they must also permit the subject to contact identified persons at specified times.⁴² Those persons may be identified by their legal or familial relationship to the subject, rather than by name.⁴³

The subject's right of contact with a lawyer can only be exercised once three conditions are met.⁴⁴ The first is that the subject is in detention. The second is that the subject has been taken before the prescribed authority for questioning, and has informed the prescribed authority of the identity of the lawyer they wish to contact. The third is that a person exercising authority under the warrant has had an opportunity to request that the prescribed authority give a direction under s 34TA that the subject be prevented from contacting the lawyer.

Notwithstanding the provisions of the warrant, therefore, s 34TA gives the prescribed authority the power to give a direction preventing a detained subject from contacting their lawyer. Such a direction may only be given if the prescribed authority is satisfied, on the basis of circumstances relating to the particular lawyer, that if the detained subject is permitted to contact the lawyer, a person involved in a terrorism offence may be alerted that the offence is being investigated, or a record or thing that the subject may be requested to produce may be destroyed, damaged or altered. This does not prevent the subject from choosing another lawyer, although they may also be prevented from contacting that lawyer for the same reasons.⁴⁵

Moreover, in many if not most cases a subject may not know the name of a lawyer (or a suitably experienced lawyer), and the legislation is silent about what should happen in this situation. There is no requirement, for example, that the subject be permitted to consult the Yellow Pages, or to contact the local law institute or a friend or family member for a recommendation. Absent any such requirement, a subject who is unable to identify a lawyer that they wish to contact would seem to have no right to contact any lawyer at all. Moreover, the right to contact a lawyer is a right to contact a *single* lawyer of the person's choice: if the lawyer is unwilling or unable to assist the subject, the subject does not appear to have a right to attempt to contact another lawyer. While it is true

39 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34F(8).

40 For an excellent analysis of the difficulties likely to be experienced by lawyers involved in advising detained subjects, see Kerr, above n 22.

41 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34C(3B).

42 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34D(2)(b).

43 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34D(4).

44 See *Australian Security Intelligence Organisation Act 1979* (Cth) ss 34C(3B), 34D(4A).

45 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34TA(4).

that the prescribed authority has a discretion to permit the subject to contact persons which is sufficiently wide to overcome these problems,⁴⁶ the *right* to contact a lawyer is so circumscribed that it hardly seems to be a right at all.

Where contact is permitted and in fact achieved, the detained subject has no right to have their lawyer with them during questioning,⁴⁷ although the prescribed authority must give the lawyer a reasonable opportunity to advise the subject during breaks in the questioning.⁴⁸ If the lawyer is permitted to be present during questioning, the lawyer must not intervene in the questioning or address the prescribed authority, for any purpose other than to request clarification of an ambiguous question.⁴⁹ If the prescribed authority considers the lawyer to be unduly disruptive, the prescribed authority may order their exclusion.⁵⁰

Section 34U(7) makes it an offence, punishable by five years imprisonment, for the lawyer to communicate to a third person any information relating to the questioning or detention of a subject under a warrant while that subject is in detention, unless the prescribed authority authorises that communication. The prescribed authority is obliged to authorise the lawyer to communicate to a member or registrar of a federal court, for the purposes of seeking a remedy in relation to a warrant or the treatment of the subject in relation to the warrant, or questioning or detention pursuant to the warrant.⁵¹ Apart from that, the prescribed authority is under no obligation to permit the lawyer to communicate even the mere fact of detention to persons such as the family of the detained subject.

B Privilege Issues

1 *Legal Professional Privilege*

The only reference to legal professional privilege in the Act is contained in s 34WA, which states that '[t]o avoid doubt, this Division does not affect the law relating to legal professional privilege'. While this section may have been intended by the drafters to preserve legal professional privilege, there are very strong reasons to be concerned that the new provisions may effectively deny privilege to communications between subjects and their lawyers. This is because any contact between the subject and lawyer must be made in a way that can be monitored by a person exercising authority under the warrant.⁵² Although the word 'monitored' is not defined, presumably it means not only that the contact should be observed, but also that its contents should be listened to. This is because one of the main reasons for requiring monitoring is, in all probability, to ensure that the lawyer is not used by the subject as a means of passing messages to other persons, or to alert other persons to the fact that an offence is being investigated.

46 See *Australian Security Intelligence Organisation Act 1979* (Cth) s 34F(1)(d), (8), (9)(a).

47 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34TB(1).

48 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34U(3).

49 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34U(4).

50 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34U(5).

51 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34U(9).

52 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34U(2).

There are three main ways in which monitoring could affect privilege. First, the very fact that the contact is monitored is bound to have a chilling effect on the communication, making it less likely that the subject will be willing to discuss their situation with the frankness and candour that the privilege is intended to protect. Regardless of whether or not the person monitoring the contact is permitted to give evidence about the communication – which is discussed below – there is nothing in the 2003 amendments, or anywhere else which would prevent the ‘monitor’ from telling another person about the content of the communication, informing the prescribed authority if it appeared possible that the lawyer might alert other persons involved in an offence to the fact it was being investigated, or relying on the content of the communications in some other way (for example, as an investigative lead). The effect this will inevitably have on the subject will obviously limit the usefulness of any advice their lawyer is able to give them.

