Submission No 36

Inquiry into potential reforms of National Security Legislation

Name: J Blackbourn (Post-Doctoral Fellow)
F Davis (Senior Lecturer)
K Hardy (Doctoral Candidate)
N McGarrity (Lecturer)
G Williams AO (Anthony Mason Professor and Laureate Fellow)

Organisation: Gilbert + Tobin Centre of Public Law
Faculty of Law
University of New South Wales
Law Building
Sydney NSW 2052

I GENERAL REMARKS ON THE INQUIRY AND THE DISCUSSION PAPER

a. The timing of the inquiry

We welcome the pre-emptive nature of this inquiry. A common criticism of national security and anti-terrorism legislation is that it is rushed through parliament as a response to some act or outrage:

> 'Emergency legislation passed as a consequence of national catastrophe associated with terrorism has a predictable pattern. It involves an unseemly scramble between the Executive and legislature so that they are seen by the public and the media to be doing "something." A previously prepared emergency Bill is dusted down and hastily pushed through the legislature. Policy and law are thereby tightened, with scant recourse to reasoned chamber debate or recognition of standard procedures, in order to respond to the media and public outcry. Thus, the politicians' anxiety to be viewed as resolving the crisis overrides both established process and rational action.'[1]

By contrast, the current inquiry is being conducted at a time of relative calm and without any sense of moral panic. Furthermore, the extension of the original deadline for submissions is welcomed. While the initial timeframe was too short, the revised deadline provides a suitable period for consideration of the complex issues involved.

b. Lack of detail

The Discussion Paper seems to be designed to initiate a conversation about a wide range of potential reforms. We deal in the other Parts of this Submission with a number of the proposals, however, it is important to stress that, as a wide-ranging document, the Discussion Paper often lacks specific detail. This makes it impossible to reach firm conclusions about the proposals. In order to comment usefully, especially on some of the more technological proposals, we would need enhanced detail. For example, paragraph 15(c) of the Terms of Reference contains a proposal to create a mandatory two year period of data retention. This is not given any attention in the Discussion Paper. The lack of detail in the Discussion Paper contrasts unfavourably with the National Security Legislation Discussion Paper released by the Rudd Government in July 2009. This Discussion Paper included not only detailed discussion of the proposals but also draft legislation.

---

[1] Philip Thomas, 'Emergency and Anti-Terrorist Powers: 9/11 – USA and UK' (2002-03) 26 *Fordham International Law Journal* 1209, 1196.

The task of reaching conclusions on the proposals is also made more difficult by the complicated relationship between the proposals. One legislative amendment may have a knock-on effect elsewhere. As a result, it is important that the Discussion Paper is viewed as a starting point only. Consideration of the various proposals by the Committee is not a substitute for further review by the Parliament, relevant parliamentary committees and the public of more detailed legislative proposals as they arise.

c. The issue of 'omnibus' legislation

The broad range of issues under consideration gives rise to what might be termed an 'omnibus' of provisions. Such an approach has been a feature of anti-terrorism laws over the past decade. In this context 'omnibus' refers to the length and impact of the legislation. The US Patriot Act was over 350 pages long and amended over twenty Federal Acts.[2] Scrutinising such legislation and debating the provisions meaningfully is extremely difficult. As Professor Kent Roach has noted, in the context of the Canadian Charter of Rights, effective debate and scrutiny of legislation should be accessible to the public and should act to demystify legal complexity. That is difficult where the measures under consideration are so wide ranging and complicated.

A further problem with the 'omnibus approach' is that it can be difficult to wind back the legislation if a future parliament re-evaluates the security risk. For example, following a 2011 review of anti-terrorism laws, the United Kingdom Government of Prime Minister David Cameron appeared ready and willing to undo prior intrusions into human rights. However, the resulting Protection of Freedoms Bill contained a multitude of provisions relating to anti-terrorism, data retention, CCTV and more. As such, the repealing Bill was itself an example of 'omnibus' legislation. This led one member of the House of Lords to comment:

> This Bill is a mish-mash of ill-sorted provisions, a mish-mash without any overarching or underpinning philosophy and, worst of all, a mish-mash that will bring about unintended and damaging consequences.[3]

For these reasons, we would advise against the 'omnibus' approach. Distinct pieces of legislation for each individual issue being addressed are preferable. Such an approach makes the purpose of the legislation clear to the public and parliamentarians and facilitates engaged debate and effective scrutiny. Furthermore, if and when it becomes appropriate to scale back

---

2 See also, for example, the UK Anti-Terror Crime and Security Act 2001 and the Security Legislation Amendment (Terrorism) Act 2002.

3 United Kingdom, *Parliamentary Debates*, House of Lords, 8 November 2011, vol 732, 203 (Lord Harris).

the state's national security response, separate pieces of legislation are easier to identify and to amend.

d. The new human rights framework

The altered parliamentary framework arising from the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) (*'Parliamentary Scrutiny Act'*) ought to be acknowledged. Australia has adopted a unique system of human rights protection. This system relies on Parliament and, by extension, Parliamentary Committees to ensure human rights compliance. It is premised on Parliament having a culture of human rights scrutiny.

Part 3 of the Act requires that the Member of Parliament who proposes legislation should make a 'statement of compatibility' in relation to the proposed Bill. It would be appropriate for a Discussion Paper such as this one to begin the legislative process by considering the potential compatibility of any proposals. This would assist Members of Parliament in making their 'statement of compatibility' as well as providing useful background information for the Parliamentary debate regarding the supposed compatibility of legislation with human rights. Such an approach would place human rights at the centre of the legislative process and would greatly facilitate the working of the Parliamentary Scrutiny model of human rights protection.

