Submission No 42

Inquiry into potential reforms of National Security Legislation

Name: Dr G Carne

Organisation: Faculty of Law
University of Western Australia
35 Stirling Highway
Crawley WA 6009

THE UNIVERSITY OF WESTERN AUSTRALIA
Achieve International Excellence

Faculty of Law M253
University of Western Australia
35 Stirling Highway
Crawley WA 6009
Dr Greg Carne

The Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

6 August 2012

Re: Submission to Inquiry into potential reforms of National Security Legislation (including Discussion Paper *Equipping Australia Against Emerging and Evolving Threats*)

Thank you for the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security *Inquiry into potential reforms of National Security Legislation*.

This submission focuses on selected proposals canvassed in Chapter Four 'Australian Intelligence Community Legislation Reform' of the Discussion Paper 'Equipping Australia Against Emerging And Evolving Threats".

Two important initial points can be made.

The first point is that because of the enactment in 2011 of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) and the *Intelligence Services Legislation Amendment Act 2011* (Cth), further amendments of the type proposed to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001* in Categories A, B and C of the *Terms of Reference – Inquiry Into Potential Reforms of National Security Legislation* will have larger, flow on consequences than can be immediately anticipated from the bare text of the present proposals circulated.

This is because the 2011 legislative amendments to the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) and the *Intelligence Services Legislation Amendment Act 2011* (Cth) generalize intelligence sharing and cooperative assistance across intelligence, law enforcement and government functions.

New ASIO powers and functions were conferred in 2011 to co-operate with and assist in the performance of the functions of ASIS, DSD and DIGO, Commonwealth and State authorities having a function in relation to law enforcement, as well as prescribed Commonwealth and State authorities. In addition, ASIO was granted an expanded capacity to obtain and communicate foreign intelligence on the advice of Ministers responsible for DSD, DIGO and ASIS.

A detailed analysis of the impact and consequences of the 2011 reforms (which will be built upon and expanded by any enactment of the present proposals) is contained in the article attached to this submission 'Beyond Terrorism: Enlarging the National Security Footprint Through the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth)' (2011) 13 *Flinders Law Journal* 177.

The second point is that the Discussion Paper *Equipping Australia Against Emerging and Evolving Threats* frequently couches the arguments for further expansions in intelligence agency power by repetitive phrases such as 'greater efficiency', 'administratively burdensome', 'excessive administrative resources' and 'same accountability' (as existing accountability measures) as if these

were cogent and decisive arguments in favour of expansions of power and the relaxation of safeguards.

Administrative convenience and flexibility in reducing and simplifying the work of the Attorney General, the Director General, the Attorney-General's Department and the Organisation are not suitable or credible justifications for a reduction in the existing checks and balances in the legislation.

It is important to understand that what is being articulated in the *Discussion Paper* is a further implementation of the expanded conception and enlargement of national security from the 2008 *First National Security Statement* and the integration of national security practices into mainstream governance.

The concepts mentioned above give a primacy to administrative ease and convenience, most likely because of the increased range of ASIO activities, particularly in relation to the conduct of telecommunications interception on behalf of other agencies, and in relation to co-operation and assistance to other intelligence, law enforcement and government agencies, implemented in the 2011 reforms.

What is missing, however, from the *Discussion Paper* proposals is the emphasis that the *2008 First National Security Statement* gives to safeguards and accountability, reflecting a primary obligation of national security as the protection of a democratic society:

> Our national security interests must also be pursued in an accountable way, which meets the Government's responsibility to protect Australia, its people and its interests while preserving our civil liberties and the rule of law. This balance represents a continuing challenge of all modern democracies seeking to prepare for the complex national security challenges of the future. It is a balance that must remain a conscious part of the national security policy process. We must not silently allow any incremental erosion of our fundamental freedoms.[1]

Furthermore, if the proposals were translated into legislation, such legislation would be amenable for scrutiny by the Parliamentary Joint Committee on Human Rights under the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth).. Under s.7 of that legislation, the Parliamentary Joint Committee on Human Rights has the function to examine Bills for Acts for compatibility with 'human rights', with the phrase 'human rights'[2] meaning the rights and freedoms recognised and declared by the seven listed international human rights instruments to which Australia is a party, including the *International Covenant of Civil and Political Rights* (*ICCPR*)

Central to the various civil and political rights within the *ICCPR* are the principles of prescription by law, necessity, proportionality and reasonableness in the derogation from those civil and political rights that are amenable to derogation.[3] For those articles that do permit of derogation, the typical *ICCPR* restrictions relating to national security are tempered by provision of law, as necessary in a democratic society and not in conflict with other rights recognised in the ICCPR.[4]

It is difficult to see how at least some of the proposals in the Discussion Paper and Terms of Reference, when translated to legislation, would be compatible with Australia's international human

---

[1] First National Security Statement to the Parliament 4 December 2008.
[2] See definition of 'human rights' in s.3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth).
[3] Article 4, paragraph 2 of the ICCPR states that 'No derogation from articles 6, 7, 8 (paragraphs 1 and 2), 11, 15, 16 and 18 may be made under this provision' (being the Article 4 paragraph 1 capacity to derogate from rights at time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed).
[4] See, for example, Articles 19, 20 and 21 of the *ICCPR*.

rights obligations under the *ICCPR* and for which a statement of compatibility must be prepared and presented assessing whether the Bill is compatible with human rights.[5]

On occasions the proposals present sweeping extensions of legislative reach rather than carefully calibrated and tailored legislative changes of the type demanded for compliance with Australia's international obligations under the *ICCPR* and the other listed international human rights instruments.

A. <u>Government wishes to progress the following proposals</u>

Australian Security Intelligence Organisation Act 1979

5 b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months

The warrant process is an important (albeit imperfect) attribution of executive responsibility for the application of ASIO's extraordinary and intrusive powers, (referred to as Special Powers in the *ASIO Act* – see Part III, Division 2) and an important political check involving the assessment of the reasonableness of the claim in the chain of control of the Organisation under the Director General of Intelligence and Security (s.8 of the *ASIO Act 1979* (Cth))

The three proposals – extension of the duration of a search warrant from 90 days to six months, and the removal of the requirement of a full new warrant application whenever a variation on an existing warrant is required, or a renewal of a warrant is required – if legislated, will weaken periodic Ministerial review and the opportunity for fresh assessment by the Minister of the reasonableness of the claim for the warrant, to the Minister's satisfaction, that the warrant will assist the collection of intelligence in accordance with the Act in respect of a matter that is important in relation to security as expressed, through the application of the relevant ministerial test:

. Search warrants – s.25 (2) *ASIO Act 1979* (Cth)

. Computer access warrant – s.25A (2) *ASIO Act 1979* (Cth)

. Listening devices – s.26 (3) and s.26 (4) *ASIO Act 1979* (Cth)

. Tracking devices – s.26B (2) and s.26C (2) *ASIO Act 1979* (Cth)

. Inspection of postal articles – s.27 (2) *ASIO Act 1979* (Cth)

. Inspection of delivery service articles – s.27AA (3) and (6) *ASIO Act 1979* (Cth)

Furthermore, the proposed extension of the duration of search warrants from 90 days to 6 months fails to differentiate the peculiar characteristic of a search warrant of premises – as the most overt and intrusive example of the application of warrant powers, from the less intrusive characteristics of the other special powers.

It is precisely because the various warrant powers are considered both special and intrusive that there is an existing periodic requirement to re-state the intelligence case, and ministerially re-assess that intelligence case on a periodical basis against the legislative thresholds and criteria.

In addition, the existing legislation already permits a warrant to come into force at a time other than the issuing of a warrant – see s.25AA (8) and (9) of the *ASIO Act 1979* (Cth).[6] This already provides for an extended scope in timing of the execution of the warrant.

---

[5] *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) s.8.

6 e Provide additional scope for further secondment arrangements

This proposal provides for an extension and variation (in different form) of the extensive co-operation and assistance arrangements with and by ASIO implemented by the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) – which provides for the availability of full ASIO technical and personnel capabilities for non-security intelligence purposes, on a discretionary basis, divorced from ASIO's hitherto primary security role – to ASIS, DSD and DIGO, law enforcement agencies and prescribed Commonwealth and State authorities.

The *Discussion Paper* makes clear 'Such a secondment regime would operate independently from section 19A of the ASIO Act and section 13A of the IS Act...It is suggested that unlike section 19A arrangements, these secondment arrangements would not be limited to intelligence, law enforcement and prescribed agencies'.

By disconnecting supervisory responsibility and accountability of the ASIO secondment from the *ASIO Act 1979* (Cth) – (the Discussion Paper notes 'If the ASIO Act were amended to expressly enable staff to be 'seconded' to and from ASIO and to clarify that during the secondment, a seconded staff member carries out only the functions of the host organisation in accordance with any procedures or restrictions that apply under legislation to the host organisation) – a range of unexplored consequences may follow.

A secondment (in the manner the reform seeks) of ASIO personnel to a law enforcement agency or a prescribed Commonwealth or State authority *that is simultaneously the recipient of s.19A cooperation and assistance from ASIO* is *in practical terms*, unlikely to maintain such a strict separation between functions and accountabilities. The consequences of this *simultaneous application* of secondment and s.19 A co-operation and assistance with a mixture of personnel – those seconded and those providing s.19 A co-operation and assistance - have not been thought through.

In addition, the secondment so described to law enforcement agencies carrying out the functions of the host organisation again contributes to a dismantling of the separation between policing and law enforcement functions, and intelligence gathering and analysis, and the potential to introduce a policing and law enforcement culture into the Organisation.

7 Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies

This proposal effectively enlarges the scope of DIGO's cooperation and assistance capacity in the exercise of its functions (by clarifying its functions as also including material obtained during both intelligence and non-intelligence functions) to the equivalent scope of co-operation and assistance capability conferred on ASIS and DSD by the s.13 A of the *Intelligence Services Act 2001* (Cth).

Issues surrounding this application of s.13 A are canvassed in (2011) 13 *Flinders Law Journal* 177, 188-189 (copy attached to this submission).

---

[6] S.25AA of the *ASIO Act 1979* (Cth) (8) states that 'The warrant may state that it comes into force on a specified day (after the day of issue) or when a specified event happens. The day must not begin nor the event happen more than 28 days after the end of the day on which the warrant is issued'.

B. Government is considering the following proposals

Australian Security Intelligence Organisation Act 1979

10. Amending the ASIO Act to create an authorized intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorized intelligence operations

The principle of ASIO being subject to accountability in the courts and to the rule of law is long established in Australian law – see *A v Hayden* (1984) 156 CLR 532; *Alister v R* (1984) 154 CLR 404 and *Church of Scientology v Woodward* (1983) 154 CLR 42. It is a cardinal principle essential to the maintenance of democratic norms that government organisations (including the intelligence community) be answerable to an independent judicial system and judicial process for alleged breaches of the law.

The inherent danger in the proposal is that in contrast to the bodies authorized for the controlled operations scheme under the *Crimes Act* (Cth), ASIO is by definition a secret organisation reliant for its supervision upon bodies more circumscribed as to their capacity and methods (given the subject matter of national security) to publicly examine and publicise improprieties and improper conduct – the Inspector General of Intelligence and Security, the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor. With the application of prosecutorial discretion, the subjection of ASIO to the ordinary application of the criminal law should continue.

The risks of abuse of power associated with such a proposal are perhaps best illustrated in the case of *R v Ul-Haque* [2007} NSWSC 1251, (2007) 177 A Crim R 348, at 369 where Adams J Of the New South wales Supreme Court, for the purposes of assessing the admissibility of interviews as evidence at trial, found that ASIO officers had committed improper acts amounting to criminal offences of false imprisonment and kidnapping and the tort of false imprisonment:

> I am satisfied that B15 and B16 committed the criminal offence of false imprisonment and kidnapping at common law and also an offence under s.86 of the *Crimes Act*. It follows, a fortiori, that they committed the tort of false imprisonment. Their conduct was grossly improper and constituted an unjustified and unlawful interference with the personal liberty of the accused. So far as their conduct in his parents' home is concerned, it also constituted an unlawful trespass against the occupants, since they gained admittance under colour of the warrant which did not authorise what they did.

A preferable course of action might be to amend Part 5.3 of the *Criminal Code* to provide an available defence to a criminal charge under that Part for a limited range of activities (specifying conduct which cannot amount to a defence) so described were done solely for the purpose of engaging in lawful intelligence collection purposes.

It is similarly inappropriate in any event that given that the various intrusive special warrant powers in the *ASIO Act 1979* (Cth) require authorisation by the *Attorney-General's warrant* upon application by the Director General of Security, that 'the *Director-General of Security* issue authorized intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months)

11. Amending the ASIO Act to modernize and streamline ASIO's warrant provisions to:

a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target

This proposal seeks to apply the concept of a named person warrant from the *Telecommunications (Interception and Access) Act 1979* (potentially applying to multiple telecommunications services) and intended to be of utility where the named person is using or likely to use more than one telecommunications service) to the *completely different situation* of consolidating warrant authority in a single warrant to authorise the full panoply of special powers under Part III Division 2 of the *ASIO Act 1979* (Cth) – search warrants, computer access warrants, listening devices, tracking devices, inspection of postal articles and inspection of delivery service articles.

It is difficult to see how in each and every application the blanket application of all of the above means of surveillance could satisfy the existing threshold test that the Minister must apply in relation to search warrants and computer access warrants[7] or in relation to other forms of warrant, such as computer access warrants, tracking device warrants, postal articles warrants and delivery service articles warrants.[8]

The likelihood is that for such an all encompassing warrant, the level of the threshold test would have to be reduced, and with it the level of the political check applied to the application of the Director-General., and indeed, to resource allocation and prioritization within the Organisation.

It is also difficult to consider how the removal of individual warrant applications for particular special powers squares with the requirements of necessity and proportionality for the legislation to conform with the ICCPR human rights compatibility obligations mandated by the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Instead of tailoring the individual surveillance requirements and application of techniques to a particular case, the proposed legislative amendments will create applications for warrant authority which fail to differentiate between the suitability and effectiveness of available measures in different cases and the level of surveillance truly required for purposes relating to security.

This is even more extraordinary when the *Discussion Paper* openly admits that it is in only 'approximately one third of cases [that] more than one ASIO Act warrant type is sought against a particular target'[9] and again gives primacy the 'administratively burdensome' argument as the driver of reform.[10]

In addition, the checks and balances for such an extensive and comprehensively authorized system of surveillance are proposed to be weakened by the removal of a fresh warrant application process where renewal of the warrant, or variation of the warrant, based on the re-presentation of the intelligence case - becomes necessary – please refer to the discussion above under the heading '5 b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.'

It is also unclear from the proposals whether the named person warrant would also be used to supplant the existing warrant procedures for ASIO questioning powers and ASIO detention and

---

[7] 'The Minister is only to issue the warrant if he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to records or other things on particular premises will substantially assist the collection of intelligence that is important in relation to security

[8] "will or is likely to assist the Organisation in carrying out its function of obtaining intelligence relevant to security'

[9] Discussion Paper, 47.

[10] Discussion Paper, 47.

questioning powers, under Part III, Division 3 of the *ASIO Act 1979* (Cth). There is nothing in the *Discussion Paper* which rules out such a measure, an extraordinary situation given the protracted debate, amendments, reviews and controversies surrounding these powers enabling up to 168 hours of detention of non suspects and the detention of innocent persons affected at the scene of a terrorist incident.

c. Enable the disruption of a target computer for the purposes of a computer access warrant

The proposal is exceptional in that it seeks to authorise interference with and damage to the data and operating systems of a target computer in accessing, under warrant, data held in the target computer.

There is inherent difficulty in legally defining disruptive activity to the target computer in a manner that is "activity proportionate to what is necessary to execute the warrant". More properly, the proportionality aspect would be better directed, in legislation, to the end or consequence relating to security sought to be prevented by the execution of the computer access warrant.

The collection of intelligence via a computer access warrant should be done in a manner which is consistent with the continuing proper functioning of the target computer and its data for those who (though presumably shared access) lawfully use the target computer for a lawful purpose.

d. Enable person searches to be undertaken independently of a premises search

Insufficient information has been provided in the *Discussion Paper* as to why it is necessary for ASIO to acquire a freestanding personal search power, directed against named individuals, under a warrant which would be of six months duration.

Again, such a personal search warrant power would then be incorporated under the claim for a single warrant authority for all special powers, as discussed under the above heading 'a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.'

The conferral of such a power raises again the transformational questions for the Organisation from being an intelligence gathering and analysis agency to quasi-policing powers and functions conducted under proposed general warrant powers.

Separate personal search powers are already available for policing matters by policing authorities. The conferral of such personal search powers on the Organisation would greatly expand the potential for day to day interventions in the lives of named warrant targets and potentially raise the sort of improper transactional issues reflected upon by Adams J in *R v Ul-Haque* [2007} NSWSC 1251, (2007) 177 A Crim R 348, as raised above.

There is no suggestion in the Discussion Paper of any limit to the number of personal searches that could be conducted within the limits of a six month warrant, which, following the discussion under the heading '5 b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months' above, the supporting intelligence case underpinning the warrant would not be reassessed at the time of renewal or variation of the warrant in the manner currently required.