Secondly, there is a long line of authority that permits a third party to give evidence of a privileged communication, even if the lawyer or client could claim privilege in respect of that communication.⁵³ McNicol summarises the authority as follows:

The ‘third party exception’ to legal professional privilege states that a third party who overhears a privileged communication between a legal adviser and a client or obtains a privileged document or copy of it (by being given it, by stealing it or by just seeing it) is not precluded from giving evidence of the contents of the communication or document despite the legal professional privilege which exists between the legal adviser and the client.⁵⁴

This rule does not apply under the *Evidence Act 1995* (Cth), the *Evidence Act 1995* (NSW) or the *Evidence Act 2001* (Tas) (‘Uniform Evidence Legislation’) because the privilege is expressed as a rule which renders certain evidence inadmissible, rather than a rule which exempts a person from what would otherwise be a compulsory demand for information;⁵⁵ but it would still operate in proceedings to which the common law applies. In some cases the rule in *Calcraft v Guest* may be ameliorated by a conflicting line of equitable authority founded on the decision in *Lord Ashburton v Pape*.⁵⁶ This line of authority permits a privilege holder to seek an injunction restraining the third party from giving evidence of the communication, where the third party’s use of the communication would constitute a breach of confidence, or some other impropriety. Given, however, that the communications between the subject and his or her lawyer are required to be monitored, it is clear that there is no impropriety in the means by which the monitor obtained his or her knowledge of the communication. Nor is in there anything in the *ASIO Act* that imposes a duty of confidence on the monitor in relation to that communication. It is therefore

53 See *Calcraft v Guest* [1898] 1 QB 759.

54 Suzanne McNicol, *The Law of Privilege* (1992) 83. For further discussion of this line of authority, see also 25–6 and 83–94; J D Heydon, *Cross on Evidence* (6th ed, 2000) [25025]–[25030].

55 See Uniform Evidence Legislation ss 118, 119.

56 [1913] 2 Ch 469.

difficult to see how the line of authority in *Lord Ashburton v Pape* could be used to prevent the monitor from giving evidence of the communication.

Thirdly, the monitoring could arguably prevent privilege from arising at all, which would mean that not only would the monitor be permitted to give evidence about the communication, but also, the lawyer and the subject could be compelled to. The argument arises out of the fact that privilege only applies to confidential communications, whereas the fact that communications must be monitored by a third party, and that this would be known to the subject and his or her lawyer, could mean that any communication was not confidential, and therefore not privileged. This result, while regrettable and possibly unintended, is consistent with the ‘law relating to legal professional privilege’, which, according to s 34WA, is not affected by the new Division. The proposition that privilege only protects confidential communications is not a controversial one.⁵⁷ The real issue is whether the fact that a communication is monitored, and known to be monitored, affects its confidentiality.

At common law there are a number of cases dealing with analogous situations.⁵⁸ In *R v Braham and Mason*⁵⁹ (*‘Braham’*), the accused Braham telephoned his solicitor after the completion of his record of interview. He made this phone call in the presence of a police officer, who testified at the committal to the effect that the accused told his solicitor that he had admitted his involvement in the offence. At trial, the prosecution did not seek to lead the evidence but counsel for the co-accused did. Justice Lush referred to an earlier decision, *Re Giffin*,⁶⁰ where Innes J had made the following comment: ‘It seems to me that if a statement is made in the presence of a third party there can be no privilege properly so called. The only privileged communications are those made between a solicitor and client when they are alone.’

Justice Lush was unable to accept the ‘categorical statement that the presence of a third party will always destroy privilege’,⁶¹ holding instead that

each case must be examined to see whether the communication was one which should be classed as confidential. The fact of the presence of a third party should be examined to see whether that presence indicates that the communication was not intended to be confidential, or whether the presence of the third party was caused by some necessity or some circumstances which did not affect the primary nature of the communication as confidential ...⁶²

Turning to the facts of the case, Lush J made the following observations:

57 At common law, see Heydon, above n 54, [25255]; for the legislative response, see Uniform Evidence Legislation is concerned, see ss 118, 119.

58 Apart from those referred to below, see also *Newcastle Wallsend Coal Co Pty Ltd v Court of Coal Mines Regulation* (1997) 42 NSWLR 351, 394 (Smart AJA); *Gotha City v Sotheby’s* [1998] 1 WLR 114, 122.

59 [1976] VR 547.

60 (1887) 8 LR (NSW) 132.

61 *Braham* [1976] VR 547, 548.

62 *Ibid* 549.

I do not regard it as decisive that Braham did not ask to be alone when he spoke to his solicitor, but I find in the circumstances described as I have set them out, no real indication that this communication was intended to be confidential, or that it was only made in the presence of Inspector Phelan as a matter of necessity. It appears to me that so far as the situation between Braham and Inspector Phelan at the time was concerned, it is most likely that Braham considered that there was no reason why Inspector Phelan should not hear the conversation because what he was telling his solicitor was in substance what he had been telling Inspector Phelan for the last hour or more.