This is particularly important for the current Discussion Paper because the national security context is one which gives rise to significant challenges to human rights. In the decade after the 9/11 terrorist attacks, Australia has adopted a range of anti-terrorism measures that significantly impact on the rights of citizens. Many of the proposals contained in the Discussion Paper have similar potential. While the Joint Committee almost certainly is conscious of this, it is important that the human rights compliance of proposals is overtly addressed. This is especially true give that the *Parliamentary Scrutiny Act* places the sole responsibility for human rights scrutiny on the Parliament.

e. A strong accountability framework

The Discussion Paper makes a number of proposals to modernise and streamline the warrants regimes for intelligence and law enforcement agencies. The cumulative effect of the proposals is to significantly expand the powers of intelligence and law enforcement agencies and, in so doing, to diminish the privacy of Australians. The Discussion Paper states that the aim of the proposals is to equip intelligence and law enforcement agencies 'with contemporary skills and technologies, and backed by necessary powers – *coupled with the appropriate checks and balances and oversight mechanisms society rightly demands*'

(emphasis added).[4] The Discussion Paper does not, however, provide any details. We are concerned that at the same time as the warrant powers are expanded, there will be a weakening of the existing accountability framework.

The Discussion Paper emphasises, at a number of points, that there is a need to reassess the balance between the individual's right to privacy and the public interest in the protection of national security. This is particularly evident in the proposal to amend the current record-keeping regime. The Discussion Paper proposes to 'introduc[e] new reporting requirements that are *less process oriented* and more attuned to providing the information needed to *evaluate whether intrusion to privacy under the regime is proportionate to public outcomes*' (emphasis added).[5] The Discussion Paper goes on to state that the current record-keeping regime reflects 'historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which the agencies operate'.[6] This is incorrect. The recent cases of Izhar Ul-Haque and Joseph Thomas, from the anti-terrorism context, indicate that there is a very real potential for Australian intelligence and law enforcement officers to act improperly and even illegally. A strong accountability framework must be maintained to ensure that corruption and abuses of power do not occur.

II EXPANSION OF WARRANT POWERS UNDER THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979* (CTH) ('*TIA ACT*')

a. Standardisation of warrant thresholds

The Australian Government proposes in paragraph 2(b) of the Terms of Reference to standardise the threshold for issuing telecommunications interception and stored communications warrants under the *TIA Act*.[7] Currently, a telecommunications interception warrant may be sought by a law enforcement agency in relation to a 'serious offence'.[8] In general terms, this is defined as an offence punishable by a maximum period of at least *seven years imprisonment* (and which satisfies certain other criteria).[9] The definition also deems a long list of other offences to be serious offences.[10] In 2006, a separate warrants regime was enacted enabling agencies to access stored communications.[11] Such a warrant may be sought

4 Discussion Paper, 3.
5 Discussion Paper, 26.
6 Discussion Paper, 26.
7 Discussion Paper, 23-34.
8 *TIA Act* s 46(1)(d).
9 *TIA Act* ss 5D(2) and (3).
10 *TIA Act* ss 5D(3AA)-(9).
11 *Telecommunications (Interception) Amendment Act 2006* (Cth).

in relation to 'serious contraventions.'[12] These are defined as offences punishable by at least *three years imprisonment*.[13]

There are clear benefits to standardisation. As the Discussion Paper states, it would 'remove the complexities inherent in the current interpretation of what is a serious offence'.[14] It is also incorrect, as a matter of principle, to differentiate between telecommunications interception and access to stored communications. Their impact on the right to privacy is the same. In March 2006, one of the authors of this submission, Professor Williams, gave evidence to the Senate Legal and Constitutional Affairs Committee that:

> [I]t strikes me as strange that there would be a double standard here between stored communications of the type we are dealing with and other forms of communications such as voice. Indeed, the thresholds and tests that apply to those different types of communications are different. It strikes me as nonsensical that a differentiation would be drawn between speaking to somebody on a mobile phone and sending them an SMS message. Many of the students whom I teach today see them as equivalent forms of communication. It makes no sense as a matter of law or public policy why, indeed, it is easier to gain one type of information than the other.[15]

The real issue is which offences are of a sufficient gravity that they justify the interception of telecommunications and access to stored communications. The Australian Government suggests in the Discussion Paper that a three year threshold should be adopted. We disagree. The thresholds should be standardised by raising the threshold for stored communications to seven years. In the alternative, the seven year threshold for telecommunications interception warrants should be maintained. The benefits of standardisation should not be based on a lowest common denominator approach that allows a greater override of the right to privacy.

Article 17(1) of the International Covenant on Civil and Political Rights relevantly provides that '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence'. Interference with this right by intercepting a person's communications should only be permitted to the extent that it is necessary and proportionate to protect Australians from serious criminal offending. Indeed, if interference was disproportionate a Member of Parliament could not in good faith make a statement of compatibility with the *Parliamentary Scrutiny Act*. It must be kept in mind that the warrant threshold refers to the maximum penalty available. Many offences with a maximum penalty

---

12 *TIA Act* s 116(1)(d).
13 *TIA Act* s 5E.
14 Discussion Paper, 24.
15 Senate Legal and Constitutional Affairs Committee, Australian Parliament, *Hansard*, 15 March 2006, 28, 31 (George Williams).

of three years imprisonment capture conduct that is relatively minor in nature. These offences may ultimately be punished by only a very short period of imprisonment (if at all). Therefore, a lowering of the threshold for telecommunications interception from seven to three years would capture criminality that is not of a serious level.