C. Government is expressly seeking the views of the Committee on the following matters

Australian Security Intelligence Organisation Act 1979

17 c. Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry

The subsections mentioned may require clarification if it was the intention to authorise the use of force under a warrant subsequent to entry to the premises – but it is necessary in any such amendment that it be made clear that the use of force be reasonable in all the circumstances and to only effectuate in a reasonable and necessary manner the purpose of the warrant.

Intelligence Services Act 2001

18 b. Enable the Minister of an Agency under the IS Act 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 section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required.

The intention here appears to be to add to the categories of Ministerial authorisation available under Section 9 of the *Intelligence Services Act 2001*(Cth) for those Ministers responsible for ASIS, DIGO and DSD when co-operative and assistance arrangements are entered into with ASIO under s.13A of the *Intelligence Services Act*, to the extent to allow such co-operation and assistance to include the production of an intelligence on an Australian person under ASIO powers.

It is important to understand that this Ministerial authorisation for ASIS, DIGO and DSD technical and personnel co-operation and assistance contributions under s 9 of the *Intelligence Services Act 2001* stands conjunctively and exponentially with the proposals for increased ASIO warrant powers discussed above under the headings:

> . 5 b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months
>
> . 10. Amending the ASIO Act to create an authorized intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorized intelligence operations
>
> . 11. Amending the ASIO Act to modernize and streamline ASIO's warrant provisions to:
> a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target

Whilst the *Discussion Paper* states

> The proposal is principally intended for ASIS and ASIO cooperation relating to the capabilities, intentions and activities of people or organisations outside Australia. Given existing Defence agencies' functions and capabilities, and the nature of the activities to which the proposal is sought to address, it is unlikely that Defence would utilize the proposed change,[11]

[11] Discussion Paper, 53

it is nowhere evident that the proposed legislative drafting would so tightly confine that extended authorisation of co-operation and assistance to the discrete situation of the principal intention of ASIS and ASIO co-operation so described in the above example.

Indeed the other descriptive language leaves open the full deployment, under Ministerial authorisation, of the technological resources of DSD and DIGO to fulfill co-operation and assistance arrangements with ASIO, with ASIO acting under ASIO powers.

The statement that 'it is unlikely that Defence would utilise the proposed change' expresses a prediction of administrative conduct or prioritization of activity, rather than a legislative prohibition or restriction on such conduct.

There are further problems with the statement made in the *Discussion Paper*:

> The existing safeguards in the IS Act could apply to the proposed section 13A authorisation. These include the requirement for all ministerial authorizations to be provided to the IGIS who overseas the legality and propriety of the operations of the intelligence agencies

In fact, all that the *Intelligence Services Act 2001* (Cth) does is to oblige the Minister to:

(1) in the case of Ministerial authorizations under s.9 of the *Intelligence Services Act 2001*, make such authorisation 'available *for inspection* <u>*on request*</u> by the Inspector General of Intelligence and Security': see s.9(5) of the *Intelligence Services Act 2001*

(2) in the case of co-operative and assistance arrangements under s.13 of *Intelligence Services Act 2001* , make such approval "available <u>*on request*</u> by the Inspector-General of Intelligence and Security' (emphases added)

These provisions *should be amended* to create an obligation on the relevant Minister and Agency *to automatically provide* a copy of s.9 authorisations and s.13 co-operative and assistance arrangements to *both* the Inspector General of Intelligence and Security and to the parliamentary Joint Committee on Intelligence and Security.

There are further problems with the further statement made in the Discussion Paper:

> Additionally, the communication and retention of intelligence collected under the ministerial authorisation would be subject to the Privacy Rules

These difficulties with the Privacy Rules are identified in (2011) 13 *Flinders Law Journal* 177, 191 (footnotes omitted below) ,(copy attached to this submission):

> In addition, under section 15 of the *Intelligence Services Act 2001* (Cth),
>
> (1) The responsible Minister in relation to ASIS, the responsible Minister in relation to DIGO and the responsible Minister in relation to DSD, must make written rules regulating the communication and retention by the relevant agency of intelligence information concerning Australian persons.
>
> (2) In making the rules, the Minister must have regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agencies of their functions.

In relation to ASIS, the Minister issued new *Rules To Protect The Privacy of Australians* on 17 September 2008. The difficulty in obtaining any protective impact from these Privacy Rules under section 13A(2)(a) of the *Intelligence Services Act 2001* (Cth) ministerial directions, arises in that 'intelligence information' in section 15 of the *Intelligence Services Act 2001* (Cth) does *not* include information obtained solely under paragraph 6(1)(da) of the Act, namely, the ASIS function 'to co-operate with and assist bodies referred to in section 13A in accordance with that section'.

I would be pleased to provide the Parliamentary Joint Committee with further information in relation to this submission.

Yours faithfully,

Dr Greg Carne

Faculty of Law
University of Western Australia M253
35 Stirling Highway
Crawley WA 6009

Attachment: "Beyond Terrorism: Enlarging The National Security Footprint Through The *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth)' (2011) 13 *Flinders Law Journal* 177.

BEYOND TERRORISM: ENLARGING THE NATIONAL SECURITY FOOTPRINT THROUGH THE *TELECOMMUNICATIONS INTERCEPTION AND INTELLIGENCE SERVICES LEGISLATION AMENDMENT ACT 2011* (CTH)

GREG CARNE[†]

I INTRODUCTION

The *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) affects significant changes in intelligence functions, information sharing and co-operation amongst intelligence, law enforcement and other government agencies. The far reaching enabling nature of the legislation's changes in these areas, particularly in building upon, generalising and extrapolating from the model and experience of Commonwealth terrorism law reform from 2001 to other areas, is likely to accentuate and accelerate concentrations of Commonwealth executive authority and discretion with significant consequences for democratic governance. The circumstances regarding passage of the legislation failed to provide adequate scrutiny or modification of its far reaching provisions, but also signaled a renewal of expansionary national security legislative activity, following a hiatus with the defeat of the Howard government in 2007 with its recurrent terrorism legislation agenda. The legislation also indicates an expanded leadership role and functions for ASIO in performing activities on behalf of other intelligence, law enforcement and government agencies, confirming

that premier and pivotal role[1] in a broad array of national security functions.

The three major activities facilitated by the legislation are identified in the Attorney-General's Department submission to the Senate Legal and Constitutional Affairs Legislation Committee inquiry into the bill:[2] (i) Assistance to law enforcement with telecommunications interception, (ii) Improving cooperation and assistance between intelligence agencies and (iii) Enhancing the communication and sharing of intelligence between agencies. These three activities provide a logical structure to examine the substantive content of major legislative changes and to briefly expound the rationales advanced by the government in support of these far reaching legislative reforms. These matters form important preliminary information to a critical analysis of ASIO's, and other intelligence agencies' expanded and co-operative functions, and identification of various problems that arise from these reforms.

Collectively, the changes signal a renewed and broadened national security agenda, extending beyond, but informed and inspired by, earlier counter-terrorism legislative reforms. The present reforms generalise intelligence sharing and co-operative assistance across intelligence, law enforcement and government functions. They represent a new phase in the accretion of executive power, involving the migration or colonisation of state security values and practices to areas of Commonwealth and State public administration,

---

1 A point underpinned by several ASIO resource factors: the trebling of ASIO staff from 2001 to 2011, a six-fold increase in the ASIO budget over a decade and the construction, symbolically within the Parliamentary Triangle, of a large new ASIO building costing $585 million: see Sally Neighbour 'Hidden Agendas' (2010) *The Monthly* (November), 28 and 32; See also, Australian Security Intelligence Organisation, *Report to Parliament 2009-2010*, 63, 80, 137 (Appendix E) (*ASIO Report*).

2 Attorney-General's Department, Submission No 3 to Senate Legal and Constitutional Affairs Committee, Parliament of Australia, *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010*, 26 November 2010, 1-3 (*Attorney-General's Department submission*). See also Commonwealth, *Parliamentary Debates*, House of Representatives, 24 June 2010, 6527-6529 (Robert McClelland).

not ordinarily or traditionally associated with national security issues.[3] The changes potentially create reciprocal interests and mutual dependency between ASIO and ordinary State and Commonwealth authorities. This is through the subsidiary use of security obtained information communicated to those other State and Commonwealth agencies for use for their own routine purposes, as well as the legislation's provision for the Commonwealth to prescribe additional Commonwealth and State authorities for co-operative and assistance based purposes.

II ASSISTANCE TO LAW ENFORCEMENT AND INTERCEPTION AGENCIES WITH TELECOMMUNICATIONS INTERCEPTION

The legislation noticeably provides a significant enhancement of the functions of ASIO[4] and a pivotal leadership role for the Organisation amongst Australia's several intelligence agencies. The first example arises in relation to ASIO's expanded telecommunications interception function, through amendments to the

---

3 This process, facilitated under these legal reforms, can be described as the securitisation of Commonwealth and State agency administration and policy implementation.

4 For discussion of earlier increased functions for ASIO in response to terrorism, see Jude McCulloch and Joo-Cheong Tham 'Secret state, transparent subject: the Australian Security Intelligence Organisation in the age of terror' (2005) 38 *Australian and New Zealand Journal of Criminology* 400; Patrick Emerton 'Australia's anti-terrorism legislation: a threat to democracy and the rule of law' (2005) 19 *Dissent* 19; Greg Carne 'Gathered intelligence or Antipodean exceptionalism? Securing the development of ASIO's detention and questioning regime' (2006) 27 *Adelaide Law Review* 1; Greg Carne 'Detaining questions or compromising constitutionality?: The ASIO Legislation Amendment (Terrorism) Act 2003' (Cth) (2004) 27 *University of New South Wales Law Journal* 524; Michael Head 'Another threat to democratic rights ASIO detentions cloaked in secrecy' (2004) 29 *Alternative Law Journal* 127; Michael Head 'ASIO, secrecy and accountability' (2004) 11 *E Law* 1; Jenny Hocking 'National Security and Democratic Rights: Australian Terror Laws' (2004) *Sydney Papers* 89.

Telecommunications (Interception and Access) Act 1979 (Cth).[5] Under that amended legislation, ASIO is now empowered to exercise authority under a telecommunications interception warrant, on behalf of other agencies[6] issued with the warrant,[7] and as such, is added to other existing agencies that may provide telecommunications interception assistance. For the first time, ASIO is authorised as a direct participant in telecommunications interception activity on behalf of another agency. Various reasons, focusing upon claims of efficiency and effectiveness, are advanced

---

5 For earlier amendments about telecommunications interception counter-terrorism measures, see Niloufer Selvadurai and Rizwanul Islam 'The expanding ambit of telecommunications interception and access laws: The need to safeguard privacy interests' (2010) 15 *Media and Arts Law Review* 378, 383-385; Niloufer Selvadurai, Peter Gillies and Rizwanul Islam 'Maintaining an effective legislative framework for telecommunication interception in Australia' (2009) 33 *Criminal Law Journal* 34, 40-42; Greg Carne 'Hasten Slowly: Urgency, Discretion and Review – A Counter-Terrorism Legislative Agenda and Legacy' (2008) 13 *Deakin Law Review* 49, 77-82; David Hume and George Williams 'Who's Listening? Intercepting the telephone calls, emails and SMS's of innocent people' (2006) 31 *Alternative Law Journal* 211.

6 'Agency' in Chapter 2 of the *Telecommunications (Interception and Access) Act 1979* (Cth) is defined as an 'interception agency': *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

7 The chief officer of an agency or an officer of an agency appointed to be an approving officer may approve a range of persons to exercise authority conferred by Part 2-5 warrants issued to the agency, including members of ASIO and persons assisting ASIO in the performance of its functions: *Telecommunications (Interception and Access) Act 1979* (Cth) s 55(3)(a)-(d). Similarly, a chief officer of an agency may revoke a warrant issued to the agency, and if another agency or ASIO is exercising authority under the warrant, then before invoking the warrant, then before revoking the warrant, the chief officer must inform the chief officer of the other agency or the Director General of Security (as the case requires) of the proposed revocation: *Telecommunications (Interception and Access) Act 1979* (Cth) s 57(2). Being informed of the revocation or proposed revocation of the warrant, the chief officer of an agency or the Director General of Security (ASIO) must immediately take such steps as are necessary to ensure that interceptions of communications under warrant by the agency or the Organisation (as the case requires) are discontinued: *Telecommunications (Interception and Access) Act 1979* (Cth) s 58(2).

to support the introduction of these changes.[8] These include the fact that ASIO has technical expertise in a number of areas that would assist law enforcement agencies,[9] the need to use technological resources on a whole of government basis,[10] the opportunity to provide ASIO with flexibility to support such whole of government efforts,[11] to allow smaller agencies to keep pace with rapid technological developments,[12] an implied illogicality in the then existing arrangements excluding ASIO from the group of agencies from which technical assistance could be sought,[13] and that changed arrangements would more readily reflect a modern, co-operative security environment.[14]

A consequence of this telecommunications interception assistance now able to be provided by ASIO to other agencies is that a rather convoluted further amendment was included in the legislation.[15] This particular amendment was an attempt to reconcile the competing aspects of communication and treatment of information intercepted by ASIO on behalf of another agency, with dealings of information that are of interest to security within that meaning in the *ASIO Act 1979* (Cth). The statutory framework settled upon by the Parliament in effect provides for a temporary range of restrictions on the use, application and communication of information *incidentally obtained* by ASIO when exercising interceptions warrant authority on behalf of another agency. It subsequently provides a mechanism for the originating agency with the warrant authority (for whom ASIO has acted and for the

---

8 *Attorney-General's Department submission*, above n 2, 1-2; See also, Commonwealth, *Parliamentary Debates*, House of Representatives 24 June 2010, 6527 (Robert McClelland).

9 *Attorney-General's Department submission*, above n 2, 1.

10 Ibid.

11 Commonwealth, *Parliamentary Debates* House of Representatives 24 June 2010, 6527 (Robert McClelland).

12 *Attorney-General's Department submission*, above n 2, 1.

13 Commonwealth, *Parliamentary Debates* House of Representatives 24 June 2010, 6527 (Robert McClelland).

14 Ibid.

15 See the discussion below of the amended *Telecommunications (Interception and Access) Act 1979* (Cth) ss 64(3), 65(3), 67(1A), 68.

originating agency's purposes) to communicate the information to ASIO for ASIO's own security purposes.

The net effect of the legislation is likely to significantly enlarge the pool of available information considered as security related and therefore transmissible,[16] as a consequence of the warrant process, to ASIO for its use. The legislation therefore provides an incentive for ASIO to exercise interception warrant authority on behalf of other agencies, and an impetus for the dispersal and mainstreaming of security orientated practices and values over the activities of many government agencies.

III THE AMENDED TELECOMMUNICATIONS INTERCEPTION SCHEME

Section 64 of the *Telecommunications (Interception and Access) Act 1979* (Cth) now commences with a permissive authority to communicate information relating to the purposes and functions of ASIO.[17] The amendment[18] subsequently insulates classes of information obtained under section 55 of the *Telecommunications (Interception and Access) Act 1979* (Cth) through ASIO exercising warrant authority on behalf of another agency, from communication

---

16 The information need only relate, or appear to relate, to activities prejudicial to security: *Telecommunications (Interception and Access) Act 1979* (Cth) s 68(a).

17 Section 64 of the *Telecommunications (Interception and Access) Act 1979* (Cth) states '(1) A person may, in connection with the performance by the Organisation of its functions, or otherwise for purposes of security, communicate to another person, make use of, or make a record of the following (a) lawfully intercepted information other than foreign intelligence information; (b) interception warrant information (2) A person, being the Director-General of Security or an officer or employee of the Organisation, may, in connection with the performance by the Organisation of its functions, communicate to another such person, make use of, or make a record of, foreign intelligence information'.

18 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 64(3)-(4).

and dealing by ASIO for its own purposes.[19] The communication of and dealing with such information by ASIO, having been excised from the categories of information connected with ASIO's functions and the purposes of security, is then treated in several different ways.

First, ASIO may communicate the information obtained for purposes consistent with the original issue of the warrant[20] under which it was exercising authority on behalf of another agency. Second, section 66 of the *Telecommunications (Interception and Access) Act 1979* (Cth) provides for the interceptor to *communicate* intercepted information obtained under the warrant to the officer who applied for the warrant or other authorised person,[21] but again seeks to restrict such communication for warrant purposes.[22] Third,

---

19 'Subsections (1) and (2) do not apply to information: (a) obtained by a person referred to in paragraph 55(3)(c) or (d) by intercepting a communication when exercising authority under a warrant issue to an agency; or (b) communicated, in accordance with section 66, to a person referred to in paragraph 55(3)(c); or (c) that is interception warrant information in relation to a warrant issued to an agency; unless the information has been communicated to the Director General of Security under section 68': *Telecommunications (Interception and Access) Act 1979* (Cth) s 64(3).

20 '...a person referred to in paragraph 55(3)(c) or (d) may communicate to another person, make use of, or make a record of information referred to in paragraph (3)(a), (b) or (c) of this section, that has not been communicated to the Director General of Security under section 68, for a purpose or purposes connected with the investigation to which the warrant, under which the information was obtained relates, and for no other purpose': *Telecommunications (Interception and Access) Act 1979* (Cth) s 64(4).