In the present case I think that there is no real sign that Braham had any intention that this was to be a confidential communication. Rather it was intended to be an explanation why he was telephoning the solicitor and was intended to be a mere repetition of what Inspector Phelan already knew.⁶³

A very similar set of facts to *Braham* recently arose in the case of *R v Sharp*,⁶⁴ although this time they arose in the context of the Uniform Evidence Legislation. Justice Howie referred to s 117(1) of the legislation, which defines the phrase 'confidential communication' in the following way:

confidential communication means a communication made in such circumstances that, when it was made:

- (a) the person who made it; or
- (b) the person to whom it was made;

was under an express or implied obligation not to disclose its contents, whether or not the obligation arises under law.⁶⁵

In interpreting this definition, Howie J referred to the ALRC's Interim Report on *Evidence*, which suggested that it was not intended to change the common law approach to the question of confidentiality.⁶⁶ Reaching the same conclusion on the facts as Lush J had in *Braham*, Howie J held:

Because there was nothing said or done by the accused to indicate that she considered the conversation to be confidential, at common law she could not claim privilege notwithstanding that it was spoken to her solicitor in the course of seeking advice. The ALRC appears to have intended that the same position would apply under the Act: the communication has to be confidential at the time it was made. Of course the accused found herself in the presence of the police involuntarily and that may be a factor in determining that the privilege was not lost even though the statement was made in the presence and hearing of the police. For example had the accused indicated she wished to speak to her solicitor in private, the claim would probably be upheld notwithstanding that it was made in the presence and hearing of police.

63 Ibid 549.

64 [2003] NSWSC 1117.

65 The phrase 'confidential document' is given a very similar definition.

66 ALRC, *Evidence*, Interim Report No 26 (1985) vol 1, [879], quoted in *R v Sharp* [2003] NSWSC 1117 [32].

But on the evidence before me I do not believe that the accused intended that the conversation be confidential and the police had no reason to believe that it was. They were unaware that the accused was speaking with her solicitor. Because the statement was not made, or intended to be made, in confidence, the solicitor was, therefore, under no obligation not to disclose it. It was not a 'confidential communication' within the meaning of that term in s 117 and there was no privilege in it. It was thus unnecessary for me to consider whether any privilege in the statement had been waived by the voluntary disclosure of it to the police.⁶⁷

Applying this approach to the situation under the *ASIO Act*, it seems that the mere fact that the communication is being monitored will not be decisive on the confidentiality issue, particularly given that this is beyond the control of the subject and the lawyer. What will be most significant is the intention of the subject and his or her lawyer in relation to confidentiality: did they intend that the communications between them be confidential, notwithstanding their awareness of the fact that their communications were being monitored? This is likely to be a difficult issue: one can even imagine a lawyer quite properly advising a subject that the communication is not confidential because it is monitored, and to avoid saying anything incriminating for that reason. Indeed, lawyers in this situation will face a genuine dilemma. On the one hand, they could effectively ignore the fact of monitoring and treat the communication as confidential, thereby ensuring that the communication was privileged, but also enabling ASIO to be aware, through its monitoring, of all of this confidential material. On the other hand, in order to protect the client from disclosing such material to ASIO, the lawyer could approach the interview on the basis that it was not confidential, with the result that it may not be privileged. That said, Australian courts are no doubt likely to try and ensure that privilege does apply in these circumstances. Nevertheless, if Parliament truly does wish to ensure that legal professional privilege is not affected, it seems that further amendments to the *ASIO Act* will be necessary.

2 Privilege against Self-Incrimination and the Admissibility of Evidence Obtained during Questioning

It is customary, when abolishing the privilege against self-incrimination⁶⁸ and compelling persons to provide self-incriminating evidence, to exchange one form of protection – the privilege – for another, namely immunity from having this evidence used against them in court. Section 34G(9) does limit the use of any evidence obtained from a subject during questioning, but the limitations are partial and curious. Generally speaking, there are two kinds of immunities that can be offered: use immunity, and derivative use immunity. Use immunity merely prohibits the use of the actual evidence given by the person; derivative use immunity also prohibits the use of any evidence obtained as a result of that evidence.

Section 128 of the Uniform Evidence Legislation, for example, provides that a witness can be compelled to give evidence that would incriminate them if the

67 *R v Sharp* [2003] NSWSC 1117, [36]–[37].

68 See discussion above in Part II(A)(6).

court considers that the interests of justice require that the witness give the evidence. A witness who is so compelled must be given a certificate in respect of the evidence; that certificate prohibits the use of both the evidence given by the person, and 'evidence of any information, document or thing obtained as a direct or indirect consequence of the person having given evidence'.⁶⁹ This is an example of derivative use immunity. Examples of use immunity, on the other hand, are found in s 30(5) of the *Australian Crime Commission Act 2002* (Cth) and s 68(3) of the *Australian Securities and Investments Commission Act 2001* (Cth).