The telecommunications interception regime does not only affect the right to privacy of those who have committed crimes. A warrant may certainly be sought to intercept Person A's communications if it is suspected that he or she has committed a crime. However, the regime also impacts on the right to privacy of innocent third parties in two main ways. First, it is common sense that the issue of a warrant to intercept Person A's communications also impacts on the right to privacy of any person who communicates with him or her. Second, a warrant may be sought to intercept a telecommunications service belonging to Person B where it is likely that Person A will communicate using that service ('B-Party warrants').[16] Person B could be a spouse, child, lawyer or clergyman. Given this significant impact on innocent third parties, the New South Wales Council for Civil Liberties argued before the Senate Legal and Constitutional Affairs Committee in 2006 that the seven year threshold for telecommunications interception was too low to apply to B-Party warrants. The 'threshold [for B-Party warrants] should be where life is at risk or where life has been taken. That way, you catch real terrorism offences and you would catch murder cases, I guess'.[17] This argument was rejected. The threshold for all telecommunications interception warrants remained at seven years.

Telecommunications interceptions are particularly concerning because of their covert nature. The person whose telecommunications are intercepted does not have an opportunity to challenge the warrant or to defend himself or herself against false inferences that are drawn. This increases the likelihood that the interception power may be abused. Therefore, a very cautious approach must be taken to any broadening of the circumstances in which a warrant may be issued.

The Discussion Paper criticises the seven year threshold for telecommunications interception warrants as 'too high to cover a range of offences for which it is already recognised that general community standards would expect interception to be available'. The examples that are given are 'child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks (including offences committed using a computer or involving telecommunications networks)'.[18] If the Australian Government is

[16] See, for example, *TIA Act* ss 9(1)(a) and 46(1)(d).
[17] Senate Legal and Constitutional Affairs Committee, Australian Parliament, *Hansard*, 15 March 2006, 79 (Richard Bibby).
[18] Discussion Paper, 24.

only able to point to a couple of offences that are not currently captured by the telecommunications interception regime, it would appear to be an overreaction to reduce the threshold across the board from seven to three years. Instead, these offences should be included in the same ad hoc fashion as has been employed in the past.

The Australian Government suggests that any negative effects of such an amendment could be mitigated by simultaneously 'reducing the number of agencies able to access communications information on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so'.[19] We support this suggestion. However, it should not be an excuse for reducing the threshold for telecommunications interception.

b. Creation of a single warrant

Paragraph 8(a) of the Terms of Reference proposes creating a single warrant with multiple telecommunications interception powers.

The Discussion Paper provides some background information about the difficulties faced by law enforcement and intelligence agencies in identifying and capturing the multiplicity of means by which a person communicates.[20] This is presumably the issue to which this proposal is responding. However, the Discussion Paper does not give any details of the proposal itself.

The *TIA Act* currently provides for three warrants for law enforcement agencies to intercept real-time communications. These are: a 'telecommunications service' warrant (which authorises the interception of only one service, such as a single telephone number);[21] a 'named person' warrant (which authorises the interception of any telecommunication services or devices that are likely to be used by the person named in the warrant);[22] and, a warrant authorising 'entry on premises' in order to carry out a telecommunications service warrant.[23]

There is a further category of warrant in the *TIA Act* which authorises access to stored communications.[24] The proposal in paragraph 8(a) refers only to 'creating a single warrant with multiple *telecommunications interception* powers'. We therefore assume that a separate category of stored communication warrants would remain. If we are incorrect in this, the

[19] Discussion Paper, 24.
[20] Discussion Paper, 18-25.
[21] *TIA Act* s 46.
[22] *TIA Act* s 46A.
[23] *TIA Act* s 48.
[24] *TIA Act* s 116.

telecommunications interception and stored communications warrants should only be merged if a highest common denominator approach is adopted. As we have already discussed, the threshold for obtaining a telecommunications interception warrant is higher than for a stored communications warrant. The higher threshold should be adopted if a single category of warrant is created.[25] This issue does not arise if the proposal is limited to the three categories of telecommunications interception warrants. The same threshold applies to each of these.

This does not mean that the proposal in paragraph 8(a) is without any problems. The most recent report of the Attorney-General's Department into the operation of the *TIA Act* states that a named person warrant has a 'high impact on privacy'.[26] It should only be used 'when necessary and other alternative methods are not available'.[27] Therefore, in the majority of cases, law enforcement agencies obtain a telecommunications service warrant rather than a named person warrant.[28] This is the correct approach. Any intrusions into the right to privacy should be the minimum required to achieve the public purpose. We are concerned that merging of named person warrants and telecommunications service warrants into a single category of warrant would result in law enforcement agencies using all the powers that are available to them (regardless of whether these powers are strictly necessary to investigate the criminal activity).

III EXPANSION OF WARRANT POWERS UNDER THE *AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION ACT 1979* (CTH) ('*ASIO ACT*')

a. Creation of a single warrant

Paragraph 11(a) of the Terms of Reference states that the Australian Government is considering whether to create a single category of warrant covering multiple warrant powers under the *ASIO Act*.[29]

---

[25] A stored communication may be accessed under an interception warrant if the warrant would have authorised interception of the communication if it were still passing over a telecommunications system: *TIA* s 108. This avoids the need for a separate warrant to be sought. It is appropriate 'as the agency *has met the higher threshold* needed to obtain the interception warrant, but it would be administratively burdensome for them to also have to obtain a stored communications warrant' (emphasis added). See Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 2006 (Cth) 10.