21 'A person who has intercepted a communication under a warrant issued to an agency may communicate information obtained by the interception to (a) the officer of the agency who applied for the warrant on the agency's behalf; or (b) a person in relation to whom an authorisation under subsection (2) is in force in relation to the warrant, (2) The chief officer of an agency, or an authorising officer of an agency for whom an appointment under subsection (4) is in force, may authorise in writing a person (or class of person) referred to in any of paragraphs 55(3)(a) to (c) to receive information obtained by interceptions under warrants (or classes of warrants) issued to the agency' (s 55(3)(c) includes officers or employees of ASIO): *Telecommunications (Interception and Access) Act 1979* (Cth) s 66(1).

22 'The chief officer, or an authorising officer, of an agency may make an authorisation under subsection (2) in relation to a person (or class of person) who is not an officer or staff member of that agency only for a purpose or purposes connected with an investigation to which a warrant issued to that

similar restrictions apply under section 67 of the *Telecommunications (Interception and Access) Act 1979* in relation to the dealing for permitted purposes[23] of intercepted information obtained when ASIO exercises warrant authority on behalf of another agency, seeking to restrict such dealing for warrant purposes.

Fourth, sections 64(3), 65(3) and 67(1A) of the *Telecommunications (Interception and Access) Act 1979* (Cth) treat communications under section 68 of the Act as not attracting the prohibitions relating to ASIO in dealing with communication and treatment of information[24] obtained when ASIO exercises interception warrant authority in behalf of another agency. Section 68 accordingly permits an originating agency to communicate interception obtained security related information to ASIO.[25] It is through this formal legal mechanism that information incidentally accessed by the authorised process of ASIO exercising warrant authority on behalf of another agency can ultimately be accessed and used by ASIO for its own extremely broad purposes relevant to *security*, as defined in the *ASIO Act 1979* (Cth).[26] Therefore, the co-

---

agency relates': *Telecommunications (Interception and Access) Act 1979* (Cth) s 66(3).

23 Such dealing relates to communication, making use of, or making a record of the intercepted information: *Telecommunications (Interception and Access) Act 1979* (Cth) s 67(1).

24 Sections 64(3) and 65(3) of the *Telecommunications (Interception and Access) Act 1979* (Cth) prohibitions conclude with the statement 'unless the information has been communicated to the Director-General of Security under section 68'.

25 'The chief officer of an agency...may personally, or by an officer of the originating agency authorised by the chief officer, communicate lawfully intercepted information that was originally obtained by the originating agency or interception warrant information (a) if the information relates, or appears to relate, to activities prejudicial to security – to the Director-General of Security': *Telecommunications (Interception and Access) Act 1979* (Cth) s 68.

26 Section 5 of the *Telecommunications (Interception and Access) Act 1979* (Cth) states that security 'has the same meaning as it has in the *Australian Security Intelligence Organisation Act 1979*'. Section 4 of the *ASIO Act 1979* (Cth) defines security as '(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from: (i) espionage (ii) sabotage (iii) politically motivated violence (iv) promotion of communal

operative and collaborative nature of the arrangements for telecommunications interception facilitated by the amendments are likely to encourage anticipatory arrangements for the communication to ASIO of such information under Section 68, when ASIO agrees or is approached to exercise warrant authority on behalf of another agency. This would be as a *quid pro quo* for undertaking that interception task and indeed because of the technical and human resources ASIO would need to dedicate to that task.

The critical point that can be made is that the legislation provides merely a formal legal scheme of separating performance of the interception function from access to, communication of, and use of intercepted information. In other words, it maintains in the interception process outsourced to ASIO a technical legal distinction between security sought information and law enforcement sought information. However, the legislation's informal effects will be to break down a previous deliberate, policy distinction and the physical separation between the deployment of exceptional powers and resources for telecommunications interception involving more narrowly defined *security* purposes under the *ASIO Act 1979* (Cth), from situations involving law enforcement functions involving a Commonwealth agency or an eligible authority of a State.[27] As was noted in one submission to the Senate Legal and Constitutional Affairs Legislation Committee, 'the Bill comes close to giving a very wide range of enforcement agencies...access to the same extraordinary powers that have been limited to date to a few specialised agencies with narrow and targeted functions'.[28] The

violence (v) attacks on Australia's defence system or (vi) acts of foreign interference whether directed from, or committed within, Australia or not and (aa) the protection of Australia's territorial and border integrity from serious threats; and (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).'

27 See the definition of 'interception agency' in section 5 of the *Telecommunications (Interception and Access) Act 1979* (Cth), picking up the meaning of 'agency' in section 5 as being 'in Chapter 2 – an interception agency'.

28 Australian Privacy Foundation, Submission No 9 to Senate Legal and Constitutional Affairs Legislation Committee Inquiry into *Telecommunications Interception and Intelligence Services Legislation*

potential inefficacy of the legislation's separations was underlined by the fact that the Ombudsman has no authority to inspect ASIO records regarding telecommunications interception undertaken on behalf of other agencies.[29] The legislation requires ASIO to provide particulars of interception to the agency that sought the warrant,[30] and it is only those records, once removed, that would be available for Ombudsman inspection,[31] such records being of a qualitatively different nature.[32]

IV IMPROVING CO-OPERATION AND ASSISTANCE BETWEEN INTELLIGENCE AGENCIES, LAW ENFORCEMENT AND PRESCRIBED STATE AND COMMONWEALTH AUTHORITIES

ASIO's expansionary focus and leadership role in relation to conducting telecommunications interception on behalf of a variety of agencies, and in obtaining intercept information relating or

---

Amendment Bill 2010 (Cth), Parliament of Australia, 26 November 2010, 1 (*Australian Privacy Foundation submission*).

29 Commonwealth Ombudsman, Submission No 8 to Senate Legal and Constitutional Affairs Legislation Committee Inquiry into *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010* (Cth), Parliament of Australia, 26 November 2010, 3 (*Commonwealth Ombudsman Submission*). 'Under Chapter 2 of the TIA Act, the Ombudsman is required to inspect the records of the AFP, the ACC and the Australian Commission for Law Enforcement Integrity...as my office has no authority in respect of ASIO, interceptions undertaken by ASIO on behalf of other agencies may not be subject to the same level of scrutiny' at 3.

30 *Commonwealth Ombudsman submission*, above n 29, 3.

31 Ibid.

32 '...interceptions undertaken by ASIO on behalf of other agencies may not be subject to the same level of scrutiny...The logistics and record keeping proposed should assist in retaining an adequate, albeit different, oversight arrangement': Ibid. See also, Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 [Provisions]* (2010), 18-19 (*Senate 2010 Report*).

appearing to relate to activities prejudicial to security from the originating agency, is further consolidated by a second tier of amendments. These amendments are intended to broaden and facilitate greater co-operation and assistance between ASIO and other prescribed Australian intelligence agencies[33] and amongst those other prescribed intelligence agencies themselves, in the performance of their respective functions. These amendments are founded upon common and interchangeable intelligence interests, expertise and resources, as well as a potential to extend such intelligence matters to both intelligence and non intelligence agencies alike.

The *ASIO Act 1979* (Cth) is amended[34] by the legislation to include new ASIO powers and functions to co-operate with and assist in the performance of their functions, three other Australian intelligence agencies,[35] a law enforcement agency[36] and prescribed Commonwealth and State authorities.[37] The new capacity of ASIO to co-operate with and assist these bodies is particularly broad, given the exceptionally wide definition of law enforcement agency,[38] effectively encompassing Commonwealth and State authorities with *any* law enforcement aspect, which most agencies will have in some form. The breadth is further underlined by the discretionary capacity to prescribe by regulation,[39] (rather than a requirement of parliamentary amendment) on a case by case basis, other

---

33 Namely ASIS (Australian Secret Intelligence Service), DSD (Defence Signals Directorate) and DIGO (Defence Imagery and Geospatial Organisation)

34 Through the inclusion of a new section 19A.

35 ASIS, DSD and DIGO.

36 Defined in section 4 of the *ASIO Act 1979* (Cth) as 'an authority of the Commonwealth, or an authority of a State, that has functions relating to law enforcement'.

37 Defined as 'an authority of the Commonwealth, or an authority of a State, that is prescribed by the regulations for the purposes of this paragraph': *ASIO Act 1979* (Cth) s 19A(1)(e).

38 Section 4 of the *ASIO Act 1979* (Cth) states that 'law enforcement agency means an authority of the Commonwealth, or an authority of a State, that has functions relating to law enforcement'. An alternative was to nominate 'a finite list of specified agencies set out in the Act': *Australian Privacy Foundation submission,* above n 28, 3.

39 *ASIO Act 1979* (Cth) s 19A(1)(e).

Commonwealth and State authorities[40] to whom ASIO co-operation and assistance can be made available.

The type of co-operation and assistance that ASIO is able to provide the nominated bodies is left open, with the inclusion of an indicative only legislative provision.[41] The critical point is that full ASIO technical and personnel capabilities are available under this provision for non security-intelligence purposes, on a discretionary basis, and divorced from ASIO's hitherto primary security role.[42] Because the limits of such *assistance* are not legislatively confined, it has been argued that the new provision might even include the collection of information by ASIO (using its far reaching technical and human intelligence capacities) to serve the functions of the other agency or authority.[43]

The intelligence co-operation and assistance provisions also apply to intelligence agencies other than ASIO.[44] The *Intelligence Services Act 2001* (Cth) is amended to enable 'an agency'[45] to co-operate with and assist nominated bodies in the performance of their

---

40 Flexibility and responding to emerging situations appeared to inform the Attorney-General's Department response in this aspect of the legislation: Evidence to Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, Canberra, *Committee Hansard*, 11 November 2010, 21 (Mr McDonald).

41 'Without limiting subsection (1), in co-operating with and assisting a body in accordance with this section, the Organisation may make the services of officers and employees, and other resources of the Organisation available to the body': *ASIO Act 1979* (Cth) s 19A(3).

42 See Castan Centre for Human Rights Law, Submission No 14 to Senate Legal and Constitutional Affairs Legislation Committee Inquiry into the *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010*, Parliament of Australia, 26 November 2010, 6 (*Castan Centre submission*), on this point. This necessitated amendment to the functions of the Organisation, reflected in the addition of section 17(f) to the *ASIO Act 1979* (Cth), 'to co-operate with and assist bodies referred to in section 19A in accordance with that section'.

43 *Castan Centre submission*, above n 42, 6.

44 That is, the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation and the Defence Signals Directorate.

45 Defined as ASIS, DIGO or DSD: *Intelligence Services Act 2001* (Cth) s 3.

functions.[46] Again, the type of co-operation and assistance that in this instance the agency is able to provide is left open, in an indicative legislative provision.[47]

Importantly, the amendments signal that potent and specialised intelligence capabilities, previously having as their function the collection of intelligence outside Australia, are now primed to take on a significant domestic operation,[48] and are available for targeted application and deployment in non security intelligence areas.[49] Of significance here is the powerful electronic surveillance, eavesdropping and electronic intelligence assessment capacities of the Defence Signals Directorate (DSD) within its signals intelligence and information security roles, in particular its Echelon signals intelligence collection and analysis network operated under the UKUSA intelligence agreement.[50]

In both the *ASIO Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth), the capacity of the respective agency to so co-operate and assist the other nominated bodies is made subject to any

---

46 Those bodies being in section 13A of the *Intelligence Services Act 2001* (Cth) (a) another agency, (b) ASIO, (c) a Commonwealth authority, or a State authority, that is prescribed by regulations for the purposes of this paragraph.

47 *Intelligence Services Act 2001* (Cth) s 13A(3). This raises the same questions about the scope of the information gathering capabilities of these national security agencies falling under the description of 'assistance' and therefore being made available for Commonwealth and State authority purposes.

48 *Castan Centre submission*, above n 42, 9.

49 The capacities of co-operation and assistance conferred by section 13A of the *Intelligence Services Act 2001* (Cth) are reflected in the enlargement of functions for ASIS, DIGO and DSD by the inclusion of 'to co-operate with and assist bodies referred to in section 13A in accordance with that section': see *Intelligence Services Act 2001* (Cth) ss 6(1)(da), 6B(f), 7(f).

50 DSD shares its intelligence with the other states to the UKUSA agreement, namely the United States, the United Kingdom, Canada and New Zealand. For further discussion of DSD, see Ken Barnes 'The Defence Signals Directorate – Its Role and Functions' (1994) 108 *Australian Defence Force Journal* 3; David Wright-Neville 'The Australian Intelligence Community' in Daniel Baldino (ed), *Democratic Oversight of Intelligence Services* (Federation Press, 2010) 33.

Ministerial directions given or arrangements made,[51] and on request of the head of the body to be co-operated with and assisted.[52] These provisions are central to the new arrangements for co-operation and assistance amongst intelligence agencies and between intelligence agencies and other agencies.

The reference in the legislation to the giving of ministerial directions or the making of arrangements, while cohering to principles of Ministerial control and responsibility, and agency line management, in fact only involves optional and non obligatory directions.[53] The coverage and effectiveness of such ministerial directions, where made, is also potentially problematic, both in relation to ASIO and in relation to the intelligence agencies covered by the *Intelligence Services Act 2001* (Cth).

Section 8A of the *ASIO Act 1979* (Cth) provides for Ministerial guidelines to be given to the Director General of Security.[54] Current ASIO ministerial guidelines were issued on 12 October 2007 and include guidance on the handling of personal information.[55] In the Commonwealth Information Commissioner submission to the Senate Legal and Constitutional Affairs Legislation Committee, it was stated:

---

51 *ASIO Act 1979* (Cth) s 19A(2)(a); *Intelligence Services Act 2001* (Cth) s 13A(2)(b).

52 *ASIO Act 1979* (Cth) s 19A(2)(b); *Intelligence Services Act 2001* (Cth) s 13A(2)(a).

53 The simple point is that there may not be any such directions: see *Australian Privacy Foundation submission* , above n 28, 4.

54 Section 8A of the *ASIO Act 1979* (Cth) states that '(1) The Minister may, from time to time, by written notice given to the Director-General, give to the Director-General guidelines to be observed: (a) in the performance by the Organisation of its functions or the exercise of its powers; or (b) in the exercise by the Director General of his or her powers under sections 85 and 86'.

55 *Senate 2010 Report*, above n 32, 20. See especially paragraphs 13.1 to 13.6 (Treatment of Personal Information) in *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security* (including politically motivated violence).

> Given the proposed expansion of ASIO's functions and powers under the Bill, the Office considers it may be appropriate for these guidelines to be reviewed. The Office would be available to assist in any review process.[56]

However, the Attorney-General's department responded less than favourably to review or change of the Attorney-General's guidelines:

> Active consideration has been given to privacy issues in the development of this Bill, including whether the existing Attorney-General's Guidelines and Privacy Rules remain appropriate. In light of the existing privacy regimes, the Attorney-General's Department is of the view that additional privacy frameworks or MOUs do not appear to be necessary. The existing privacy regimes will continue to be reviewed and revised as appropriate to ensure they continue to balance operational considerations with appropriate privacy protections.[57]

In addition, under section 15 of the *Intelligence Services Act 2001* (Cth),

> (1) The responsible Minister in relation to ASIS, the responsible Minister in relation to DIGO and the responsible Minister in relation to DSD, must make written rules regulating the communication and retention by the relevant agency of intelligence information concerning Australian persons.

---

[56] Office of the Australian Information Commissioner, Submission No 13 to Senate Legal and Constitutional Affairs Legislation Committee Inquiry into the *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010*, Parliament of Australia, 26 November 2010 (*Information Commissioner submission*), 8.

[57] Attorney-General's Department, Answers to Questions on Notice and Supplementary Information Senate Legal and Constitutional Affairs Legislation Committee Inquiry into *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010*, Parliament of Australia, 19 November 2010 (*Attorney-General's Department Responses to Questions on Notice and Supplementary Information*), 2. This statement followed an earlier statement in evidence that 'they will need to be reviewed in light of this legislation but possibly even more so in light of other changes in privacy legislation which are in the pipeline': Evidence to Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, Canberra, *Committee Hansard* 11 November 2010, 22 (Mr McDonald).

> (2) In making the rules, the Minister must have regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agencies of their functions.

In relation to ASIS, the Minister issued new *Rules To Protect The Privacy of Australians* on 17 September 2008. The difficulty in obtaining any protective impact from these Privacy Rules under section 13A(2)(a) of the *Intelligence Services Act 2001* (Cth) ministerial directions,[58] arises in that 'intelligence information' in section 15 of the *Intelligence Services Act 2001* (Cth) does *not* include information obtained solely under paragraph 6(1)(da) of the Act, namely, the ASIS function 'to co-operate with and assist bodies referred to in section 13A in accordance with that section'.[59]

The claim of further safeguard aspects by the inclusion of 'on request by the head (however described) of the body referred to in subsection (1)'[60] is somewhat misleading.[61] Indeed, this aspect of the legislation also potentially facilitates extensive co-operative and assistance arrangements negotiated on principles of mutually assured benefit between ASIO and other agencies. That is, other agencies or authorities of the Commonwealth or State might readily seek such co-operation and assistance because of the potency of the available intelligence, technical and other resources deployable in performance of the ordinary functions of such bodies, 'well beyond traditional concepts of national intelligence'.[62]

---

58 That is, 'subject to any arrangements made or directions given by the responsible Minister'.

59 *Intelligence Services Act 2001* (Cth) s 6 'Functions of ASIS'. See *Information Commissioner submission*, above n 56, 14, fn 23; 'In addition, the Office notes the type of information covered under the proposed amendments would not fall within the IS Act's definition of 'intelligence information' and for this reason, would not be covered by any Privacy Rules made pursuant to section 15 of the IS Act': at 14, fn 23.