Like those latter statutes, s 34G(9)(a) of the *ASIO Act* only confers use immunity; that is, it declares inadmissible anything said by the subject, while before a prescribed authority for questioning, in criminal proceedings against them (other than criminal proceedings for an offence under s 34G). It does not, however, prohibit the use of any evidence obtained as a result of anything said by the subject: there is no derivative use immunity. Even more limited is the curiously drafted s 34G(9)(b), which declares inadmissible 'the production of a record or thing by the [subject], while before a prescribed authority for questioning under warrant'. Again, there is no derivative use immunity; any evidence obtained or discovered as a result of the production of the record or thing can be used against the subject. What is of real concern, though, is the fact that what s 34G(9)(b) appears to prevent the use of is the fact that a record or thing was produced by the subject, rather than the record or thing itself. Presumably this means that the record or thing could be used as evidence against the subject, provided that its relevance and authenticity could be established without reliance being placed on the fact that it was produced by the subject.

The limitation in s 34G(9)(b) is consistent with the view of some (including this author) that the privilege against self-incrimination should not extend to incriminating objects or documents which are already in existence; producing evidence which is already in existence is very different from forcing to someone to create entirely new evidence against themselves. Nevertheless, this limitation in s 34G(9)(b) can be contrasted with s 30(5) of the *Australian Crime Commission Act 2002* (Cth), which expressly renders inadmissible the document or thing produced, rather than just the fact of production. Curiously, despite the obvious difference in wording, the Explanatory Memorandum to the 2002 amendments to the *ASIO Act* suggests that the records or things produced will be inadmissible in proceedings against the subject. It is difficult to see what the basis of this claim is.

C Other Admissibility Issues

1 Use of Evidence by or against Others

Subject to the ordinary rules of evidence, evidence obtained from a subject during questioning under a warrant could be used against persons other than the subject. A record or thing produced by the subject could be used in evidence

69 Uniform Evidence Legislation s 128(7)(b).

against another person, as could the fact that it was produced by the subject, assuming these things to be relevant. What about the things said by the subject? The use immunity provisions discussed above only prevent anything said by the subject from being used against that subject; they have no operation in proceedings against a person other than the subject. The hearsay rule, however, is likely to restrict the use of things said by a subject during questioning. If the subject's answers are being used for their truth – that is, as a means of proving that the facts asserted in those answers are true – then they would be hearsay, and inadmissible for this purpose unless an exception to the hearsay rule applies. It is difficult to see what exception could apply to such evidence.⁷⁰

It would be different if it were the defence that wished to rely on the subject's answers, as, for example, where the answers were exculpatory of the accused. In proceedings in which the Uniform Evidence Legislation applied, the exception contained in s 65(8) of the Uniform Evidence Legislation might permit the use of the answers. It applies to 'a previous representation adduced by a defendant if the evidence is given by a person who saw, heard or otherwise perceived the representation being made', and the maker of the representation (that is, the subject), is unavailable to testify as a witness. A document – such as a transcript of the questioning – can also be admitted for its truth under s 65(8). At common law, there is some patchy authority supporting the existence of an analogous exception.⁷¹ The exception in s 65(8) does not apply, however, when the maker of the previous representation is a co-accused.

The answers given by the subject during questioning could, however, be used against another person if the use was not a hearsay use; that is, if the answer was not being used for its truth. One can imagine, for example, that a subject's answer might reveal knowledge that they could only have got from a specific source. Perhaps, their answer reveals that they are aware of certain classified information, which had only been in the hands of one or two persons. In proceedings against either or both of those persons for leaking the information, the fact that the subject had the information could provide the foundation for an inference that one or other of the persons must have leaked it to them. This would not appear to be a hearsay use, so the evidence could be admitted for that purpose. In Uniform Evidence Legislation jurisdictions (but not at common law), once evidence is admitted for a non-hearsay purpose it also becomes admissible

70 In Uniform Evidence Legislation jurisdictions, it is arguable – but in this author's view doubtful – that the subject's answers might satisfy the requirements of one or more of the exceptions contained in s 65, provided that the subject was unavailable to testify in the proceedings. In particular, the answers could conceivably satisfy the requirements of the exceptions for representations made under a duty (s 65(2)(a)), for representations against the interests of the person who made them (s 65(2)(d)) and for representations made in circumstances that make it highly probable that the representation is reliable (s 65(2)(c)). There is no common law equivalent to the third of these exceptions. While there are common law equivalents to the other two exceptions, they would only apply if the subject was dead; and both are narrower than their Uniform Evidence Legislation equivalents. See Jeremy Gans and Andrew Palmer, *Australian Principles of Evidence* (2004) 199, 204–6.

71 See Gans and Palmer, above n 70, 197–8.

for its truth, although the trial judge retains a discretion to prevent it from used for that purpose.⁷²

In joint trials, the hearsay rule would prevent a co-accused of the subject from relying on any answers given by the subject during questioning as evidence of the truth of those answers. The co-accused would also be prohibited from using the answers as a prior inconsistent statement to impugn the credibility of the subject as a witness. To use the answers in this fashion would appear to breach the use immunity provision in s 34G(9)(a) of the Act.