[26] *Telecommunications (Interception and Access) Act 1979 Report for the Year Ending 30 June 2011* (2011) 22.

[27] *Telecommunications (Interception and Access) Act 1979 Report for the Year Ending 30 June 2011* (2011) 22.

[28] 628 named person warrants were issued in the 2010/11 reporting period whereas 3,488 telecommunications service warrants were issued: *Telecommunications (Interception and Access) Act 1979 Report for the Year Ending 30 June 2011* (2011) 18, 22-23.

[29] Discussion Paper, 47.

We assume that this proposal does not extend to the special powers of coercive questioning and detention in Pt III Div 3. Even still, there are a broad range of other warrant powers available to ASIO under Pt III Div 2. These include search warrants, computer access warrant, listening device warrants, tracking device warrants, postal article warrants and delivery service article warrants. There are a few possibilities as to how the merging of these warrant powers into a single warrant could operate. Below we examine two possibilities.

The first is that the effect of the single warrant would be simply to reduce the amount of paperwork. That is, ASIO would complete one application (instead of multiple) and there would be one warrant issued (instead of multiple). However, ASIO would have to nominate in the application which of the warrant powers it was seeking and satisfy the relevant legislative thresholds for each of these. We have no objection to a proposal along these lines.

The second is that the single warrant would involve a *single legislative threshold* for all the warrant powers. At present, there are two discrete thresholds for the issue of Pt III Div 2 warrants (depending on what type of powers they grant). Search warrants and computer access warrants require the Minister to be satisfied that there are reasonable grounds for believing that access by ASIO to records or other things on particular premises[30] or to data held in a particular computer[31] will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.[32] The other warrants involve a two-stage process:

a. The person is engaged in, or reasonably suspected by the Director General of being engaged in or of being likely to engage in activities prejudicial to security;[33] and,

b. The use of listening or tracking devices or access to postal or delivery service articles will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security.[34]

In requiring reasonable suspicion that the person is engaging, or is likely to engage, in activities prejudicial to security, the latter threshold is significantly higher than that for search warrants and computer access warrants. If a single legislative threshold is adopted, we therefore recommended that it be the latter threshold. Simplifying ASIO warrants must not also have the effect of weakening the accountability framework.

---

30 *ASIO Act* s 25(2).
31 *ASIO Act* s 25A(2).
32 *ASIO Act* ss 25(2) and 25A(2).
33 *ASIO Act* ss 26(3)(a), 26B(2)(a), 26C(2)(a), 27(2)(a), 27(3)(a), 27AA(3)(a) and 27AA(6)(a).
34 *ASIO Act* ss 26(3)(b), 26B(2)(b), 26C(2)(b), 27(2)(b), 27(3)(b), 27AA(3)(b) and 27AA(6)(b).

Further, ASIO should be required to specify in its application for the single warrant which of the warrant powers it is seeking. This means that ASIO must direct its mind to which of the warrant powers are necessary to carry out its functions. The single warrant should not be a carte blanche for ASIO to exercise any and all of the warrant powers. The tendency is for agencies to use all the power that is available to them.

b. Amending the definition of 'computer'

The Australian Government proposes in paragraph 5(a) of the Terms of Reference to amend the definition of a 'computer' in section 25A.[35]

This proposal would increase the number of devices that could be covered by a single computer access warrant. It would mean that a computer access warrant could be issued 'in relation to a computer, computers on a particular premises, computers connected to a particular person or a particular computer network.'[36] We are concerned that this proposal would have a disproportionate effect upon the rights of innocent third parties. For example, if ASIO wanted to gather intelligence about the activities of an academic at the University of New South Wales, it could seek a warrant to access all computers on the University's network. In our opinion, the broader the terms of the warrant, the stricter should be the criteria applying to its issue. ASIO should not be able to seek a warrant to access the computers on a particular network unless there are reasonable grounds to believe that the person in relation to whom intelligence is being sought had a connection with computers other than his own on the network.

c. Introduction of person search warrants

Paragraph 11(d) of the Terms of Reference states that the Australian Government is considering whether to create a separate category of person search warrant. ASIO has very limited powers to conduct a person search. It may only conduct a search if: (a) it is specified in the warrant; (b) the person is 'at or near' the premises where the warrant is being executed; and (c) 'there is reasonable cause to believe that the person has on his or her person records or other things relevant to the security matter'.[37] The Discussion Paper states that this power is insufficient because:

---

35 Discussion Paper, 41.
36 Discussion Paper, 41.
37 *ASIO Act* s 25A(4A)(a).

> [I]t is not always feasible to execute a search warrant on a person of interest where they are "at or near" the premises specified in the warrant'.[38] Instead, a separate category of person search warrant should be created. For example, some persons of interest employ counter-surveillance techniques such that predicting the likely timing and location at which a search would yield the desired intelligence dividend is not always possible.[39]

Therefore, the proposal is to allow ASIO to apply for a warrant to search a person, regardless of whether a premises search warrant has been issued and where the person is.