60 *ASIO Act 1979* (Cth) s 19A(2)(b); *Intelligence Services Act 2001* (Cth) s 13A(2)(b).

61 The *Australian Privacy Foundation submission*, above n 28, 1, describes it as 'being a weak safeguard – invitations would easily be contrived': at 1.

62 *Australian Privacy Foundation submission*, above n 28, 4.

A major component of direct assistance and co-operation by ASIO is provided for in the amended section 19A(4) of the *ASIO Act 1979* (Cth). This section substantially broadens the grounds for the sharing of information that has come into the possession of ASIO in the course of performing its functions under section 17 of the *ASIO Act 1979* (Cth), to circumstances where 'the information is communicated for the purposes of co-operating with or assisting the body' under section 19A of the *ASIO Act 1979* (Cth),[63] being a law enforcement agency,[64] or an authority of the Commonwealth, or an authority of a State, prescribed by regulations.[65] The separate inclusion of this provision, where co-operation and assistance have already been indicatively but not definitively listed,[66] confirms the central function of information communication as a highly important method of co-operation and assistance contemplated by the new section 19A.

V THE RATIONALE FOR CHANGES FACILITATING CO-OPERATION AND ASSISTANCE

Different rationales were advanced by the government in support of these measures removing existing boundaries between agency functions to facilitate co-operation and assistance. A major rationale was a new focus of national security priorities and threats,[67] the

---

63 This amendment extends the provision of such information for purposes of co-operation and assistance, beyond existing provisions only permitting communication of such information to ASIS, DSD and DIGO where the information obtained by ASIO while performing its functions under section 17 of the Act, 'relates, or appears to relate, to the performance of ASIS, DSD or DIGO's functions': *ASIO Act 1979* (Cth) s 18(4A).

64 *ASIO Act 1979* (Cth) s19A(1)(d), (4).

65 *ASIO Act 1979* (Cth) s19A(1)(e), (4).

66 *ASIO Act 1979* (Cth) s19A(3).

67 Commonwealth, *Parliamentary Debates*, House of Representatives 24 June 2010, 6528 (Robert McClelland); *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010* (Cth) *Replacement Explanatory Memorandum*, 24.

interconnectedness of these issues,[68] and producing whole of government national security priorities.[69] Linked to these aspects was an intended capacity to be readily able to expand the range of agencies involved in co-operative arrangements if this became necessary in the future.[70] In responding to such interconnected priorities and threats, resource utilisation issues were also discussed– interoperability of personnel between agencies,[71] the use of multi-agency teams to assist other agencies to carry out functions,[72] and the effective provision of various forms of identified assistance[73] to agencies.

VI ENHANCING THE COMMUNICATION AND SHARING OF INFORMATION BETWEEN AGENCIES AND AUTHORITIES

Aside from circumstances involving discretionary ASIO and other intelligence agency *co-operation and assistance* with performance of functions of other intelligence agencies, law enforcement agencies and prescribed Commonwealth and State authorities, the legislation also makes enhanced provision for ASIO to communicate information that has *incidentally* come into ASIO's possession,[74] while performing its section 17 *ASIO Act 1979* (Cth) functions,[75]

---

68 *Attorney-General's Department submission*, above n 2, 2.

69 Ibid.

70 *Replacement Explanatory Memorandum*, above n 67, 24; *Attorney-General's Department submission*, above n 2, 2.

71 Commonwealth, *Parliamentary Debates* House of Representatives 24 June 2010, 6528 (Robert McClelland); *Attorney-General's Department submission*, above n 2, 2.

72 *Attorney-General's Department submission*, above n 2, 2; *Replacement Explanatory Memorandum*, above n 67, 24.

73 Commonwealth, *Parliamentary Debates* House of Representatives 24 June 2010, 6528 (Robert McClelland); *Replacement Explanatory Memorandum*, above n 67, 24.

74 This provision obviously applies to information sourced by a wide variety of ASIO intelligence gathering techniques extending beyond telecommunications interception information.

75 See *ASIO Act 1979* (Cth) s 17(1)(a) to (f).

where such '...information relates, or appears to relate, to the performance of the functions, responsibilities or duties' of Ministers, Commonwealth authorities and State authorities.[76] Each of these relevant phrases is of wide import, so the dimensions of potential information communication are bounded by the wide facility for its collection[77] and the broad categories of potential recipients of that information.[78]

This capacity for such information communication is nominally restricted by two qualifications. Firstly, that the information relates, or appears to relate, to the intended commission, of a serious crime.[79] The limited nature of this qualification and the contrasting broadening of activity included is confirmed by the fact that activities committed outside of Australia constituting no crime where committed are incorporated within the legislation's definition of 'serious crime'. This inclusion is on the hypothesis that *if* the conduct were engaged within or in connection with Australia, such conduct would constitute a Commonwealth, State or Territory offence punishable by imprisonment exceeding 12 months.[80] The removal of previous requirement that the offence be an indictable offence[81] has also broadened the category of information able to be communicated, by reducing the seriousness of the relevant real or hypothetical offence.

---

76 See *ASIO Act 1979* (Cth) s 18(3)(c), 18(4).

77 That is, under section 18(3)(a) of the *ASIO Act 1979* (Cth) the information has come into the possession of the Organisation in the course of performing the Organisation's functions under section 17.

78 Namely, '(a) A Minister, (b) a staff member of an authority of the Commonwealth, (c) a Staff member of an authority of a State': *ASIO Act 1979* (Cth) s 18(4).

79 Defined as 'conduct that, if engaged in within, or in connection with, Australia, would constitute an offence against the law of the Commonwealth, a State or a Territory punishable by imprisonment for a period exceeding 12 months': *ASIO Act 1979* (Cth) s 4.

80 *ASIO Act 1979* (Cth) s 4. For comments on this point see *Australian Privacy Foundation submission*, above n 28; *Castan Centre submission*, above n 41.

81 See previous section 18(3)(a) of *ASIO Act 1979* (Cth) (as at 7 June 2010).

A second, alternative restriction is that the Director-General of Security, or a person authorised for the purpose by the Director-General, is satisfied that the national interest requires the communication.[82] Two points are of significance here. The legislation is now broadened in that the national interest test applies to all information, both external and internal, to Australia, which has come into the possession of ASIO in performing its section 17 functions. This replaces the previous narrower requirement 'where the information has come into the possession of the Organisation *outside* Australia or concerns matters *outside* Australia'.[83] Furthermore, the characteristics of the information under application of a national interest test for potential communication clearly go beyond any connection with the real or hypothesised commission of criminal offences.[84]

More important perhaps are the circumstances attaching to the application of the national interest test. The Director General of Security is able to authorise other persons for the purpose of being satisfied that the national interest requires the communication.[85] Furthermore, there is no legislative specification, guidance or determination as to what constitutes 'national interest' for the purpose of communication of ASIO acquired information. Accordingly, the assessment of what information should be communicated as in the national interest is likely to be considered and determined from a dominant national security perspective, even where no genuine national security issue arises, and the information relates to the broadest application of government policy and the implementation of government programs.

---

82 See *ASIO Act 1979* (Cth) s 18(3)(b)(i), (ii) (as at 7 June 2010).

83 See former section 18(3)(b) of the *ASIO Act 1979* (Cth) (as at 7 June 2010).

84 As the *Castan Centre submission*, above n 42, identifies, 'the potential recipients of communication would be broadened well beyond those Australian agencies concerned with the enforcement of Australian law, to encompass a wide range of agencies concerned with the full spectrum of Australian government policy': at 3.

85 *ASIO Act 1979* (Cth) s 18(3)(b)(ii). The delegation to an authorised person itself expands the scope and discretion of the power to communicate.

The highly subjective, and hence security determinable nature, of what constitutes the national interest for the purposes of communication[86] is confirmed by evidence which emerged during the Senate Committee inquiry into the legislation.[87] The Attorney-General's department cited examples involving taxation and migration matters that would justify communication of information in the national interest.[88] A more general response of the Attorney-General's department to the content of national interest, and who determines that national interest, alarmingly confirms the executive discretionary and enabling characteristics of the ASIO communicative provision:

> The term 'national interest' is used in other contexts in Commonwealth legislation where it is also not defined. Courts, when considering decisions made on grounds of national interest in other contexts, have generally expressed views indicating that the primary determination of what is in the national interest is for the Minister. In a democracy, it is appropriate for the Government of the day to set its priorities and determine what is in the national interest. The types of matters that might be encompassed by the term may include matters of importance to Australia's international relations or to sustaining the economy. In the national security context, national interest may be informed by the National Security Statement and the National Security Priorities, which are set by the Government and reviewed on at least an annual basis.[89]

The dominance of self-regulating and discretionary security perspectives in assessing what falls within the national interest is reinforced by the loose and tentative connection that the information '*appears to relate* to the performance of the functions, responsibilities or duties of the person referred to in subsection (4)'.[90] In turn, the potential recipients to whom information may be

---

86 Under the *ASIO Act 1979* (Cth) s 18(3)(b)(ii).

87 Submissions from the Law Council of Australia, the Australian Privacy Foundation and the Castan Centre to the Senate Legal and Constitutional Affairs Legislation Committee raised concerns about the content and application of the national interest test.

88 See *Senate 2010 Report*, above n 32, 37.

89 Attorney-General's Department, above n 57, 15-16. See also *Senate 2010 Report*, above n 32, 37-38.

90 *ASIO Act 1979* (Cth) s 18(3)(c).

communicated, in particular an authority of the Commonwealth[91] and an authority of a State,[92] extend to a host of government activities that do not even have a remote connection with security and the security purposes for which the information was originally obtained, with the legislation now allowing that information so obtained to be derivatively applied.

This aspect of the legislation is remarkable for its generous drafting which will facilitate ASIO dissemination of both domestic[93] and international information originally obtained under its variety of covert intelligence collection procedures,[94] and linked to the expanded definition of 'security'.[95] This significant expansion of potential information communication and its concentration of executive power and discretion are the defining features of this aspect of the legislation. The facilitation of such information communication to Commonwealth and State authorities on a security sourced interpretation and application of national interest, affords significant risks of introducing improper and extraneous considerations into Commonwealth and State authority decision making, derived from adverse and untested conclusions from the information communicated about individuals and associations. In other words, such decisions may be made or influenced on the basis of intelligence rather than evidence, hypotheses rather than facts, with the real basis of the decision so influenced, then withheld from individuals affected by the decision and so not properly contestable.

---

91 *ASIO Act 1979* (Cth) s 18(4)(b). An authority of the Commonwealth is broadly defined: see *ASIO Act 1979* (Cth) s 4.

92 *ASIO Act 1979* (Cth) s 18(4)(c). An authority of a State is broadly defined: see *ASIO Act 1979* (Cth) s 4.

93 Under the previous legislation, the information subject to the national interest test had to have come into the possession of ASIO outside of Australia or concern matters outside Australia

94 As part of its functions under section 17(1)(a) of the *ASIO Act 1979* (Cth) 'to obtain, correlate and evaluate intelligence relevant to security', ASIO is able to exercise a range of special powers: see *ASIO Act 1979* (Cth) ss 22 to 34 ('Division 2 – Special Powers'), ss 34A to 34S ('Division 3 – Special powers relating to terrorism offences').

95 See definition of 'security': *ASIO Act 1979* (Cth) s 4.

The inclusion of the expanded function of information communication, as an ASIO function, is subject to the general protective requirement of section 17A of the *ASIO Act 1979* (Cth), which states that 'This Act does not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly'. However, the new expansive and discretionary powers enabling the communication of security sourced information for Commonwealth and State authority purposes will encourage a narrow, technical reading of that protective provision[96] as meaning only directly imposed limitations on the right of persons to engage in lawful advocacy, protest or dissent.[97]

A further significant change relating to communication and intelligence sharing is provided for in liberalising the communication of information from ASIO to the other intelligence agencies, ASIS, DSD and DIGO,[98] particularly as the former restriction that the information has come into the possession of ASIO outside Australia or concerns matters *outside* Australia[99] has been removed. The significance of this change is that domestic sourced and domestic related information obtained by ASIO, under its variety of covert intelligence collection procedures[100] and linked to a broad and expanded definition of 'security',[101] may be provided

---

96 A similar point is made in the *Castan Centre submission*, above n 42, 4, that while the expanded grounds for communication may not actively limit political freedom, the possibility of communication by ASIO of information deemed contrary to the national interest to authorities may produce a chilling effect on such political activity.

97 Such an interpretation would also cohere with section 17(2) of the *ASIO Act 1979* (Cth) which states 'It is not a function of the Organisation to carry out or enforce measures for security within an authority of the Commonwealth'.

98 ASIO may communicate information to a staff member of ASIS, DSD or DIGO if (a) the information has come into the possession of the Organisation in the course of performing the Organisation's functions under section 17; and (b) the information relates, or appears to relate, to the performance of ASIS, DSD or DIGO's functions: *ASIO Act 1979* (Cth) s 18(4A).

99 See previous version of section 18(3)(b) of the *ASIO Act 1979* (Cth) (at 7 June 2010).

100 *ASIO Act 1979* (Cth) ss 22-34 pt 3 div 2.

101 *ASIO Act 1979* (Cth) s 4.

to the three foreign focused Australian intelligence agencies, provided, at a minimum, the information '*appears to relate* to the performance of ASIS, DSD or DIGO's functions'.[102] The legislation therefore facilitates a blurring of the roles between domestic source intelligence and foreign source intelligence and intelligence collection, collation and analysis; all of the attendant consequences of the enlargement and concentration of discretionary intelligence agency executive power; and the potential application of domestic sourced information obtained in pursuit of a legislative security mandate under special collection powers being applied, on a discretionary and incidental basis, to the performance of ASIS, DSD or DIGO's functions.

This liberalisation of the collection and communication of ASIO intelligence in relation to the other, overseas focused intelligence agencies has been rapidly supplemented through additional *ASIO Act 1979* (Cth) amendments, which were made by the *Intelligence Services Legislation Amendment Act 2011* (Cth).[103] The principal addition is ASIO's expanded capacity to obtain and communicate foreign intelligence, prompted by advice received from the Ministers with portfolio responsibilities for DSD, DIGO and ASIS.[104] The obtaining and communication of foreign intelligence continues as a legislated ASIO function under section 17(1)(e) of the *ASIO Act 1979* (Cth).[105] However, two important changes expand the scope of

---

102 *ASIO Act 1979* (Cth) s 18(4A)(b) (emphasis added).

103 For a brief online commentary of this legislation see Michael Head 'ASIO's overseas powers dramatically expanded', ABC *The Drum* Opinion 18 August 2011 <http://www.abc.net.au/unleashed/2844934.html> at 1 December 2011.

104 Sections 27A and 27B of the *ASIO Act 1979* (Cth), respectively relating to the collection of foreign intelligence through the exercise of ASIO's warrant powers and the collection of foreign intelligence by other means, rely upon the authorising Minister's satisfaction 'on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, that the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being'

105 Section 17(1)(e) provides the ASIO function 'to obtain within Australia foreign intelligence pursuant to section 27A or 27B of this Act or section 11A, 11B or 11C of the *Telecommunications (Interception and Access) Act 1979* and to communicate any such intelligence in accordance with this Act or the

this provision, and also of the reach of the intelligence agencies communication and co-operation amendments in the *ASIO Act 1979* (Cth).[106]

First, 'foreign intelligence' now means 'intelligence about the capabilities, intentions and activities of people or organisations outside Australia'.[107] Accordingly, the meaning has been expanded to encompass individuals and groups with no state based affiliation. Second, the thresholds justifying the collection of foreign intelligence (as broadly defined) have also been generously expanded, with the issuing Minister or authorising Minister (in this case the Commonwealth Attorney-General) required to be satisfied on Defence or Foreign Affairs ministerial advice 'that the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being'.[108] These three amorphous sets of interests replace the previous narrower criteria that the 'collection of foreign intelligence...is important in relation to the defence of the Commonwealth or to the conduct of the Commonwealth's international affairs'.[109]

In this sense, the new thresholds mirror the indefinite and security determined concept of 'national interest' as the criterion for the communication of incidentally obtained ASIO information to Ministers and State and Commonwealth authorities in section 18 of the *ASIO Act 1979* (Cth).[110] In particular, the conception of Australia's national security and its economic well-being as being a new set of interests relevant to warrant and other intelligence gathering powers for foreign intelligence, reveals the scope of the reforms. The obtaining of that foreign intelligence as an ASIO

Telecommunications (Interception and Access) Act 1979': *ASIO Act 1979* (Cth) s 17(1)(e).

106 *ASIO Act 1979* (Cth) s 18(4A), s 19A(1).