2 *Evidential Significance of any Breach of the Rules*

If the provisions of the Act, or the protocol,⁷³ have been breached, then it may be possible to establish that a person has been illegally or improperly detained or questioned.⁷⁴ So too, if something has occurred that constitutes a breach of some more general human rights norm.⁷⁵ If the questioning or detention was illegal or improper, then the things said, and records or things produced by the subject may be regarded as having been illegally or improperly obtained. In Australia, illegally or improperly obtained evidence is admissible, but can be excluded by the court in the exercise of the ‘public policy’ discretion recognised by the High Court in *Bunning v Cross*⁷⁶ and given statutory form by s 138 of the Uniform Evidence Legislation. This would be of no significance in relation to the admissibility of anything said by the subject during questioning in subsequent proceedings against the subject, because – as a consequence of the use immunity conferred by s 34G(9)(a) – the things said by the subject are not admissible against them in any case.⁷⁷ By contrast, the records or things produced by the subject can be used against them – because of the limited nature of that use immunity – and so could be made the subject of a public policy argument for discretionary exclusion. Public policy arguments could also be made in cases where illegally obtained evidence was being used in proceedings against a person other than the subject.

Before the discretion falls to be exercised, of course, it must be shown that some illegality or impropriety has occurred. This may be difficult, even if it is the subject who is seeking to prove that their treatment breached the provisions of the Act or the protocol. If there is no documentary evidence suggesting the occurrence of an impropriety, and persons involved in the impropriety present a united front, the only evidence of an impropriety is likely to come from the

72 Uniform Evidence Legislation ss 60, 136.

73 See discussion above in Part II(A)(4).

74 In relation to Federal Court challenges to the legality of warrants and so on, see Kerr, above n 22, 10–11.

75 Section 138(3)(f) of the Uniform Evidence Legislation specifically requires a court to take into account a breach of the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). Nevertheless, the subject will still have to persuade the court that a provision of the Covenant was breached, and that the evidence ought to be excluded as a consequence of this.

76 (1978) 141 CLR 54.

77 For the same reason, there is no point in considering whether a statement made by a subject in response to compulsory questioning can properly be regarded as ‘voluntary’, voluntariness being a condition of admissibility for confessions in criminal proceedings.

subject him or herself. The difficulties would obviously be even greater where it is a person other than the subject who is seeking to have evidence excluded on public policy grounds, because such a person will not even have any personal knowledge about how the subject was treated during detention. Unless it is possible to persuade a court that an illegality or impropriety has occurred, the evidence will not be subject to discretionary exclusion.

Another interesting issue arises in relation to the admissibility of evidence discovered as a result of the things said, or records or things produced, by the subject in circumstances of an illegality or impropriety. Such evidence is sometimes referred to as the ‘fruit of the poisoned tree’; in this case, the ‘poisoned tree’ would be the illegally obtained evidence of what the subject said or produced during questioning, the fruit of that tree is evidence obtained in consequence of it. There is very little authority in Australia in relation to whether the public policy discretion applies to such evidence. However, the wording of s 138(1)(b) of the Uniform Evidence Legislation, which refers to ‘evidence that was obtained ... *in consequence* of an impropriety or of a contravention of an Australian law’ (emphasis added), suggests that under the Uniform Evidence Legislation at least, the ‘fruit’ of the ‘poisoned tree’ may also be subject to discretionary exclusion.⁷⁸

III SECRET EVIDENCE

This part of this article deals with issues which arise in trials involving classified and security sensitive information.⁷⁹ Governments are obviously concerned to maintain the confidentiality of such information, as is their prerogative. A familiar difficulty arises when a party to litigation seeks access to information that the government does not wish to disclose; legislation before the Commonwealth Parliament seeks to establish a new mechanism for dealing with this problem, which has traditionally been dealt with through the doctrine of public interest immunity. The main provisions of the Bill are discussed in the second section of this part of the article.

A rather different problem arises when a government both wishes to maintain the secrecy of information and to use it against someone in judicial or quasi-judicial proceedings. One response might be that the government cannot have its cake and eat it too: either it should forego reliance on the evidence, or it should be prepared to allow its disclosure. Controversially, however, the ALRC has recommended that in certain circumstances the government should be permitted to use evidence against a person without having to reveal it to them. The ALRC’s proposals are dealt with in the third section of this part of the article. First, however, the article examines the background to these proposals.

⁷⁸ See Gans and Palmer, above n 70, 426–9.

⁷⁹ The various legislative proposals discussed in this part are dealt with in more detail by Patrick Emerton, ‘Conviction without Evidence: A Disturbing Trend in Australia’s “Anti-Terrorism” Laws’ (2004) 4 *Queensland University of Technology Law and Justice Journal* (forthcoming).