The power to search a person is highly intrusive in nature. It should only be bestowed upon agencies that exercise their powers in a transparent manner and are subject to a rigorous accountability framework. Law enforcement agencies fall within this category. However, ASIO does not. It should therefore be with great caution that ASIO's power to conduct person searches is expanded. No clear justification has been given for such an expansion. There are adequate powers for law enforcement officers to search a person. To give ASIO an independent power to search a person would blur the distinction between intelligence gathering and law enforcement. It would grant what is essentially a law enforcement power to a domestic intelligence agency. The distinction between law enforcement and intelligence gathering functions plays an important role in protecting the civil liberties of Australians. For these reasons, we oppose the proposal to give ASIO a separate category of person search warrant.

However, in the event that a separate category of person search warrant is established, ASIO searches must be accompanied by similar safeguards as apply to searches by law enforcement officers. If not, there is a risk that ASIO searches will be used as a means of circumventing the safeguards attaching to law enforcement searches. It must be noted that our primary recommendation is that set out above, namely, that a separate category of person search warrant should not be created. Nevertheless, in the interests of completeness, we now examine the minimum level of safeguards that should be attached to any power – regardless of whom exercises it – to search a person.

First, person search warrants should be issued by an independent judicial officer. At present, a premises search warrant may be issued by the Attorney-General. Second, a reasonable suspicion requirement should be included. For example, s 3E(2) of the *Crimes Act 1914* (Cth) provides that a person search warrant may be issued if there are reasonable grounds for suspecting that the person has, or within the next 72 hours will have, in his or her possession

[38] Discussion Paper, 48.
[39] Discussion Paper, 48.

any evidential material. 'Evidential material' means a thing relevant to an offence (whether indictable or summary). We do not believe it is appropriate for highly intrusive powers, such as person searches, to be used for 'fishing' purposes. Therefore, strict limits must be imposed on ASIO's ability to obtain a person search warrant. Third, it would not be appropriate for the person to be informed of the reasons for the search (as is the case for law enforcement agencies). However, he or she must be informed of the identity of the agency conducting the search and to whom he or she may make complaints. Fourth, the search must be conducted in public. Fifth, the warrant should operate for only a short period of time. Under s 3E, a warrant may operate for a maximum of seven days. In contrast, premises search warrants currently operate for 90 days (and there is a proposal to double this period to six months). Finally, the search should be no more intrusive than is reasonably necessary in the circumstances. As part of this, only one search may be conducted under the warrant. This limits the potential for ASIO to use the search power to harass a particular person.

d. Doubling the length of search warrants

The Australian Government proposes in paragraph 5(b) of the Terms of Reference to more than double the duration of search warrants from 90 days to six months.[40]

This is an example of how the Australian Government's concern to streamline and simplify the various warrants regimes may override the civil liberties of the individual. The vast majority of ASIO warrants may operate for a maximum of six months. Search warrants, in contrast, only operate for a maximum of 90 days.[41] There is a rational reason for this distinction. Searches, whether of premises or of person, are far more intrusive than the other ASIO warrant powers (such as the covert use of listening devices and inspection of postal articles). As a consequence, there should be greater control over search warrants by the issuing body. For example, by requiring ASIO to reconsider every 90 days whether a search warrant is necessary. If so, it must reapply to the issuing body. This is not a disproportionate administrative burden given the significant inroads that searches make into the individual's right to privacy.

e. Variation and renewal of warrants

The Australian Government proposes in paragraph 5(b) of the Terms of Reference to enable the Attorney General to vary and renew warrants.[42] In principle, we do not have an objection to this proposal. However, the proposal does not specify what criteria will be attached to an

[40] Discussion Paper, 42.
[41] *ASIO Act* s 25(10).
[42] Discussion Paper, 41-42.

application to vary or renew a warrant. The Discussion Paper simply states that it 'would provide appropriate oversight and accountability without requiring excessive administrative resources'.[43] It is therefore impossible to reach any conclusions on this proposal. We would, however, note that the criteria, especially for renewal, should not be significantly less than those for issuing a warrant in the first place. This is particularly important given the proposal to merge warrant powers into a single category of warrant. Otherwise, renewal may become a means of rolling all of the warrant powers over every six months without meaningful consideration of whether the need still exists.

IV INTRODUCTION OF AN EVIDENTIARY CERTIFICATE REGIME INTO THE *ASIO ACT*

In paragraph 17(d) of the Terms of Reference, the Australian Government requests the Committee's advice on whether an evidentiary certificate regime should be introduced to protect the identities of officers and sensitive capabilities of ASIO involved in the execution of warrants under the *ASIO Act*. The Discussion Paper proposes that the evidentiary certificate regime would be 'similar to those which exist under the *TIA* and [*Surveillance Devices Act* 2004 (Cth) ('*SD Act*')]'.[44] This would avoid the need for ASIO to rely upon public interest immunity claims or orders obtained under the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).

The purpose of an evidentiary certificate is to protect sensitive information from disclosure. It does this by acting as prima facie evidence of the matters contained therein. The tender of telecommunications intercepts and surveillance device products in court would traditionally have required witnesses to give evidence as to the method by which the material was obtained. This would adversely affect the intelligence, law enforcement and telecommunications agencies by revealing their sensitive capabilities and the identity of the officers involved.[45] The evidentiary certificate regime balances the individual's right to a fair hearing against the public interest in non-disclosure by incorporating two safeguards. First, an evidentiary certificate does not address or prove the substantive elements of an offence. The information contained therein is of a technical nature only. Second, an evidentiary certificate only operates as *prima facie* evidence. The trial judge may, for example, if there is any reason to doubt the content of a certificate, use his or her discretion under s 137 of the *Evidence Act 1995* (Cth) to exclude the evidence.[46]

---

[43] Discussion Paper, 42.
[44] Discussion Paper, 51.
[45] *R v Baladjam [No 17]* [2008] NSWSC 1439 [69].
[46] *Cheikho v R* [2008] NSWCCA 191 [177].