107 *ASIO Act 1979* (Cth) s 4 (as at 29 July 2011). Previously, foreign intelligence meant 'intelligence relating to the capabilities, intentions or activities of a foreign power': *ASIO Act 1979* (Cth) s 4 (as at 29 March 2011).

108 *ASIO Act 1979* (Cth) s 27A(1)(b), 27B(b).

109 See *ASIO Act 1979* (Cth) s 27A(1)(b), 27B(b) as at 29 March 2011.

110 See the discussion above under the present heading.

function is linked to the power to 'communicate any such intelligence *in accordance with this Act* or the *Telecommunications (Interception and Access) Act 1979* (Cth)'.[111] The prefacing of the gathering of such foreign intelligence on the basis of Defence and Foreign Affairs ministerial advice, points *primarily* to the communication of such information to foreign focused intelligence agencies within those portfolios, namely DSD, DIGO and ASIS, under section 18(4A) of the *ASIO Act 1979* (Cth). However, that foreign intelligence material is also amenable to communication as 'information [that] has come into the possession of the Organisation in the course of performing the Organisation's functions under section 17', the incidental information prefacing requirement for communicating that information to a Minister or a State or Commonwealth authority[112] and for communication of information to a law enforcement agency or a prescribed Commonwealth or State authority for purposes of co-operation and assistance.[113] Accordingly, foreign intelligence obtained by ASIO within Australia under these additional powers is ultimately available to the same information communication audiences as other sources of ASIO intelligence.

Some brief rationales were advanced by the government relating to the legislative changes made by to increase the communication and sharing of intelligence between agencies and authorities. The effectiveness of responding to identified national security threats was identified as a reason for increasing the connectivity of agencies by removing barriers to communication and information sharing.[114] ASIO was also said to require flexible arrangements to support its capacity to co-operate with and assist other national security agencies.[115]

---

111 *ASIO Act 1979* (Cth) s 17(1)(e) (emphasis added).

112 *ASIO Act 1979* (Cth) s 18(4).

113 *ASIO Act 1979* (Cth) s 19A(4).

114 Commonwealth, *Parliamentary Debates* House of Representatives, 24 June 2010, 6527 (Robert McClelland).

115 *Attorney-General's Department submission*, above n 2, 3; *Replacement Explanatory Memorandum*, above n 67, 25.

VII THE HISTORICAL CONTEXT OF THE LEGISLATION – TRANSITION, CHANGE AND CONTINUITY FROM THE HOWARD GOVERNMENT

A clearer and more comprehensive appreciation of the impact and consequences of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) for the evolution of Australian national security policy can be obtained by briefly assessing the transitional circumstances from Howard government national security enactments (which preponderantly dealt with terrorism matters) to the Rudd and Gillard government national security enactments (which have expanded the scope of national security legislative topics).

The expansionary subject matters of information communication and agency assistance and co-operation as found in the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) represent and reflect new emphases and priorities in national security policy under a different government. There is however, common ground between the Howard and Rudd/Gillard governments in the ongoing accretion of executive discretion and authority in national security matters, facilitated by a renewed round of legislative reform. In that sense, the transition from the legislative program of one government to its successors simultaneously reflects both continuity and change – that is, both shared and different characteristics in legislative and policy formation. It is more accurate to see the relationship between the two government policies and practices as evolutionary, rather than as differentiated.

VIII THE HOWARD GOVERNMENT AND ITS TERRORISM LEGISLATIVE AGENDA

There are certain distinctive identifying features of the Howard government national security legislative agenda. A multiplicity of terrorism laws were enacted over a period of years, amounting to a serial counter-terrorism legislative agenda,[116] far exceeding that of comparable common law nations.[117] Two prominent features emerged as part of this Howard government legislative agenda - the paradigm of urgency in the legislative process,[118] as well as an asserted compliance of the legislation with international human rights law, in spite of considerable contrary evidence.[119] The general legacy of this legislative agenda was in the concentration of executive control, power and discretion that the various new terrorism laws conferred. Swift passage of the legislation, accompanied by few amendments, was the preferred legislative method, often accompanied by a discounting of parliamentary and other review recommendations and a subsequent unwillingness or

---

116 Over 40 pieces of counter-terrorism legislation were passed by the Howard government since 2001: *Chronology of Legislative and other Legal Developments since September 11 2001* (Parliamentary Library) <http://www.aph.gov.au/library/intguide/law/terrorism.htm#terrchron> at 12 June 2011. For four distinct phases in Howard government terrorism law enactment, see Anthony Reilly 'The processes and consequences of counter-terrorism law reform in Australia: 2001-2005' (2007) 10 *Flinders Journal of Law Reform* 81.

117 Such as the United Kingdom, Canada and New Zealand.

118 See Andrew Lynch, 'Legislating with Urgency – the Enactment of the Anti-Terrorism Act [No 1] 2005 (2006) 30 *Melbourne University Law Review* 747; Reilly, above n 116, 91; Martin Krygier, 'War on Terror' in Robert Manne (ed) *Dear Mr Rudd: Ideas for A Better Australia* (2008), 137; Carne, 'Hasten Slowly: Urgency, Discretion and Review – A Counter-Terrorism Legislative Agenda and Legacy', above n 4.

119 See Greg Carne, 'Neither Principled nor Pragmatic? International Law, International Terrorism and the Howard Government', II 'Assertions of Compliance with International Law in Developing Domestic Counter-terrorism legislation' (2008) 27 *Australian Year Book of International Law* 11, 13-19.

neglect to review and amend enacted legislation to strengthen safeguards and increase accountability.[120]

Some particularly controversial national security matters relating to counter-terrorism arose during the Howard government. Four significant reviews arising from national security terrorism law topics arising during the tenure of the Howard government were conducted,[121] with responsibility for legislative and other responses to those reviews falling to its Labor successors.

This initial difference between these governments in content and chronology in national security legislative matters – one government exhaustively legislating and the other government reviewing and responding to the reviews of that legislation – provides an important prism for comprehending the developments in the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth).

IX THE RUDD AND GILLARD GOVERNMENTS

Importantly, the present legislation emerges after a sharp reduction in national security legislative enactment, following the change of

---

[120] This process became pronounced with the Howard government gaining control of the Senate in 2004, and with the appointment of Philip Ruddock as Attorney-General in 2003.

[121] The relevant reviews were: MJ Clarke QC, *Report of the Inquiry into the Case of Dr Mohamed Haneef* (2008) (*Clarke Inquiry*); Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia* Report 104 (2006); Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the proscription of 'terrorist organisations' under the Australian Criminal Code* (2007); Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of Security and Counter-Terrorism Legislation* (2006). For a discussion of the *Clarke Inquiry* into the Haneef matter, see Michael Head 'What the Haneef Inquiry Revealed (and did not)' (2009) 34 *Alternative Law Journal* 243; Mark Rix 'The Haneef Case and an independent reviewer of terrorism law' (2009) 34 *Alternative Law Journal* 50.

government in 2007. This reflected a period of consolidation in the Government response to the four national security legislation reviews,[122] and early indications of a shift in emphasis in national security policy. This shift in emphasis was signaled in the first major national security address of Attorney General McClelland, which emphasised community building, public diplomacy and inclusive development, as a method of reducing alienation in relevant sections of the community.[123] At the same time, criticism was made of the previous government's emphasis upon, and political use of, a national security legislative agenda.[124]

The changed legislative context after 2007 is reflected in the cessation of serial counter-terrorism legislative enactments and, for the most part, the cessation of the paradigm of urgency in those legislative enactments. Instead, what has emerged on the topic of terrorism and national security is a more regular legislative program. This has comprised relatively few significant pieces of national security legislation, and several other consequential amendments to national security legislation.[125] The significant pieces of national security legislation can be identified as the *Telecommunications (Interception and Access) Amendment Act 2008* (Cth), the *Independent National Security Legislation Monitor Act 2010* (Cth), the *National Security Legislation Amendment Act 2010* (Cth) and of course, the present legislation, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth). This reduction in national security legislative activity should not mask the fact that the present legislation engineers a new paradigm for interactions between intelligence agencies and ordinary government agencies. As such, it is ground breaking and likely to

---

122 See the four reviews detailed in footnote, above n 121.

123 Robert McClelland, 'Security in Government Conference' (Speech delivered at Security in Government Conference, Canberra, 7 December 2007) <http://www.attorneygeneral.gov.au/Speeches/Pages/2007/Fourthquarter/7December2007SecurityinGovernmentConference.aspx> at 1 December 2011.

124 Ibid.

125 See, eg, the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011* (Cth); *Crimes Legislation Amendment (Serious and Organised Crime) Act (No 2) 2010* (Cth); *Financial Transaction Reports Amendment (Transitional Arrangements) Act 2008* (Cth)

affect profound change in the relational aspects of democracy between the citizen and the state, through an increasing capacity to incorporate national security elements in the decision making and program delivery of Commonwealth and State instrumentalities.

Context and timing are therefore important in understanding the present Act and its transformative characteristics in information communication, co-operation and assistance, from a national security perspective. Responding to the four significant national security legislation reviews[126] arising from matters in the term of the Howard government has been the dominant priority of national security legislative change from 2008 and the term of the Rudd and Gillard governments. This priority commenced with the announcement of comprehensive legislative and other responses to these reviews.[127] Accordingly, a Discussion paper,[128] with draft legislation, was open for public comment and submissions until 25 September 2009. The *National Security Legislation Amendment Bill 2010* (Cth), which proposed a series of reforms in response to the four national security law reviews, was referred by the Senate[129] to the Legal and Constitutional Affairs Legislation Committee for inquiry and report.[130] Following the 2010 Federal election, the bill

---

126 See the four reviews detailed in footnote, above n 121.

127 Robert McClelland, 'Comprehensive Response to National Security Legislation Reviews' (Attorney-General Media Release 23 December 2008) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2008/Fourthquarter/23December2008ComprehensiveResponsetoNationalSecurityLegislationReviews.aspx> at 1 December 2011.

128 See *National Security Legislation Discussion Paper* (2009) which was released by the Attorney-General on 12 August 2009: Robert McClelland, 'National Security Legislation Discussion Paper' (Attorney-General Media Release 12 August 2009) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2009/Thirdquarter/12August2009NationalSecurityLegislationDiscussionPaper.aspx> at 1 December 2011.

129 On 18 March 2010.

130 Commonwealth of Australia Senate Legal and Constitutional Affairs Legislation Committee *National Security Legislation Amendment Bill 2010 [Provisions] and Parliamentary Joint Committee on Law Enforcement Bill 2010 [Provisions]* (June 2010).

was reintroduced into the Parliament[131] and was finally enacted on 15 November 2010.[132]

It is apparent that the publicity and controversy surrounding the four reviews, the facility provided by the Discussion paper for debate and submissions, and the fact that the *National Security Legislation Amendment Bill 2010* (Cth) was drafted as remedying widely publicised, problematic national security Howard era issues, meant that this bill attracted significant, prolonged publicity and scrutiny. The protracted process and the significant content of the four reviews also meant that the *National Security Legislation Amendment Bill 2010* (Cth) dominated a visibly less active national security legislative agenda.

The timing of the *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010* (Cth) is important, having been being reintroduced into the Parliament on the same day[133] as the *National Security Legislation Amendment Bill 2010* (Cth). The circumstances of the former bill, in not being of a directly remedial response to a well publicised set of identified problems, and in appearing to deal with technical issues, meant that it was overshadowed by the attention given to the *National Security Legislation Amendment Bill 2010* (Cth). This is reflected in the fairly bland and uncritical report of the Senate Legal and Constitutional Affairs Legislation Committee.[134] The Senate Committee report typically states criticisms and observations from submissions on the bill, and then provides the Attorney General's Departmental

---

131 Robert McClelland, 'Reintroduction of national security legislation' (Attorney-General Media Release 30 September 2010) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2010/Thirdquarter/30September2010Reintroductionofnationalsecuritylegislation.aspx> at 1 December 2011.

132 Robert McClelland, 'National Security Legislation passes the Parliament' (Attorney-General Media Release 15 November 2010) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2010/Fourthquarter/15November2010NationalSecurityLegislationpassestheParliament.aspx> at 1 December 2011

133 30 September 2010.

134 *Senate 2010 Report*, above n 32.

response. It fails to provide a stringent critical appraisal or analysis of the legislation, reflected also in the minimalist recommendations made by the Committee.[135] The Senate Committee erroneously appears to have assumed that this new legislation dealt with fairly routine matters.

However, these contrasting issues of timing and content between the two contemporary pieces of legislation provide a revealing, but incomplete appraisal of the transformative characteristics in information communication, co-operation and assistance, from a national security perspective, of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth). There are other significant influential explanatory factors.

X TRANSFORMING THE MEANING OF NATIONAL SECURITY AND NATIONAL SECURITY PRIORITIES

Of great formative influence for the present legislation are the important national security policy documents[136] promoted by the

---

[135] The *Senate 2010 Report* only recommended '(1) a revision and reissue of the Explanatory Memorandum (2) that guidelines be developed by the Attorney-General's Department to provide further clarification to carriers and carriage service providers about their reporting requirements under the Bill and (3) that subject to these first two recommendations, the committee recommends that the Senate pass the bill': see *Senate 2010 Report*, above n 32, recommendations 1-3, paras 3.104, 3.105, 3.106.

[136] Namely, the Prime Minister's National Security Statement: *First National Security Statement to the Parliament* (2008) (*National Security Statement*); see also Commonwealth, *Parliamentary Debates*, House of Representatives, 4 December 2008, 12549 (Kevin Rudd)); Ric Smith, *Summary and Conclusions Report of the Review of Homeland and Border Security* (2008) (*Smith Review*); Department of Prime Minister and Cabinet, *Counter-Terrorism White Paper: Securing Australia- Protecting our Community* (2010) (*Counter Terrorism White Paper*); Department of Prime Minister and Cabinet *National Security Information Environment Roadmap: 2020 Vision*

Rudd and Gillard governments. In one sense, these policy documents replace rapid and serial legislative enactment as the major influence or characteristic in shaping the present national security legislative response. The perspectives and approaches in the policy documents are, in a different way, the formative source of the significant legislative changes and consequences in the present legislation. These changes and consequences are profound, in that the information sharing, co-operation and assistance facilitated by the legislation marks a significant re-alignment of the future governance relationship between the citizen and the Australian executive.

Rather than seeing the changes to that relationship brought about by serial legislative enactments on discrete counter-terrorism topics, change is now being affected in a new paradigm - an overarching principle of the integration of agency activity and the dismantling of existing and protective legislative separations between national security agencies and other Commonwealth and State agencies. The reforms demonstrate a strong move towards the securitisation of ordinary aspects of government administration. That change is open ended and potentially incremental, limited in practical terms mostly by resource and budgetary constraints. It is likely that the consequences of such change will outweigh other contrary accountability measures,[137] to slow or reverse the concentration of executive power or discretion emerging from the legacy of the Howard government terrorism law enactments.

(2010) (*Roadmap*). On the *National Security Statement*, see 'First National Security Statement to the Australian Parliament' (2009) 24 *The Australian Journal of Emergency Management* 3. On the *Counter-Terrorism White Paper*, see Gregor Urbas 'Counter-terrorism white paper' (2010) 12 *Internet Law Bulletin* 175.

[137] Such as the establishment of an Independent National Security Monitor to review the operation, effectiveness and implications of national security legislation; amending the *Inspector General of Intelligence and Security Act 1986* (Cth) to allow the Inspector General of Intelligence and Security to inquire into the activities of Commonwealth agencies that are not members of the Australian Intelligence Community; and establishing the Parliamentary Joint Committee on Law Enforcement to oversee the Australian Federal Police and the Australian Crime Commission.

XI THE IMPORTANCE AND INFLUENCE OF THE NATIONAL SECURITY POLICY DOCUMENTS

Some key features are discernable in the policy documents which inform and underpin the significant changes in the present legislation. Foremost of these is an enlarged conception of national security. By significantly expanding the parameters of what constitutes national security for legislative policy purposes, it becomes conceptually consistent that ordinary (that is, non intelligence or non national security) Commonwealth and State agencies become the recipients of co-operation, assistance and information sharing from national security agencies, and become enmeshed as participants in a national security culture. The Prime Minister's December 2008 National Security Statement first provides an expansive conception of national security supportive of those ends, in a manner that will inevitably intersect with ordinary government administration:

> What is meant by national security? Freedom from attack or the threat of attack; the maintenance of our territorial integrity; the maintenance of our political sovereignty; the preservation of hard won freedoms; and the maintenance of our fundamental capacity to advance economic prosperity for all Australians ...Of course, not all security challenges we face are by definition national security challenges. Some, such as community safety and low level criminality, quite properly fall outside the scope of national security. Our state and territory governments have constitutionally mandated responsibilities for these. This distinction allows the Australian government to focus on clear and enduring security interests that transcend the scope of state and territory jurisdictional responsibilities. [138]

In citing the Prime Minister's meaning of national security, the Commonwealth Attorney General later identified threats to national security as including:

> ...non traditional threats such as serious and organised crime, electronic attack and ...natural disasters...Second, in response to the

[138] *National Security Statement*, above n 136, 1-2.