A Background to the Proposals

In April 2003, the Commonwealth Attorney-General made a reference to the ALRC in relation to ‘measures to protect classified and security sensitive information in the course of investigations and proceedings’.⁸⁰ The catalyst for this reference appears to have been *R v Lappas*,⁸¹ in which an employee of the Defence Intelligence Organisation was charged with offences relating to the disclosure of classified information. According to a newspaper account of the case, ‘battling depression, [Lappas] had a relationship with a prostitute, Sherryl Dowling, and to help her out of financial problems he gave her material and asked her to sell it to a foreign embassy, reportedly the Russians’.⁸² During the course of the trial, the court upheld a claim for state interest immunity in relation to two of the documents in question. However, the court also held that the withholding of the documents meant that it was not possible for the accused to receive a fair trial on a charge that related to those documents; accordingly, the prosecution on that charge was stayed.⁸³

The ALRC released its background paper, *Protecting Classified and Security Sensitive Information* in July 2003,⁸⁴ and its discussion paper of the same title (‘discussion paper’) in February 2004.⁸⁵ The key recommendations of the discussion paper included the enactment of a National Security Information Procedures Act, modelled on the *Classified Information Procedures Act* (US),⁸⁶ to deal specifically with the protection of classified and sensitive national security information in court, tribunal and other proceedings.⁸⁷ The Act would apply at all stages of proceedings in any Australian court in which classified or sensitive national security information arose.⁸⁸

The ALRC’s final Report was due to be handed down on 31 May 2004 (‘the report’), although it would not have been publicly available until tabled in Parliament. Before the report could be tabled, however, the Government introduced the National Security Information (Criminal Proceedings) Bill 2004 (Cth) (‘the Bill’).⁸⁹ The Bill adopts some, but not all, of the ALRC’s recommendations; most obviously, the Bill only deals with federal criminal proceedings, whereas the ALRC’s proposals were intended to deal with all types

80 See ALRC, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, Report No 98 (2004) 5. The final Report only became publicly available after the writing of this article was completed.

81 [2001] ACTSC 115, [30].

82 Brendan Nicholson, ‘Balance of Justice and National Security, or Blindfold for the Courts?’, *The Age* (Melbourne), 5 June 2004, 7.

83 See *R v Lappas* [2001] ACTSC 115.

84 ALRC, *Protecting Classified and Security Sensitive Information*, Background Paper No 8 (2003).

85 ALRC, above n 2.

86 18 USC Appendix (1980).

87 ALRC, above n 2, [10.1]. See also [10.2].

88 *Ibid* [10.4].

89 See Second Reading Speech, National Security Information (Criminal Proceedings) Bill 2004 (Cth), House of Representatives, 27 May 2004, (Philip Ruddock, Attorney-General); Explanatory Memorandum, National Security Information (Criminal Proceedings) Bill 2004 (Cth).

of proceeding in all Australian courts.⁹⁰ More significantly for present purposes, the Bill does not contain any provisions adopting the ALRC's recommendations to allow, in limited circumstances, evidence to be used against a person, without it being disclosed to them. This rather suggests that the Government may be intending to introduce further legislation designed to cover the proceedings not covered by the Bill. For this reason, the discussion below will deal both with the ALRC's proposed Act, and the Bill actually introduced into Parliament.

One of the main aims of both the Bill and the ALRC's proposals is to ensure the early identification of cases in which either or both of the parties might seek to rely on classified or sensitive national security information. Each party to proceedings would be required to give notice to the court and to all other parties (and under the Bill, to the Attorney-General) as soon as practicable after it became aware that classified or sensitive national security information is reasonably likely to be used in those proceedings.⁹¹ Both the Bill and the ALRC's proposals apply to the accused in criminal proceedings, thereby requiring a degree of pre-trial disclosure on the part of the defence. In making these recommendations, the ALRC relied on the fact that legislation in a number of Australian jurisdictions already requires a degree of pre-trial disclosure on the part of the defence.⁹²

B Withholding of Secret Evidence

Under the Bill, the Attorney-General may issue a certificate to a 'potential discloser' which states that they are not to disclose the information in question, but may disclose a summary, or redacted version, of the information.⁹³ Such a certificate is conclusive evidence that disclosure of the information is likely to prejudice national security.⁹⁴ If a certificate has been issued, then the court must hold a closed hearing (as described in cl 27) in order to determine whether or not to make an order under cl 29. Under cl 27, the defendant and his or her legal representatives may be excluded from those parts of the closed hearing in which the information is disclosed, if the court considers that their presence might

90 At the time of writing the Bill had been introduced in the House of Representatives and referred to the Senate Legal and Constitutional Legislation Committee. The Committee's Report, recommending a number of amendments to the Bill, was handed down in August 2004: *Inquiry into the Provisions of the National Security Information (Criminal Proceedings) Bill 2004 and the National Security Information (Criminal Proceedings) (Consequential Amendments) Bill 2004* (2004).

91 National Security Information (Criminal Proceedings) Bill 2004 (Cth) cl 22; ALRC, above n 2, [10.5]; and ALRC, above n 80, 21, Recommendation 11.6. The Bill also imposes notice requirements during the course of the trial: cl 23. Under the ALRC's proposed Act, the parties would subsequently be required to file lists of all classified or sensitive national security information that they anticipate might be used in the proceedings: ALRC, above n 2, [10.9].

92 See, eg, *Criminal Procedure Act 1986* (NSW) ss 134–51, the *Crimes (Criminal Trials) Act 1999* (Vic), and the *Criminal Code* (WA) s 611C(1), referred to in ALRC, above n 2, [10.20]–[10.36].