We accept that it would be appropriate to adopt a similar evidentiary certificate regime in respect of *some* of the warrant powers in the *ASIO Act*. That is, those warrant powers which are technological in nature. These include computer access warrants (s 25A), listening device warrants (s 26) and tracking device warrants (ss 26B and 26C). However, the *ASIO Act* also contains warrant powers that are physically intrusive in terms of their effect on both property and person. These warrants include search warrants (s 25), inspection of postal and delivery service article warrants (ss 27 and 27AA) and, most controversially, questioning and detention warrants (Pt III Div 3). It is unclear from the Discussion Paper whether the Australian Government also proposes to extend the evidentiary certificate regime to these warrant powers. We do not believe that this would be either workable or appropriate.

V CREATION OF AN AUTHORISED INTELLIGENCE OPERATIONS SCHEME FOR ASIO OFFICERS

Paragraph 10 of the Terms of Reference states that the Australian Government is considering whether to create an authorised intelligence operations scheme similar to the controlled operations scheme for law enforcement officers in Part 1AB of the *Crimes Act*.[47] The purpose of the proposal is to protect ASIO officers and human sources who become involved in criminal activity during the course of an undercover operation. The proposed scheme would allow the Director-General of Security (the head of ASIO) to issue 'authorised intelligence operation certificates'. A certificate would give ASIO officers and human sources immunity from criminal and civil liability for specified conduct for a specified period.

The *TI Act* and *ASIO Act* already allow ASIO officers, with a warrant, to perform a range of activities that would otherwise be unlawful, for example, intercepting communications and searching premises. They do not, however, have a general immunity from civil and criminal liability.[48] The same basic situation exists in the United Kingdom, New Zealand and Canada.[49] A general immunity should not be bestowed upon ASIO lightly. It should only be granted where that organisation demonstrates that it is necessary in order for its officers to perform their functions. The Discussion Paper gives the example of ASIO officers infiltrating an organisation and, in so doing, committing the offence of providing training to, or receiving training from, a terrorist organisation.[50] This example does not, however, justify the proposal.

---

47 Discussion Paper, 46.

48 ASIO officers do have immunity from liability where they commit a criminal offence under an assumed identity. This immunity only applies to an act that would not otherwise constitute a criminal offence; the act must be criminal only by virtue of the fact that the officer used an assumed identity. See *Crimes Act* s 15KQ. Section 91 of the *ASIO Act* provides that the Director-General, officers and employees are Commonwealth officers for the purposes of the *Crimes Act*.

49 See *Intelligence Services Act 1994* (UK); *New Zealand Security Intelligence Service Act 1969* (NZ) s 4A; *Canadian Security Intelligence Service Act 1985* (Can) s 20; *Criminal Code 1985* (Can) s 25(1).

50 Discussion Paper, 46. See also *Criminal Code Act 1995* (Cth) s 101.2.

If anything, it simply indicates how broadly Australia's terrorism offences have been drafted. ASIO officers may attract liability under the training offence, for example, because that offence captures conduct well in advance of the commission of an act of political violence. Furthermore, it does not distinguish between the nature of the training or the purposes for which it is undertaken. It would be extraordinary for the Australian Government to solve this problem of over-breadth by giving the Director-General of Security a power to authorise his own officers to engage in terrorist activity. This is especially so when the Commonwealth Director of Public Prosecutions has a discretion whether or not to prosecute individuals for terrorism and other offences. It is highly unlikely that an ASIO officer would be prosecuted for activities done in the course of an undercover operation.

An immunity from civil and criminal liability has typically been given to foreign intelligence agencies. This is because the activities of such agencies, in particular, spying on foreign interests, may attract liability under the criminal and civil laws of that country or under the extraterritorial operation of Australia's laws. Even then, foreign intelligence agencies have not been given a carte blanche to engage in unlawful acts. Under s 14 of the *Intelligence Services Act 2001* (Cth) ('*IS Act*'), ASIS, DSD and DIGO are granted immunity from civil and criminal liability for any act 'done outside Australia'. Those agencies also have immunity for any act which 'is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned'. This immunity does not extend to domestic acts that, in the absence of the overseas activities, would have constituted an offence. Similar limits exist in the United Kingdom. The United Kingdom Home Secretary may authorise intelligence officers (whether domestic or foreign) to engage in unlawful activity on British soil where this is necessary for the proper discharge of the functions of the foreign intelligence services.[51] In addition, the unlawful acts must be related to an 'apparatus' outside the United Kingdom.[52] The Home Secretary does not have a power to authorise MI5 officers to engage in unlawful acts on British soil for the purposes of a domestic intelligence gathering operation.

The Australian Government may be justified in giving the Director-General of Security a power to authorise unlawful activities by ASIO officers where they are engaging in intelligence gathering on foreign soil. However, is impossible to reach a conclusion on this. The Discussion Paper does not address itself to this issue. However, it would clearly be unprecedented – in light of the experience in both Australia and other comparable nations – for the Director-General of Security to be given a power to authorise unlawful activity by

---

[51] *Intelligence Services Act 1994* (UK) ss 7(1) and 7(3)(a).

[52] *Intelligence Services Act 1994* (UK) s 7(9).The definition of 'apparatus' includes any 'equipment, machinery or device and any wire or cable': *Regulation of Investigatory Powers Act 2000* (UK) s 81.