> broader concept of national security, the Government has re-iterated its commitment to an "all hazards" approach. By "all hazards" approach, we mean agencies well-equipped and ready to detect, deter and/or deal with a crisis or attack on Australia's security of any kind.[139]

This meaning, in the National Security statement, forming 'part of the Government's long term reform agenda by setting out our national security policy framework for the future',[140] conceives of an ever expanding, evolutionary list of 'non traditional threats or new security challenges'.[141] These threats and challenges include transnational crime, border security, people smuggling, information technology vulnerability, e-security, vulnerability to disease and pandemics, climate change and regional demographic change.[142] The concept of national security necessarily being enlarged and engaged by the emergence of a multiplicity of threats and hazards is also a strong feature of other formative sources, such as the Smith Review,[143] the National Security Information Environment Roadmap[144] and in contemporary comments by the Commonwealth Attorney General.[145]

---

139 Robert McClelland, 'Address 7th Annual National Security Australia Conference' (Speech delivered at 7th Annual National Security Australia Conference, Sydney, 23 March 2009) <http://www.attorneygeneral.gov.au/Speeches/Pages/2009/Firstquarter/23March20097thAnnualNationalSecurityAustraliaConference.aspx> at 1 December 2011.

140 *National Security Statement*, above n 136, 1.

141 Ibid 5.

142 Ibid 6.

143 *Smith Review*, above n 136, 1: 'Australia faces threats from a range of sources which in different ways can put our institutions of state, our people, our economic assets and our technology at risk. These hazards include espionage, foreign interference, terrorism, politically motivated violence, border violations, drug trafficking, cyber attack, organised crime, natural disasters, industrial accidents and biosecurity events': at 1.

144 The *Roadmap* states that 'numerous complex threats to our nation's security have emerged', involving diverse national security challenges 'ranging from terrorism, cyber-threats, trans-national crime, climate change and natural disasters': *Roadmap*, above n 136, 1, 4.

145 See Robert McClelland, 'Address to the National Security College Senior Executive Development Course Dinner' (Speech delivered at 10 March 2011, Old Parliament House, Canberra), 2

With the dimensions of the national security threats and challenges stated exponentially, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) was drafted in circumstances favourable to an extended national security mandate, beyond the hitherto dominant topic of terrorism. Indeed, the Counter Terrorism White Paper[146] itself emphasises collaboration, co-ordination and co-operation – noting the importance of the relationships between agencies and the need for these identified qualities across the full range of government counter-terrorism measures.[147] Similar observations of inter-agency co-operative approaches in relation to counter-terrorism are made elsewhere.[148] Accordingly, these formative documents indicate that national security responses to terrorism provided an example or template for the significantly expanded co-operative, communicative and assistance framework favoured by the present legislation,[149] as applied to much more broadly conceived national security purposes.

<http://www.attorneygeneral.gov.au/Speeches/Pages/2011/First%20Quarter/10March2011AddresstotheNationalSecurityCollegeSeniorExecutiveDevelopmentCourseDinner.aspx> at 1 December 2011: 'This broad approach recognises that, at any given time, there are many risks and dangers that threaten Australia's security – from espionage, terrorism, border violations, cyber attack, organised crime, natural disasters and biosecurity events. These threats pose both security and safety risks, not only to Australia's institutions of state but also to its people, economic assets, infrastructure and technology': at 4.

146 *Counter-Terrorism White Paper*, above n 136.

147 Ibid iv, 23, 59.

148 *Smith Review*, above n 136, 11; McClelland, above n 145, 4; Commonwealth, *Parliamentary Debates*, House of Representatives, 23 February 2010, 1498 (Robert McClelland): It is 'an essential part of the strategy is establishing a Counter-Terrorism Control Centre, which will be established within the Australian Security Intelligence Organisation. It will provide coordination across government agencies in counter-terrorism intelligence, decision making and operations...It will drive a fully integrated national approach to counter-terrorism by identifying specific counter-terrorism priorities and developing a stronger fusion of the intelligence and law enforcement community effort': at 1498.

149 As discussed under the three headings examining the main characteristics of the present legislation, above, namely 'Assistance to law enforcement and interception agencies with telecommunications interception', 'Improving co-operation and assistance between intelligence agencies, law enforcement and prescribed state and Commonwealth authorities' and 'Enhancing the communication and sharing of information between agencies and authorities'.

XII ADDITIONAL INFLUENCES OVER THE FORMATION OF THE LEGISLATION

Other factors also appear to have been influential in developing the present legislation. One explanation for the new legislation is opportunism – the legislation extrapolates from the investment, development and achievement in counter-terrorism activity since September 2001 and the resultant high levels of inter-agency and cross-jurisdictional co-operation. Two examples are illustrative of this development. The first example relates to the inter-operability between the AFP and ASIO and the AFP and state police forces in counter-terrorism programs, following the Street Review of national security operations.[150] A Joint Operations Protocol was established between the AFP and ASIO[151] in response to the Street Review. Joint Counter Terrorism Teams, now established in each Australian jurisdiction, 'are a partnership arrangement, comprising members from the AFP, state and territory police, Australian Security Intelligence Organisation officers and representatives from other agencies where required'[152] and have led major counter-terrorism

---

[150] Sir Laurence Street, *A Review of the Interoperability Between the AFP and its National Security Partners* (2008) (*Street Review*). The *Street Review* was asked to report on, *inter alia*, '1. the current role and responsibilities of the AFP and other relevant national security agencies, including ASIO and State police, in conducting national security operations, 2. the status and terms of the current relationship and interaction between relevant national security agencies including observations about the effect that the current interaction has on the discharge of AFP functions in the conduct of national security operations'. Among other things, the Street Review recommended 'full time attachment, physical co-location and participation in Joint Counter-Terrorism teams': *Street Review*, Recommendation 4.

[151] The protocol providing for a 'regular opportunity for the agency heads to review and resolve strategic priorities and interoperability issues in national security operations': see Robert McClelland, 'Attorney-General Welcomes Progress On Implementation Of Street Review' (Attorney-General's Media Release 16 October 2008) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2008/Fourthquarter/16October2008AttorneyGeneralWelcomesProgressonImplementationofStreetReview.aspx> at 1 December 2011.

[152] See Australian Federal Police *Annual Report 2010-2011* (2011) (*AFP Report*) 25. Importantly, during 2010-2011, the AFP negotiated nationally consistent memoranda of understanding with each state and territory jurisdiction, to

preventive operations.[153] The second example relates to the inter-operability of both Commonwealth and State counter-terrorism preventative detention legislation, with other forms of Commonwealth detention, in the legislative arrangements made after the September 2005 COAG meeting. In an attempt to address Chapter III *Commonwealth Constitution* limitations on detention, the application of preventative detention under the Commonwealth legislation[154] was confined to 48 hours,[155] with reliance then placed upon State and Territory legislation[156] for 14 days of preventative detention. In addition, preventative detention under the *Anti-Terrorism Act (No 2) 2005* (Cth) or under the authority of the individual 14 day State and Territory preventative detention legislation, was drafted to contemplate a high degree of flexibility in shifting of the detainee between various other forms of detention, including ASIO questioning and detention warrants and *Crimes Act 1914* (Cth) arrest powers for *Criminal Code* (Cth) offences.[157]

From this type of experience, it appears timely and advantageous to leverage from the existing terrorism focus to focus on other national security threats and hazards.[158] Of course, that expanded

---

'integrate and coordinate the roles and functions of law enforcement and security intelligence agencies as equal partners in the investigation of terrorism-related activities': at 24.

153 Being Operation Neath and Operation Pendennis: *AFP Report*, above n 152, 24.

154 *Anti-Terrorism Act (No 2) 2005* (Cth).

155 See *Criminal Code* (Cth) s 105.10(5) (initial preventative detention order), s 105.12(5), s 105.14(6) (continued preventative detention order).

156 See *Terrorism (Police Powers) Amendment (Preventative Detention) Act 2005* (NSW); *Terrorism (Preventative Detention) Act 2005* (Qld); *Terrorism (Preventative Detention) Act 2005* (SA); *Terrorism (Preventative Detention) Act 2005* (Tas); *Terrorism (Community Protection)(Amendment) Act 2006 (Vic); Terrorism (Preventative Detention) Act 2005* (WA); *Terrorism (Extraordinary Temporary Powers) Act 2006* (ACT); *Terrorism (Emergency Powers) Act 2003* (NT).

157 On this point see Greg Carne, 'Prevent, Detain, Control and Order?: Legislative Process and Executive Outcomes in Enacting the *Anti-Terrorism Act (No 2) 2005* (Cth) (2007) 10 *Flinders Journal of Law Reform* 17, 65-66 (esp fn 343), 67-71.

158 *Smith Review*, above n 136, 11.

legislative reach will coincidentally correspond to the significantly broadened legal and policy conception of national security.

Another theme is that of integration and community amongst government agencies and activities, advanced as the principal alternative to an organisational merger of intelligence and law enforcement agencies and functions.[159] This approach is clearly compatible with the language of a whole of government and all hazards approaches to national security.[160] As the Smith Review states:

> In building on the existing Australian model, two things are required. First, the departments and agencies concerned, both those dedicated to security functions and those that contribute to national security as well as performing other functions, should be regarded as a community. This is important both to enable the Government to make strategic judgments across a wide range of hazards, including on the allocation of resources, and to ensure that agencies benefit from access to each others skills, experience and other capabilities. Second, the departments and agencies concerned must be well connected and networked, and cultural, technical and other barriers minimized.[161]

To achieve such a community, various proposals affecting different committees and governmental units are then proposed by the Smith Review – examples being broadening the mandate and membership of the Secretaries Committee to embrace the full range of national security issues,[162] and to forge a closer relationship between the

---

159 *National Security Statement*, above n 136, 8.

160 'This aspect is necessarily consistent with a significantly broadened meaning of national security, a 'whole of government approach' and an all hazards approach to national security, the latter meaning 'having agencies well-equipped and ready to detect, deter and/or deal with a crisis or attack on Australia's security of any kind...the threats we face are not the task of one agency, or any one government. Moreover, many of the threats are cross-jurisdictional or transnational in nature...The Government's 'all hazards' approach is not just about government agencies. The success of this approach is also dependent on industry and community involvement': McClelland, above n 139, 2-3.

161 *Smith Review*, above n 136, 10.

162 Ibid 11.

Australian Intelligence Community (AIC) agencies and the intelligence analysis units established within non AIC agencies in response to newly emerging threats.[163] Similarly, the *National Security Information Environment Roadmap*[164] expresses with an exhortatory and reformist zeal, the task of 18 Commonwealth agencies committing themselves to information management reform:

> In many ways, this Roadmap marks a shedding of our legacies and hails a new era of cooperation and sense of community...18 Commonwealth organisations have publicly committed to a journey of change which challenges some outdated notions of information stovepipes, data ownership and protectionist behaviours. I applaud and thank those national security organisations for their courage and willingness to make this public declaration to enter a new era of information sharing to make Australia a safer place.[165]

Of immediate relevance for the present legislation, a key element of the Roadmap is 'a harmonised policy and legislative environment that supports the smooth flow of people, ideas and activities across boundaries'.[166] The Roadmap sets an ambitious agenda to achieve by 2020 a full integration of national security information communication and accessibility. Most striking is the Roadmap's proselytising message of desirability and inevitability of that objective,[167] and the absence of consideration of the significant impact upon privacy and human rights. The present legislation provides a framework to substantially achieve the full integration as contemplated by the *Roadmap.*

The influence of the formative background documents over the content of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) is therefore quite

---

163 *Smith Review*, above n 136, 11.

164 *Roadmap*, above n 136, 9.

165 Ibid 2 (Foreword by National Security Adviser).

166 Ibid 9.

167 See *Roadmap*, above n 136. In the *Roadmap* refer to the comments, 'publicly committed to a journey of change': at 2; 'public commitment ...to enact fundamental change': at 7; 'fulfillment of this vision is unlikely to be the end of the journey': at 9; 'formally committed to the Roadmap and our 2020 Vision': at 12.

significant. However, another major background influence over the enabling format and the functions in the legislation has been the perceived need for Australian intelligence agency leadership and a centralising, co-ordination role being instituted for ASIO. On one level, this leadership development is an institutional increase in status and functions for ASIO, commensurate with the expanded meaning of national security and the migration of those national security practices and values to ordinary aspects of government agency administration.[168] On another level, the integrative nature of the changes as mandated through the ASIO leadership role signal movement towards a high policing model[169] so identified by Brodeur[170] – with its four features of absorbent policing, conflation of separate powers, the protection of national security[171] and the use of informants and technological tools – being clearly evident in the information collection, communication and co-operation and assistance provisions of the present legislation.

This leadership role further means several aspects of reinvention for ASIO. As information exchanges and co-operative arrangements are liberalised and facilitated under the legislation, what were once much more narrowly confined, national security methods of collection and dissemination of information, change in tandem with

---

168 An earlier, similar development of enlargement and reverse migration of functions (from policing and customs and border protection to an intelligence and security agency) is to be found in the enlargement of ASIO's 'security' functions under section 17 of the *ASIO Act 1979* (Cth) to include 'protection of Australia's territorial and border integrity from serious threats'. See definition of 'security': *ASIO Act 1979* (Cth) s 4.

169 In the sense that the policing activity is directed towards and beneficial for, higher interests of the state and government, rather than for those being governed. See Jean-Paul Brodeur, 'High and Low Policing: Remarks about The Policing of Political Activities' (1983) 30 *Social Problems* 507.

170 Jean-Paul Brodeur, 'High and Low Policing in Post 9/11 Times' (2007) 1 *Policing* 25; James Sheptycki, 'High Policing in the Security Control Society' (2007) 1 *Policing* 70.

171 Described by Brodeur as the 'raison d'etre of high policing...In its democratic variant, high policing agencies are tasked to protect the nation's political institutions and constitutional framework. In its nondemocratic variant, high policing is devoted to the preservation of a particular regime that may consist of the hegemony of a political party or the rule of a dictator': Brodeur, above n 170, 27.

the adopted expanded conception of national security. The once specialised, elite character and status of intelligence collection and analysis engaged in by ASIO is altered by this generalisation. This change brings evolutionary opportunities under the legislation able to be seized by ASIO. The status and primacy of ASIO's organisational activities is maintained by it assuming a co-ordinating and gatekeeping role for information, communication and assistance to the AIC and other Federal and State instrumentalities. It places the Organisation in a potentially highly influential position within the Commonwealth bureaucracy and over the development and delivery of public administration and policy. In its centralised *proxy* role in interceptions, information collection and assistance, ASIO can in time exert a significant standardising influence over these arrangements, especially over the non intelligence agencies it interacts with under the present legislation.

This influence will be heightened by the concentration of technical expertise and capacity in intelligence collection methods in the Organisation and in the budgetary imperatives supporting centralising these functions to promote economies of usage. The legislation affords the pivotal co-ordination role for ASIO, and does so within an environment where the national security and counter-terrorism role since 2001 has seen a massive expansion in funding and resources for various agencies.[172] However, such incremental budgetary increases must invariably slow and the capacity for such agencies to service their entire mandate, for example, in the case of the broader law investigation and enforcement functions of the Australian Federal Police, will be placed under stress.

---

[172] See Chris Michaelsen, 'Our Flawed responses to 9/11' *The Canberra Times* (Canberra), 9 September 2011. Over the period 2001-2011, 'ASIO's budget has increased by 655 per cent, the Australian Federal Police budget by 161 per cent, ASIS by 236 per cent and the Office of National Assessments by 441 per cent': at 1. See also Cynthia Banham and Jonathan Pearlman, 'Budget control for federal police could cost them' *Sydney Morning Herald* (Sydney), 25 August 2009: 'The Howard government embarked on a massive expansion of the AFP as part of an increase in counter-terrorism programs after the September 11 attacks. Between 2001 and 2009, the AFP's budget grew from $325 million to $1.48 billion and staff numbers more than doubled to 6265': at 1.

The AFP is presently adjusting to a new budgetary reality in the aftermath of the 2009 Beale Federal Audit of Police Capabilities.[173] Commentary preceding the Beale audit suggested that the AFP's counter-terrorism operations focus had been to the detriment of the investigation of major crime, including fewer referrals of serious crimes from the AFP to the Commonwealth DPP.[174] Two budgetary features relevant to present analysis are now impacting upon AFP operations. First, there has been a slowing 'in the growth of agency expenditure since 2007-2008',[175] reflecting the fact that in prior years' expenditures from 2002-2006, 'around half of the new funding has been directed to transforming AFP operational capability, including in the areas of national security and serious crime.'[176] Second, there has a clear movement away from budgetary allocations to the AFP for quite specific tasks:

> The government's acceptance of the budget related recommendations from the Beale review has restructured the AFP's budget funding so that, in 2010-11, 65 per cent of our funding is now base funding compared to 27 per cent in 2009-10. This has allowed us to consolidate the AFP's national capabilities around three core operational programs. Firstly, security and protection; secondly, international deployments; and thirdly, serious crime.[177]

The increase in AFP budgetary discretion and budgetary control has brought with it increased institutional accountability over the performance of programs outside of counter-terrorism mandate. This creation of internal budgetary pressures within the AFP will

---

173 Conducted by former senior public servant Roger Beale AO, from the Allen Consulting Group. See Paul Maley, 'Federal audit for AFP' *The Australian* (Sydney), 29 January 2009.