93 National Security Information (Criminal Proceedings) Bill 2004 (Cth) cl 24; see also ALRC, above n 2, [10.32].

94 National Security Information (Criminal Proceedings) Bill 2004 (Cth) cl 25(1).

prejudice national security.⁹⁵ As a result, a hearing that determines whether or not relevant information should be made available to the defence may effectively be conducted without any input from the defendant.⁹⁶

Clause 29 allows the court to take a different view from the Attorney-General, either by allowing disclosure of the information, or by permitting disclosure in the form of a redacted copy or summary, which may be different from the summary or redacted copy that the Attorney-General would have permitted. Before making any such order, the court must first decide whether or not the information is admissible; if the court decides that the evidence is not admissible, then it is not permitted to make the order. In deciding whether to make an order, the court must take into account any adverse effect on the defendant's right to receive a fair hearing, but must give greatest weight to the risk of prejudice to national security (as conclusively evidenced by the fact that the Attorney-General has issued a certificate).⁹⁷

These provisions differ from the ALRC's proposals, which would have made an Attorney-General's certificate stipulating that information was not to be disclosed, or was only to be disclosed in a particular form, conclusive.⁹⁸ The conclusiveness of the certificate would obviously raise the concern that a party might be hampered in its ability to present its case, or to test its opponent's case, by restrictions on the use of classified evidence,⁹⁹ as well as the prospect of a court reaching the wrong decision because not all of the relevant information is before it. The ALRC's response to this concern was to provide that, once such a certificate had been issued, the court would have to determine whether in light of the unavailability of the information referred to in the certificate, the proceedings should be stayed, discontinued, dismissed or struck out in part or in whole.¹⁰⁰

The ALRC's proposals can be contrasted with public interest immunity (and its statutory equivalent contained in s 130 of the Uniform Evidence Legislation). With public interest immunity a party to the proceeding, or a third party such as the government, may claim that it is contrary to the public interest for particular information to be disclosed. However, it is for the court to decide where the balance of public interest lies, and so to decide whether or not the information will in fact be disclosed. While it is true that an executive claim that disclosure of certain information would jeopardise national security is likely to be treated with the utmost deference by the judiciary, the fact remains that the question of disclosure is ultimately a decision for the judiciary and not the executive.

95 Clause 34 of the Bill contains provisions relating to security clearances for defence lawyers. These provisions have been strongly objected to by the Law Council of Australia: Submission 8 to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, discussed in ALRC, above n 90. A lawyer without a security clearance is obviously much more likely to be excluded from the closed hearing than one who does, so the Bill effectively contains heavy incentives to encourage a defendant to engage a lawyer who has a security clearance.

96 These provisions have also been strongly objected to by the Law Council of Australia: see ALRC, above n 90, [3.52].

97 National Security Information (Criminal Proceedings) Bill 2004 (Cth) cl 25(1).

98 ALRC, above n 2, [10.32].

99 Cf *Alister v R* (1984) 154 CLR 404.

100 ALRC, above n 2, [10.32].

Although nothing in the ALRC's proposals (or in the Bill for that matter) would affect the right of a party or the Government to make a claim for public interest immunity,¹⁰¹ the issuing of a conclusive certificate would seem to be a more attractive option for the government than having its claim for immunity queried by the parties and determined by the court.

As it turns out, however, the provisions of the Bill actually have more in common with public interest immunity – in particular, the fact that a court may effectively overrule the certificate – than they do with the ALRC's proposals. Indeed, given the similarities to public interest immunity, one might question whether there is actually any need for this legislation. Another contrast with the ALRC's proposals is the fact that the Bill does not require the court to consider whether the unavailability of any information pursuant to an order under cl 29 means that the proceedings should be stayed or dismissed. The general powers of the court in relation to the conduct of proceedings are retained by cl 18, and no doubt this includes the power to stay or dismiss proceedings, as in *R v Lappas*. Nevertheless, the omission of a specific provision requiring the court to consider making such an order is unfortunate. The assumption seems to be that in determining what orders, if any, to make under cl 29, the court will be able both to protect the interest in national security, and to ensure that the accused receives a fair trial. Yet, as the ALRC's proposals recognise, and as *R v Lappas* demonstrated, the question as to whether information should be disclosed, and the question as to whether – if the information is not to be disclosed – the accused can receive a fair trial, are fundamentally separate questions.

C Use of Secret Evidence

Rather different issues are raised by the ALRC's proposals in relation to the use of secret evidence; that is, proposals which would allow a court to act on information adduced by one party to the proceedings without it being disclosed to the other party.¹⁰² Any such proposal raises very serious fairness concerns about the ability of a party to test its opponent's case, because it is impossible for a party to test a case based on evidence that is withheld from it.¹⁰³ Indeed, the use of secret evidence is very much at odds with our common law legal culture, which is based on the idea that it is the adversarial parties to a proceeding who are best able to determine what evidence is relevant, and to decide whether, and how, to challenge evidence adduced by an opponent. To remove the adversary from some part of the proceedings is to fundamentally change the nature of those proceedings. Moreover, secret evidence based on information provided by intelligence agencies seems to be just the kind of evidence that ought to be subjected to a vigorous process of testing by an adversary. As the ALRC noted:

101 See *ibid* [10.12].

102 These proposals are not included in the National Security Information (Criminal Proceedings) Bill 2004.

103 See, eg, *Statement of Professor David Cole, Georgetown University Law Centre on the Use of Secret Evidence in Immigration Proceedings and HR 2121 Before the House Judiciary Committee* (2000), referred to in ALRC, above n 90, 378–9.