ASIO officers on domestic soil. It would also be undesirable. Therefore, our strong recommendation is that this proposal be rejected.

In the event that the proposal is progressed – whether for all intelligence activities or for foreign intelligence gathering only – strong safeguards would need to be attached to the authorised intelligence operations scheme. Guidance could be taken from the safeguards applicable to the controlled operations scheme for law enforcement officers under Pt IAB of the *Crimes Act*. It is very concerning that the proposed safeguards in the authorised intelligence operations scheme are considerably weaker than those that apply to law enforcement officers. The first weakness in the Discussion Paper's outline of the authorised intelligence operations scheme is that it does not set out any criteria for this scheme. The two main criteria for issuing a controlled operations certificate are: first, that 'a serious Commonwealth or State office with a general aspect has been, is being, or is likely to be committed'; and, second, the nature and extent of the criminal activity are such as to justify the conduct of a controlled operation.[53] These criteria ensure that immunity is only granted to law enforcement officers to investigate crimes of a sufficiently high level of seriousness. If an authorised intelligence operations scheme was established, similar criteria setting out the types of intelligence operations for which unlawful conduct may be authorised. Authorisation could, for example, be restricted to operations of a sufficient duration or level of seriousness.

Second, the Discussion Paper states that authorisation for an intelligence operation would expire after 12 months.[54] This time-limit is considerably longer than that for controlled operations certificates in the law enforcement context. A controlled operation certificate lasts only three months unless it is renewed in three month increments (up to a maximum of 24 months) by a nominated member of the Administrative Appeals Tribunal ('AAT').[55]

Third, the Discussion Paper states that authorisation for an intelligence operation would be issued by the Director-General of Security.[56] This is similar to the process for authorising a 'major controlled operation' under the *Crimes Act*. Authorisation for such an operation may only be given by the Commissioner or Deputy Commissioner of the Australian Federal Police.[57] The critical difference, however, is that the decision whether to renew a controlled operations certificate, after it has been in effect for three months, is given to the AAT. This limits the discretion of the Commissioner or Deputy Commissioner to authorise unlawful

---

53 *Crimes Act* s 15GI(2).

54 Discussion Paper, 47.

55 *Crimes Act* s 15GT. Where an 'urgent' application is made for a controlled operation, the authorisation will expire after 7 days and cannot be renewed: *Crimes Act* s 15GU(5)(b)(ii)

56 Discussion Paper, 46.

57 *Crimes Act* s 15GF(1)(a). Non-major controlled operations may be authorised by senior members of the Australian Federal Police, Australian Crime Commission and Australian Commission for Law Enforcement Integrity: *Crimes Act* s 15GI.

conduct by their employees. In *A v Hayden*, the High Court considered the immunity of ASIS officers from the criminal law. Justice Brennan stressed that '[t]he incapacity of the Executive to dispense its servants from obedience to laws made by Parliament is the cornerstone of a parliamentary democracy.'[58] If the authorised controlled operations scheme goes ahead, the power to issue (or at least to renew) authorisations should therefore be given to an independent body.

Fourth, the Discussion Paper states that the proposed regime would be overseen by the IGIS. Amongst other things, the IGIS must be notified when a certificate has been approved by the Director-General.[59] Under the *Crimes Act*, Chief Officers of each authorising agency must keep records on the details of their controlled operations. They must also provide six-monthly reports to the Commonwealth Ombudsman and Minister for Police.[60] The Ombudsman must then produce an Annual Report.[61] We recommend that similar record-keeping and reporting requirements should apply to the Director-General of ASIO and the IGIS under an authorised intelligence operations scheme.

The Discussion Paper states that certain specified conduct could not be authorised under intelligence operations certificates. Such conduct may include intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit, conduct that is likely to cause death or serious bodily injury and conduct that involves sexual offences against any person.[62] The concept of prohibited conduct under the *Crimes Act* is considerably broader. In addition to the above categories, the authorising officer must also be satisfied that the unlawful conduct is not likely to seriously endanger health or safety or to result in serious damage to property.[63] It would be appropriate to include these additional categories of prohibited conduct in any authorised intelligence operations scheme. There is no logical reason for prohibiting such conduct in the law enforcement context but allowing it in the intelligence gathering context. Under the *Crimes Act*, the authorising officer must also be satisfied that any unlawful conduct will be 'limited to the maximum extent consistent with the effective controlled operation'.[64] Once again, such a criterion should be incorporated into any authorised intelligence operations scheme.

Finally, the Discussion Paper states that there would be independent review of the operation, effectiveness and implications of the scheme five years after its commencement.[65] In addition

[58] (1984) 156 CLR 532, 580.
[59] Discussion Paper, 47.
[60] *Crimes Act* s 15HM-HN.
[61] *Crimes Act* s 15HO.
[62] Discussion Paper, 47.
[63] *Crimes Act* s 15GI(2)(g)(i),(iv).
[64] *Crimes Act* s 15GI(2)(c).
[65] Discussion Paper, 47.

to mandatory review, a sunset clause should be included. This means that the legislative provisions would cease to operate at a certain point in time. The Parliament would then, in light of any recommendations made by the review body, have to decide whether to allow them to lapse or to enact new legislation in the same terms. Given the unprecedented and extraordinary nature of the authorised intelligence operations scheme, we believe that the default position should be that the legislation will expire after five years unless the Australian Government presents a case for its renewal. Otherwise, any review may simply rubber stamp the legislation.