174 Maley, above n 173.

175 Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Examination of the Australian Federal Police Annual Report 2009-2010* (2011) (*PJCLE Report*), para 2.5.

176 Ibid para 2.4. See also Banham and Pearlman, above n 172, 'According to a report by the Australian Strategic Policy Institute, the bulk of counter-terrorism funding since 2001 has been directed towards 'capacity building' – such as new equipment and additional police training': at 1.

177 AFP Commissioner Tony Negus cited in *PJCLE Report*, above n 175, para 2.6.

ultimately affect how, for example, the AFP avails itself of the information sharing, co-operation and communication arrangements mandated by the present legislation and the influence ASIO is able to wield in negotiating that relationship within its legislated parameters.

There has also been a deliberate inclusion within revised national security arrangements, of quite specific new policy or program functions, integrated with the present legislation's operation, so as to enable and enhance the new ASIO leadership function in its dealings with relevant agencies. The first example is in the establishment of a Counter-Terrorism Control Centre,[178] within ASIO itself and facilitative of the integrated arrangements between agencies as discussed in analysing the legislation:

> It will improve coordination across government agencies in counter-terrorism intelligence, decision making and operations. This centre will bring together senior officials – experts from Australia's key intelligence and law enforcement agencies. It will drive a fully integrated national approach to counter-terrorism by identifying specific counter-terrorism priorities and developing a stronger fusion of the intelligence and law enforcement community effort.[179]

> [It] will set and manage counter-terrorism priorities, identify intelligence requirements, and ensure that the processes of collecting and distributing counter-terrorism information are fully harmonized and effective across the spectrum of Australia's counter-terrorism activity.[180]

---

178 See Robert McClelland, 'Opening of counter-terrorism control centre' (Prime Minister and Attorney-General Joint Media Release 21 October 2010) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2010/Fourthquarter/21October2010Openingofthecounterterrorismcontrolcentre.aspx> at 1 December 2011; Robert McClelland, 'Launch of the Counter Terrorism Control Centre Australian Security Intelligence Organisation' (Speech delivered at Canberra 21 October 2011) <http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/Speeches_2010_21October2010-launchofthe CounterTerrorismControlCentre-AustralianSecurityIntelligenceOrganisation> at 1 December 2011.

179 Commonwealth, *Parliamentary Debates*, House of Representatives, 23 February 2010, 1498 (Robert McClelland).

180 *Counter-Terrorism White Paper*, above n 136, 28.

> The Centre will, of course, be hosted by ASIO with representatives from Australia's key security, intelligence and law enforcement agencies including the Australian Security Intelligence Organisation, the Australian Federal Police, the Australian Secret Intelligence Service and the Defence Signals Directorate. Each of these representatives will have the ability to reach back into their own organisations to call on expertise and marshal capability if, and when, action is required.[181]

A second example surrounds the present legislation's function of ASIO providing technical assistance and intercepting on behalf of other agencies, practically implemented through a dedicated interceptions centre:

> ASIO has a lead agency role to provide technical advice relating to telecommunications interception to all interception agencies. The National Interception Technical Assistance Centre (NITAC) pilot program commenced on 1 July 2010 and is intended to operate for two years. With the assistance from the AFP, ASIO will provide coordinated technical assistance to other Australian interception agencies by providing a central point of reference from which agencies can receive technical assistance to help keep pace with technical change.[182]

The idea is that the rapidity of technological change and development necessitates and justifies a centralisation of expertise and co-ordination of response amongst agencies with interception powers. What is perhaps more illuminating regarding the present legislation's introduction is the executive centric assumption in government documentation that the then bill would be passed, enabling the programs planned and budgeted for in the pilot program to be activated, and with a preliminary budgetary allocation justifying the far reaching, enabling legislative changes:

> While some of the measures intended by the NITAC program are able to operate under current legislation, the proposed amendments

---

[181] McClelland, 'Launch of the Counter Terrorism Control Centre Australian Security Intelligence Organisation', above n 178, 4.

[182] Attorney-General's Department, above n 57, 4. See also McClelland, above n 145, 4.

> in the Bill will ensure the pilot is able to fully function in the remainder of the two year period.[183]
>
> During the budget process you might remember we had renewal of funding in the TI area. As part of that, we found a way of looking after future technological challenges by establishing a process whereby ASIO would be able to provide assistance on a pilot basis to two law enforcement agencies – the Crime Commission and the ACLEI, the anticorruption body. That was part and parcel of our budget strategy. We felt that without these cooperative amendments in the TI area, we would not be able to use that pilot to its full potential...We can do some aspects of it but, to do the pilot in the way the whole thing is intended, yes (i.e. the bill needs to be passed to do the pilot).[184]

There is a clear expectation from the Attorney General's department representative that the parliamentary process will accommodate itself to executive convenience, including a truncated legislative process curtailing opportunities for detailed scrutiny of legislation, and the legislation affecting significant change in the scope of information accessible to the agencies concerned in the performance of their functions.

XIII THE EVOLUTION OF TERRORISM LAW REFORM CHARACTERISTICS TO REFORM OF NATIONAL SECURITY COMMUNICATION, ASSISTANCE AND CO-OPERATION

As the model of terrorism law and policy reform since September 2001 has provided a foundation for concepts and practices now reflected in the national security communication, co-operation and assistance reforms of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth), it is

---

183 Attorney-General's Department, above n 57, 4.

184 Evidence to Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, Canberra, *Committee Hansard,* 11 November 2010, 23 (Mr McDonald).

important to consider that some identifiable features from that earlier phase have evolved to be both influential and transformative in that reform. The present legislation signals a new phase in the adaptation and evolution of counter terrorism law developments and practices to broader national security applications.

Several characteristics can be identified which provide context and assist in comprehending the directions and implications of the current legislation – and the government's stated objectives for the legislation of information communication, co-operation and assistance.

XIV THE NORMALISATION OF LEGISLATIVE EXCEPTIONALITY

A clearly emergent factor after ten years of terrorism law and policy reform has been the tendency of previously perceived extraordinary and exceptional measures becoming part of a permanent, established legal landscape, within which those measures become normalised.

One clear trend reflected in the legislation's potential deployment of national security technical resources, and co-operation and assistance for broader government agency purposes, is the normalisation and mainstreaming of what once would have been extraordinary powers. In relation to the development of terrorism powers, several characteristics of this phenomenon have been identified.[185]

[185] Various academic commentators have written on the process and characteristics of normalisation of once extraordinary powers in terrorism law.

First, the principles of exceptionality and normalisation are generally recognised.[186] In the alternative, some practices 'have their origins in existing practices operating in many Western domestic criminal justice systems'.[187] There is a strong pre-emptive and preventative aspect,[188] considered by some to be derived from the precautionary principle[189] as applied in other areas of law. A marked tendency has emerged to enact more and more law – either as 'temporary measures become permanent and political pressure to be hard on terror leads more and more law'[190] or a cycle of new laws follows in the wake of new terrorist attacks.[191] In addition, the migration of national security practices into mainstream government administration is identifiable by various synonyms.[192]

---

186 See especially Jenny Hocking and Colleen Lewis, 'Counter-terrorism and the rise of 'security policing' in Jenny Hocking and Colleen Lewis (eds), *Counter Terrorism and the Post Democratic State* (2007) 148; Neil Hicks, 'The Impact of Counter-Terror on the Promotion and Protection of Human Rights: A Global Perspective' in Richard Ashby Wilson (ed), *Human Rights in the War on Terror* (2005) 221; Simon Bronitt, 'Balancing Security and Liberty: Critical Perspectives on Terrorism Law Reform' in Miriam Gani and Penelope Mathew (eds), *Fresh Perspectives on the 'War on Terror'* (2008), 82; Benjamin J Goold and Liora Lazarus, 'Introduction: Security and Human Rights: The Search for a Language of Reconciliation' in Benjamin J Goold and Liora Lazarus (eds), *Security and Human Rights* (2007), 4.

187 David Brown and Janice Gray, ''Devils and dust': extending the 'uncivil politics of law and order' to the 'war on terror'' in Jenny Hocking and Colleen Lewis (eds), *Counter Terrorism and the Post Democratic State* (2007) 154.

188 See David Dyzenhaus and Rayner Thwaites, 'Legality and Emergency – The Judiciary in a Time of Terror' in Andrew Lynch, Edwina MacDonald and George Williams (eds), *Law and Liberty In The War On Terror* (2007) 17; Goold and Lazarus, above n 186, 5.

189 See Bronitt, above n 186, 78, citing Goldsmith.

190 Gani and Mathew, above n 186, 4.

191 Andrew Lynch and George Williams, *What Price Security? Taking Stock of Australia's Anti-Terror Laws* (2006), 7.

192 'Synonyms for this phenomenon include 'seepage', 'migration', 'colonising', 'modelling', 'bleeding' and 'snowballing', describing the expansion of national security subject matter, methodologies and techniques into other regulatory environments: see Greg Carne, 'Remedying the Past or Losing International Human Rights in Translation? – 'Comprehensive' Responses to Australian National Security Legislation Reviews' (2009) 13 *University of Western Sydney Law Review* 37, 49 fn 52.

This experience from the example of terrorism law is relevant to the present national security based legislation. That legislation effectively extends the model of normalisation and mainstreaming of powers developed from the example of terrorism, draws upon broader concepts of national security, as previously discussed, and applies that model to flexible and potentially exponential administrative circumstances. A legislative evolution has occurred in the acceptance and normalisation of the exceptional, with a *migration of that exceptionality* to the very broadly defined circumstances of co-operation and assistance by intelligence agencies. The enactment of this legislation has been eased by security issues emerging in recent times as a primary political preoccupation of the state – as expressed, 'the legitimacy of late modern states has become increasingly bound up with their role as guarantor of security and within a politics of security'.[193]

As such, the present legislation breaks down longstanding legal assumptions about the separation of extraordinary national security powers from everyday legislation and policy implementation. Within its technical assistance,[194] other assistance, communication and co-operation provisions,[195] there is a framework for discretionary, selective inclusion and expansion of national security activity[196] into ordinary State and Commonwealth agency activity. This normalisation is best indicated in the facilitatory and discretionary characteristics of the legislation,[197] and that express and rigorous safeguards, ordinarily marking out exceptionality, are absent. The loose structure and approval processes within the legislation[198] likewise encourage practices conducive of such normalisation.

---

193 Goold and Lazarus, above n 186, 5-6.

194 See *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) Schedule 1 – Exercise of warrant powers.

195 See *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) Schedule 6 – Co-operation, assistance and communication between intelligence agencies.

196 In particular, see *ASIO Act 1979* (Cth) s 19A(1), (2); *Intelligence Services Act 2001* (Cth) s 13A(1), (2).

197 *ASIO Act 1979* (Cth) s 19A(1)-(2); *Intelligence Services Act 2001* (Cth) s 13A(1)-(2).

198 See, eg, *ASIO Act 1979* (Cth) s 18(3)(b)(ii), s 19A(2)(a)-(b).

XV THE WEAKNESS OF SAFEGUARDS IN SHIFTING TO THE NEW PARADIGM

Given the broadened conception of national security underpinning the legislation and the legislation's facilitation of national security expertise and resources being used for a variety of agency purposes, there is a relative weakness, even tokenism, in the safeguards purported to be provided by the present legislation. This is not surprising as the quintessential character of the legislation is to break down the hitherto important separation between national security powers and activities and ordinary government administration.[199] A parallel introduction within the legislation of substantive checks and balances upon what agencies may do in relation to communication, co-operation and assistance, would therefore be contradictory. Such checks and balances as exist in the legislation derive from existing concepts – the making of ministerial guidelines under existing powers in the *ASIO Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth) and in the discretions integrated into the legislation.[200] Such executive discretionary capacity has oddly in the past, in relation to terrorism legislation, been advanced as a safeguard.[201] It

---

199 This is the practical, as distinct from the legal technical, import of the legislation. The Government's approach has been to deny that the distinction between national security and law enforcement has been has been dismantled: Attorney-General's Department, above n 57, 11-12. The complex drafting of the legislation, as discussed under the heading 'Assistance to law enforcement and interception agencies with telecommunications interception', above, reflects an attempt to maintain that legal textual distinction.

200 See, eg, the *ASIO Act 1979* (Cth) s 19A(4)A, allowing that the Director General of ASIO or a person acting within the limits of authority conferred on the person by the Director General 'may communicate information to a staff member of a (law enforcement agency or an authority of the Commonwealth, or an authority of a State) prescribed by regulations...(a) if the information has come into possession of the Organisation in the course of performing the Organisation's functions under section 17; and (b) the information is communicated for the purposes of co-operating with or assisting the body under this section'.

201 'What was striking was that the executive discretions conferred...were actually advanced as a safeguard. The ambit of such discretion was inverted to be presented as a positive, requiring an investment of trust by the public in the executive and an emphasis upon the integrity of those entrusted with that

is possible to see the sanguine dismissal by the Attorney General's department of the need for new ministerial guidelines,[202] as confirming this unconventional view of executive discretion.

The government's further response contemporaneous with the legislation has been to mention legislative enactments establishing an Independent National Security Legislation Monitor,[203] reforms concerned with two Parliamentary Committees involved in review of national security activity[204] and reforms to the function of the

---

executive based discretion': Carne, 'Hasten Slowly: Urgency, Discretion and Review – A Counter-Terrorism Legislative Agenda and Legacy', above n 4, 86. The scope of ASIO discretionary powers has long been considered as extensive: see Joo Cheong Tham, 'ASIO and the rule of law' (2002) 27 *Alternative Law Journal* 216, 217-218. Discretion as a safeguard has also been linked to the integrity and capacity of current key office bearers exercising the discretion: see Carne, above n 157, 74.

202 See Attorney-General's Department, above n 57, 2: 'Active consideration has been given to privacy issues in the development of this Bill, including whether the existing Attorney-General's Guidelines and Privacy Rules remain appropriate. In light of the existing privacy regimes, the Attorney-General's Department is of the view that additional privacy frameworks or MOUs do not appear to be necessary': at 2.

203 See *Independent National Security Legislation Monitor Act 2010* (Cth); Wayne Swan, 'Appointment of the Independent National Security Legislation Monitor' (Deputy Prime Minister and Treasurer Media Release 21 April 2011) <http://www.treasurer.gov.au/DisplayDocs.aspx?doc=pressreleases/2011/036.htm&pageID=&min=wms&Year=&DocType=0> at 1 December 2011; Andrew Lynch and Nicola McGarrity, 'A 'watch dog' of Australia's counter-terrorism laws: the coming of the national security legislation monitor' (2010) 12 *Flinders Law Journal* 63.

204 See Commonwealth, *Parliamentary Debates* House of Representatives 23 March 2011, 2861 (Robert McClelland): 'Members would recall that amendments to increase the size of the Parliamentary Joint Committee on Intelligence and Security were recently passed as part of the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010'. Increasing the Committee to 11 members, 5 of whom must be Senators and 6 of whom must be members of the House of Representatives: *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) Schedule 8. The second committee reform was the establishment of the Parliamentary Joint Committee on Law Enforcement: see *Parliamentary Joint Committee on Law Enforcement Act 2010* (Cth).

Inspector General of Intelligence and Security.[205] While these are positive developments, the legislation presents such dimensional and paradigmatic shifts in national security based executive power, that such relatively modest and general reforms do not specifically address the extent of the change, or provide an accountability framework commensurate with that change.

The problematic issue of accountability mechanisms in legislation is of course, a continuing theme in relation to terrorism legislation. That experience can again be seen as formative and influential over the present legislation, in the persistent, unresolved question of ensuring that the legislated objective of security is methodologically aligned in the legislation with liberal democratic values.

In the context of terrorism legislation, commentators have identified points logically critical to alignment with liberal democratic values. Security measures are justifiable in support of a liberal constitution,[206] constrained by the principles of proportionality and necessity.[207] As such, human rights and security must be complementary concepts, particularly in countering the development of precursor conditions to terrorism.[208] In achieving a reconciliation of security and human rights, a fixation on legislating for the worst possible situations will fail to achieve rule of law values.[209] In the Australian terrorism law context, the absence of a

---

[205] See Commonwealth, *Parliamentary Debates* House of Representatives, 23 March 2011, 2861 (Robert McClelland): 'The mandate of the Inspector General of Intelligence and Security was recently expanded in the National Security Legislation Amendment Act 2010, so that the Inspector General can extend inquiries outside the intelligence community in appropriate cases'. See *National Security Legislation Amendment Act 2010* (Cth) s 9 sch 8, 'Additional inquiry functions of Inspector General', allowing Prime Ministerial requests to the Inspector General to 'inquire into an intelligence or security matter relating to a Commonwealth agency'.

[206] Fernando Teson, 'Liberal Security' in Richard Ashby Wilson (ed), *Human Rights in the War on Terror* (2005), 58-59.

[207] Ibid 75.

[208] Hicks, above n 186, 221-222.