There is a real concern that secret proceedings tend to encourage reliance on questionable evidence, including double and triple hearsay. When the secret evidence consists of hearsay, it is impossible even for the judge to question the sources. ... Rumour and innuendo collected by the investigative agencies can be accorded too much weight when it becomes 'evidence' – especially in secret, when there is no opposing party to challenge it or provide the context.¹⁰⁴

In light of these concerns, the ALRC accepted that in criminal proceedings the defence should have access to all evidence to be used against them: in other words, the ALRC rejected the idea that the prosecution could ever seek to rely on evidence which was not disclosed to the accused and his or her legal representatives.¹⁰⁵ The Bill does not allow this either. While the ALRC's original proposals would have allowed the use of secret evidence in any civil proceedings before a court or tribunal,¹⁰⁶ its final Report recommended that secret evidence should only be able to be used in proceedings before a tribunal, or which involve judicial review of administrative decisions withholding evidence or based on evidence withheld from a party.¹⁰⁷ Although the outcome of such proceedings can have serious consequences – such as deportation – the ALRC sought to minimise the problems flowing from the use of secret evidence by providing that such evidence could only be used when certain safeguards were met. First, secret evidence should not be allowed where it is 'the only or the major piece of evidence against the absent party'.¹⁰⁸ Secondly, it should only be permitted in 'the most extraordinary circumstances', and subject to a number of 'safeguards', including the following:¹⁰⁹

- the court or tribunal should first consider alternative methods of presenting the evidence, such as redaction, the use of summaries and so on;
- the person against whom the evidence is being led should be represented, even if it is not by a lawyer of their choosing, but by a court-appointed lawyer who has the necessary security clearance;
- the person against whom the secret evidence is led should be able to appeal against the decision that it is not to be disclosed to them;
- the person against whom the secret evidence is led should be notified of the fact that secret evidence is being relied on; and
- the normal rules of evidence should apply to the secret evidence.

No doubt these safeguards do go some way to alleviating the concerns to which the use of secret evidence inevitably gives rise; but they still leave a number of questions unanswered. For example, how effective in challenging secret evidence is a court-appointed lawyer likely to be, given that he or she is presumably not permitted to reveal to his or her client what the evidence actually is in order to obtain instructions? The application of the 'normal rules' of

104 ALRC, above n 2, [9.8]. See also ALRC, above n 95, 379; Submission 11 to ALRC, *Inquiry into Protecting Classified and Security Sensitive Information* (2004) (Law Council of Australia).

105 ALRC, above n 2, [10.38]; and ALRC, above n 95, 481.

106 See ALRC, above n 2, [10.136]. Because the Bill only applies to federal criminal proceedings, it does not address this issue.

107 ALRC, above n 95, 482.

108 ALRC, above n 2, [10.39].

109 Ibid [10.40]; ALRC, above n 95, 495–6.

evidence may eliminate some of the concerns raised by the use of hearsay evidence, but in many tribunals the normal rules of evidence do not apply. The ALRC's intention, however, seems to be that where secret evidence is to be relied on, the normal rules of evidence – such as the hearsay rule – should apply to that evidence, even if those rules are not otherwise applied in that tribunal.¹¹⁰

IV SUMMARY

The counter-terrorism legislation pushes the boundaries of the law of evidence in a number of ways:

- The investigative powers given to ASIO go far beyond those available to other investigative bodies. In particular, ASIO has the power to seek warrants that could allow a person to be taken into custody for the purposes of questioning for up to seven days at a time, without there needing to be any grounds for believing that the person had committed, or was about to commit an offence.
- It is an offence punishable by up to five years imprisonment for a person in respect of whom a warrant has been issued to fail to provide information that he or she has been asked to provide, notwithstanding that the information may be self-incriminating. While anything said by the person in response to such a demand for information can not be used against them in any subsequent criminal proceedings, evidence obtained or discovered as a result of what they say can be used. There is also some doubt about whether or not any record or things produced by the person are immune from use, or whether it is only the fact of production – rather than the things produced – which can not be used.
- The right to communicate with a lawyer is recognised, but is subject to a number of limitations; most worryingly, and despite a specific provision which states that legal professional privilege is not affected, there are serious doubts about whether or not legal professional privilege would apply to communications between a person detained under the legislation and their lawyer.

The legislation that has been proposed to deal with the use of classified and sensitive national security information would also modify the law of evidence:

- The National Security Information (Criminal Proceedings) Bill 2004 (Cth) sets up a new mechanism for determining whether security sensitive information should be disclosed in criminal proceedings. This new procedure would effectively replace public interest immunity in those proceedings in which it applies.

110 ALRC, above n 2, [10.137].

- The ALRC has also proposed legislation that would permit a court or tribunal to act on evidence that was withheld from the party against whom it was being used.