VI EXPANSION OF POWERS OF ASIS, DSD AND DIGO TO PRODUCE INTELLIGENCE ON AUSTRALIANS

Paragraphs 18(a) and (b) of the Terms of Reference ask the Committee to consider two proposals to extend the powers of ASIS, DSD and DIGO to produce intelligence on Australians. The primary function of ASIS, DSD and DIGO is to obtain intelligence about the capabilities, intentions or activities of people or organisations outside Australia.[66] There are strict limits on the ability of these agencies to undertake activities for the specific purpose (or for purposes which include the specific purpose) of producing intelligence on Australians. An agency wishing to undertake such activities must obtain ministerial authorisation under s 9 of the *IS Act*. The Minister for Foreign Affairs, in the case of ASIS, or the Minister of Defence, in the case of DSD and DIGO, must be satisfied of four matters:

- Any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned;
- There are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency;
- There are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out; and,
- The Australian is, or is likely to be, involved in one of the activities set out in s 9(1A)(a).

The first proposal in paragraph 18(a) of the Terms of Reference is to add a new category to s 9(1A)(a) where a person is, or is likely to be involved in intelligence or counter-intelligence activities.[67] The necessity for this amendment is unclear. The Discussion Paper suggests that

[66] *IS Act* s 6(1)(a).
[67] Terms of Reference, 18(a).

intelligence or counter-intelligence activities posing a risk to ASIS operations, but which do not involve a danger to personal safety, would not currently be covered.[68] However, in our opinion, such activities would fall within s 9(1A)(a)(iii), namely, the category of 'activities that are, or are likely to be, a threat to security'.[69] The issue of necessity aside, we have no objection in principle to this first proposal.

The implications of the second proposal in 18(b) of the Terms of Reference are more significant. The proposal is to enable the Minister ... to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a s 13A arrangement.

Section 13A was inserted into the *IS Act* by the *Telecommunications Interception and Intelligence Services Amendment Act 2011* (Cth). The Explanatory Memorandum stated that the purpose of the Act was to 'enable greater cooperation and assistance and information sharing among Australia's national security community'.[70] The fact that ASIS, DSD and DIGO were collection only agencies had created difficulties for multi-agency taskforces by limiting their ability to be involved in ASIO's security intelligence *assessment* functions. Section 13A remedied this problem. It allowed ASIS, DSD and DIGO, where requested by the Director-General of Security, to cooperate with and assist ASIO in the performance of its functions. This might include, for example, by making staff services and resources available to ASIO. Importantly, the Explanatory Memorandum stated:

> In carrying out the proposed new function of co-operating with and assisting other agencies, ASIS, DSD and DIGO must still adhere to the requirements of the *IS Act*. For example, ASIS, DSD and DIGO will retain their obligation to obtain a Ministerial Authorisation under section 8 of the *IS Act* when they undertake an activity for the purpose of collecting new intelligence on an Australian person even if they are solely performing the activity for the purpose of assisting another agency under proposed section 13A.[71]

The second proposal would radically alter this. It would amend 13A to allow the Minister to authorise ASIS, DSD or DIGO to produce intelligence on an Australian where the agency is

---

[68] Discussion Paper, 52.

[69] 'Security' has the same meaning as in s 4 of the *ASIO Act*. It includes the protection of the Commonwealth from espionage and sabotage.

[70] Replacement Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 (Cth) 1.

[71] Replacement Explanatory Memorandum, Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 (Cth) 33-34.

cooperating with ASIO in the performance of an ASIO function. In essence, it would create a parallel, and significantly broader, ministerial authorisation regime for ASIS, DSD and DIGO to produce intelligence on Australians.

Our primary recommendation is that the second proposal should not be adopted. The current wording of s 13A permits ASIS, DSD and DIGO to cooperate with and assist ASIO. It also allows these agencies to employ all their powers for this purpose. The only limitation is that if they wish to produce intelligence on Australians, they must comply with the criteria for a ministerial authorisation under s 9. These criteria are carefully designed to ensure that ASIS, DSD and DIGO do not unduly affect the civil liberties of Australians. For example, these agencies may only produce intelligence on an Australian where he or she is likely to engage in one of the list of (very serious) activities in s 9(1A)(a).

The single criterion for a ministerial authorisation under s 13A seems to be that the agency is cooperating with or assisting ASIO in the performance of one of ASIO's functions. The Discussion Paper states that the proposal 'is principally intended for ASIS and ASIO cooperation relating to the capabilities, intentions and activities of people or organisations outside Australia.'[72] However, ASIO's functions are to obtain, correlate and evaluate intelligence relevant to security generally. Therefore, the involvement of ASIS, DSD and DIGO could potentially extend to the production of intelligence on Australians within Australia. This is an undesirable extension of the ability of these agencies to gather intelligence on Australians.

In the event that the Committee concludes that ASIS, DSD and DIGO require an explicit power to produce intelligence on Australians for the purpose of cooperating with and assisting ASIO in the performance of its functions, our alternative recommendation is that s 9 (rather than s 13A) be amended. A new s 9(1B) could be enacted empowering ASIS, DSD and DIGO to seek ministerial authorisation for this purpose. This would operate in the alternative to the list of activities in s 9(1A) and the other substantive criteria for ministerial authorisation under s 9, for example, that the production of intelligence is necessary, would continue to apply. This approach would ensure that ASIS, DSD and DIGO are not able to circumvent these criteria by relying upon a parallel ministerial authorisation regime.

[72] Discussion Paper, 53.