[209] Goold and Lazarus, above n 186, 12.

federal charter of rights has been seen as problematic in that basic legal principles and values do not necessarily inform the development and scrutiny of such laws.[210]

In the instance of terrorism law, the failure to adopt a consistent legislative drafting and review methodology deliberately integrating human rights principles into legislative formation,[211] may partly explain the ease in arriving at the present legislation's percolation of national security activity into the functions of Commonwealth and State instrumentalities. In time, the enactment and scrutiny of a legislative compatibility statement assessing compatibility with Australia's key international human rights treaty obligations[212] might well change the legislative equation if the issue re-emerges.

---

210 Lynch and Williams, above n 191, 91-92; Brown and Gray, above n 187, 155. See also Sarah Sorial, 'The Use and Abuse of Power and Why We Need A Bill Of Rights: *The ASIO (Terrorism) Amendment Act 2003* (Cth) and the Case of *R v Ul-Haque*' (2008) 34 *Monash University Law Review* 400; Angela Ward, 'Checks, Balances' (2005) 68 *Precedent* 12; John Von Doussa, 'Reconciling Human Rights and Counter-Terrorism – A Crucial Challenge' (2006) 13 *James Cook University Law Review* 104, 120-123. Of course, this point is likely to change with the enactment of the *Human Rights (Parliamentary Scrutiny) Bill 2010* (Cth) and the *Human Rights (Parliamentary Scrutiny) (Consequential Provisions) Bill 2010* (Cth). For a contrary view about the efficacy of a charter of rights in reining in terrorism law reform excesses, see Keith Ewing, 'The futility of the Human Rights Act' (2004) *Public Law* 829; Joo Cheong Tham and Keith Ewing 'Limitations Of A Charter Of Rights In The Age Of Counter Terrorism' (2007) 31 *Melbourne University Law Review* 46; Keith Ewing and Joo-Cheong Tham 'The Continuing Futility of the Human Rights Act' (2008) *Public Law* 668.

211 See Carne, above n 192, 49-53, 79-81.

212 See 'Statements of compatibility in relation to Bills' in the *Human Rights (Parliamentary Scrutiny) Bill 2010* (Cth) s 8. Section 3 of the bill defines human rights as meaning the rights and freedoms recognised and declared by the CERD, ICESCR, ICCPR, CEDAW, CAT, CROC and CRPD.

XVI EXECUTIVE POWER AND DISCRETION AND THE ASCENDANCY OF SECURITY VALUES

Closely allied to a broadened concept of national security underpinning the legislation's facilitation of national security technical assistance, communication and co-operation to a range of Commonwealth and State instrumentalities, the securitisation of potentially many government agency activities, raises significant questions of the ongoing concentration of executive power and its transformative effects upon democracy.[213] The ascendancy of security values and practices that the legislation facilitates over ordinary government administration is something that was insufficiently highlighted in the legislation's introduction and debate. This ascendancy will reinvigorate the concentration of executive power, and a re-constitution of democracy, which was previously mediated through counter-terrorism law reform.[214]

Importantly, and emerging from the previously discussed national security leadership role of ASIO, the legislation's impact will be to increase the status and influence of intelligence agencies in general public administration and policy development.[215] In other

---

[213] In relation to an earlier emergence of an executive concentration through the enactment of counter-terrorism laws, see Duncan Kerr, 'Australia's Legislative Response to Terrorism Strengthening arbitrary executive power at the expense of the rule of law' (2004) 29 *Alternative Law Journal* 131; Jenny Hocking, 'Protecting Democracy by Preserving Justice: 'Even For The Feared and the Hated'' (2004) 27 *University of New South Wales Law Journal* 319, 322, 323, 337; Jenny Hocking, 'Counter-Terrorism and the Criminalisation of Politics: Australia's New Security Powers of Detention, Proscription and Control' (2003) 49 *Australian Journal of Politics and History* 355; Carne, above n 157, 65-75.

[214] See Robert Cornall, 'Keeping Our Balance in Troubled Times: Legal Measures, Freedoms and Terrorist Challenges' (2005) *Defender* 28, 30-31; Robert Cornall, 'Global Security in the New Millenium: The View from the Attorney-General's Department' (2003) *Canberra Bulletin of Public Administration* 66, 68-69.

[215] A point observed in that ASIO 'has grown over the past decade into one of the most powerful bodies in the land – its staff numbers trebled, its budget increased more than sixfold to $438 Million per year': Neighbour, above n 1, 28.

words, the reference and contact points of intelligence agency participation for ordinary administration and policy will expand, reflective of the stated whole of government approach to national security issues.

As the work of intelligence agencies is not amenable to ordinary methods of review, the enlarged national security role in the legislation is inherently problematic for accountability of Commonwealth and State agency activity and roles, and the capacity of public deliberation to influence political debate and ensure accountability in relation to such activity and roles. The direct interface through communication, co-operation and assistance between intelligence agencies and government agencies promises significant re-alignment about the processes of policy formation, program administration and democratic participation and accountability, and an unidentified intelligence agency influence over such public activity.

These likely further concentrations of executive power from the legislation, in turn can be seen as an evolution of the executive power concentration arising from the enactment of terrorism legislation. This phenomenon has been variously described - the width of laws resulting in executive overreach,[216] the rise of unchecked executive power directly affecting domestic human rights conditions,[217] the increasing use of pre-emptive measures challenging the viability of liberal and established legal norms,[218] the expansion of state power responding to political appeals for security[219] and a continuing conflict between rights and security as producing longstanding and potentially disturbing structural changes taking place in society.[220] The continuing prominence of security as a political issue provides an environment receptive to new iterations

---

216 Andrew Lynch, 'Achieving Security, Respecting Rights and Maintaining the Rule of Law' in Andrew Lynch, Edwina MacDonald and George Williams (eds), *Law and Liberty In The War On Terror* (2007), 231.

217 Hicks, above n 186, 216.

218 Bronitt, above n 186, 82.

219 Goold and Lazarus, above n 186, 6.

220 Ibid 9.

of expanded executive power available under the current legislation, with a potential political dividend for invoking that claim of protection and pre-emption.

XVII DEFICIENCIES IN LEGISLATIVE PROCESS AND LEGISLATIVE REVIEW

The method and circumstances of the enactment of the legislation also raise a further issue emerging from the terrorism legislation experience, namely the inadequacy of parliamentary review processes, here reflected in the report of the Senate Legal and Constitutional Affairs Legislation Committee.[221] Such inadequacies should be seen within the context of some earlier observations on the serial legislating with urgency methodology of the Howard government.[222] Commentators have also identified various adverse legislative process factors from the experience of Australian terrorism law enactment.[223] Such experiences highlighted potential future risks in broader national security legislative enactment.

Some obvious criticisms of the Senate Legal and Constitutional Affairs Legislation Committee report are its basic and uncritical methodology, represented by its collation of the views of non

---

221 *Senate 2010 Report*, above n 32.

222 See the discussion above under the heading 'The historical context of the legislation – transition, change and continuity from the Howard government'.

223 See Hocking and Lewis, above n 186, 141: 'Deficient parliamentary process at the crucial formulation stage of the policy process, accompanied as it was by the winding back of fundamental democratic safeguards, resulted in an extraordinary expansion of police power in relation to counter-terrorism. Despite the significance of the legislation, there was little if any opportunity for dissemination, debate or community interaction'; Lynch and Williams, above n 191, 86, 88-89, describing 'reactive law making', a 'cycle of new laws' and 'poor process'; Gani and Mathew, above n 186, 4: 'Precipitous and reflexive passage of anti-terrorism laws in the wake of 9/11 in multiple jurisdictions'; Bronitt, above n 186, 76, questioning the efficacy of subsequently mandated legislative review.

government opposition and government support[224] of multiple aspects of the legislation, and its failure to critically appreciate potential implications for Australian democracy flowing from the securitisation of ordinary public administration through the interception, co-operation and assistance measures. In particular, its failure to provide a range of recommendations[225] for legislative amendment, including safeguards and review, commensurate with that transformatory securitisation, is striking. Given the complexity of the legislation and its potential far reaching consequences, the Committee process was not aided by the relatively brief time available for submissions,[226] and the fact that the Committee allocated less than three hours to public hearings in Canberra.[227]

Perhaps of greater significance was the wholly inadequate submission by the Australian Privacy Commissioner.[228] As the lead agency for privacy protection in Australia, the submission failed to grasp the profound implications of the legislation. In providing a routine summary of existing legislative coverage in relation to national security and telecommunications interception matters, it observed that intelligence agencies were not covered by the *Privacy Act 1988* (Cth).[229] It noted that other regulatory arrangements existed for intelligence agencies,[230] advocated possible review of the Attorney General's Guidelines for ASIO[231] (in response to telecommunications interception warrant powers) and 'that an appropriate privacy framework be put in place to support the information sharing arrangements set out in Schedule 6 of the

---

224 This is the methodology adopted, *inter alia*, in Chapter 3 'Key Issues': *Senate 2010 Report*, above n 32, 17.

225 The Report provides only 3 recommendations: see *Senate 2010 Report*, above n 32, ix.

226 The Senate Legal and Constitutional Affairs Legislation Committee advertised the inquiry on 13 October 2010, inviting submissions by 27 October 2010: *Senate 2010 Report*, above n 32, 3.

227 Ibid Appendix 2.

228 *Information Commissioner submission*, above n 56. This Privacy Commissioner submission was made under the auspices of its parent organisation, the Office of the Information Commissioner.

229 Ibid 13, 6-7.

230 Namely *Intelligence Services Act 2001* (Cth) s 15; *ASIO Act 1979* (Cth) s 8A.

231 *Information Commissioner submission*, above n 56, 8.

bill.'[232] It attached a very general proposed 'framework for assessing and implementing new law enforcement and national security powers,'[233] otherwise described as the '4A framework'.[234] The failure of the 'Privacy Commissioner to provide 'a much more rigorous, vigorous and critical review of the proposed amendments',[235] prompted the Australian Privacy Foundation to make a supplementary submission to the Senate Committee Inquiry.[236]

Strikingly, the recommendations of the Committee are so minimalist that they fail to respond to the concerns advanced in important key submissions.[237] Indeed the recommendations by the Committee suggest a complacency, as if the amendments sought were of a minor or technical nature, a tactical description previously used in elsewhere to facilitate swift and uncontroversial passage of far reaching terrorism legislation. Alternatively, the recommendations suggest a Committee hamstrung by the self-

---

232 *Information Commissioner submission,* above n 56, 15.

233 Ibid 16, Attachment A: Framework for assessing and implementing new law enforcement and national security powers.

234 *Information Commissioner submission,* above n 56, 5.

235 Australian Privacy Foundation, Submission to Senate Legal and Constitutional Affairs Legislation Committee Inquiry into Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 [Provisions] Parliament of Australia, Canberra 2010 (*Australian Privacy Foundation Supplementary Submission*), 1: 'The Public's Reasonable Expectations of the OAIC'.

236 Ibid 1: 'We had expected the Privacy Commissioner to provide a much more rigorous, vigorous and critical review of the proposed amendments...the 4A framework ...appears to have been put forward far too late and far too timidly...the framework would only be valuable if the Privacy Commissioner applied it and made a judgment about whether the proposed amendments are 'necessary and proportionate'. By failing to provide the Committee with an independent assessment, the OAIC is failing to perform its statutory functions...'

237 Namely those of the *Australian Privacy Foundation submission,* above n 28; *Castan Centre submission,* above n 42; Law Council of Australia, Submission No 4 to Senate Legal and Constitutional Legislation Committee Inquiry into *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 [Provisions]* Parliament of Australia, 28 October 2010 (*Law Council of Australia submission*).

imposed limitations of its inquiry and perhaps through political expediency, unable to formulate adequate ideas shaped by expert opinion and an informed appreciation of relevant issues arising from the counter-terrorism legislative experience.

XVIII A RENEWED INTERNAL LEGISLATIVE CAPACITY FOR FURTHER EXPANSION AND CHANGE

A further common issue following the enactment of Australian terrorism legislation has been a subsequent constant review of that legislation. In particular, this was reflected in the multiplicity of enactments and some deliberately adaptable statutory phrases and offences.[238] The terrorism and national security legislative environment has also seen a readiness to incrementally liberalise intelligence agency power through amendments.

The present legislation internally engineers a capacity for incremental expansion and change in additional ways. The first is a range of porous terms of critical import.[239] A second is that certain sections of the legislation allow very broad discretions to agency heads to make requests for assistance and co-operation,[240] and for ministers to make arrangements or give directions to condition that

---

[238] An example is the definition of 'terrorist act' in section 100.1 of the *Criminal Code* (Cth), which forms the basis of terrorism act offences (Division 101), the proscription of terrorist organisations (Division 102), control orders (Division 104) and preventative detention (Division 105) of the *Criminal Code* (Cth).

[239] These terms include 'law enforcement agency': *ASIO Act 1979* (Cth) s 4; 'serious crime': *ASIO Act 1979* (Cth) s 4; 'Information relates or appears to relate, to the performance of the functions, responsibilities or duties of Ministers, Commonwealth authorities and State authorities' *ASIO Act 1979* (Cth) s 18(3)(c) and 18(4); 'national interest' *ASIO Act 1979* (Cth) s 18(3)(b)(i), (ii).

[240] *ASIO Act 1979* (Cth) s 19A(2)(b); *Intelligence Services Act 2001* (Cth) s 13A(2)(b).

co-operation and assistance.[241] This broad discretion is instead of a series of prescribed, graduated criteria that would need to be satisfied to invoke requests for assistance and co-operation, and then trigger, under legislation, separate review mechanisms and controls. Furthermore, the legislation's facilitation of communication and assistance through these ample discretions is likely to encourage institutional participants to reach arrangements of mutual convenience and reciprocity of interest. In addition, the budgetary allocation for pilot purposes with selected agencies,[242] which created an urgent expectation that the legislation would be passed, may generate conclusions that further amendments authorising assistance and co-operation are required.

XIX CONCLUSION

The enactment of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) brings significant change to the framework of Australian national security policy and administration, with its liberal enabling framework for agency communication, co-operation and assistance and its capacity to produce the securitisation of many aspects of Commonwealth and State instrumentality activity.

The legislation marks a clear transition from the dominance of terrorism as the legislative focus of the Howard government years and the practice of serial and multiple legislative enactments on that topic. However, in doing so, it builds upon aspects of the terrorism law experience and establishes a framework for the continuity of accretions of executive power and for the normalisation and mainstreaming of many exceptional powers under a broadly developed conception of national security. These developments

---

241 *ASIO Act 1979* (Cth) s 19A(2)(a); *Intelligence Services Act 2001* (Cth) s 13A(2)(a).

242 See discussion under the heading above 'Additional influences over the formation of the legislation'.

potentially touch upon many aspects of Commonwealth and State administrative activity.

In that sense, the legislation reinstates change as a constant, in a broader national security aspect, but adopts a set of expansive discretionary powers within this legislation to achieve this, rather than reverting to a model (at least so far) of serial legislative enactments. It confirms that the national security legislative programs of the Howard and the Rudd/Gillard governments share a trend of increasing executive power and discretion and the raising of security values and practices to a incrementally prominent role in many aspects of government administration. This trend is further consolidated by subsequent enactment of the *Intelligence Services Legislation Amendment Act 2011* (Cth).[243] The liberalisation of both what constitutes national security or related information and its potential transmission and utilisation for both security and non security purposes is engineered and facilitated by these legislative changes, which have evolved from the genesis of legislative responses to terrorism, challenging long assumed freedoms and creating a susceptibility to authoritarian state principles.[244]

---

[243] See the discussion of this further enactment under the heading above, 'Enhancing the communication and sharing of information between agencies and authorities'. Principal other relevant features of this Act provide DIGO with a general function of providing support and assistance to the ADF, and a new ground relating to breach of UN sanctions for Ministerial authorisation for the production of intelligence on an Australian person. See Robert McClelland, 'National security legislation passes Parliament' (Attorney-General's Media Release, 5 July 2011) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2011/Thirdquarter/5July2011NationalsecuritylegislationpassesParliament.aspx> at 1 December 2011.

[244] For early argument about the use of anti-terrorism laws trending towards the creation of an authoritarian state, see Emerton, above n 4; Michael Head, 'Counter-terrorism laws: a threat to political freedom, civil liberties and constitutional rights' (2002) 26 *Melbourne University Law Review* 666; Michael Head 'Orwell's Nineteen Eighty-Four 20 years on: ''The war on terrorism' 'doublethink' and 'Big Brother'' (2005) 30 *Alternative Law Journal* 208.

Perhaps more remarkable is the lack of publicity and the relatively uncontroversial circumstances surrounding the passage of the legislation. These factors unfortunately point to an ignorance amongst legislators and others that the legislation's technical provisions contest and re-shape checks and balances founded upon democratic assumptions of the desirability of containing and segregating exceptional national security powers to limited and clearly defined circumstances. In transitioning from those assumptions under the guidance of several influential national security documents and in extrapolating from, and enlarging the experience of liberalised practices and powers under a cache of terrorism laws, the facilitative powers in the present legislation pose significant questions for the operating principles of Australian democracy. This is because the changes provide security and intelligence agencies with a significantly enhanced influence or contribution, through communication, co-operation and assistance, into Commonwealth and State administration. Largely by a legislative process of ignorance, default, omission and elision, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) signals a strong move towards a more authoritative state, with the infusion and integration of national security information, co-operation and assistance as increasingly influential in the ordinary business and functions of both Commonwealth and State government.