



THE UNIVERSITY OF
NEW SOUTH WALES



FACULTY OF LAW

GILBERT + TOBIN CENTRE
OF PUBLIC LAW

31 July 2014

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

Dear Secretary

Inquiry into the National Security Legislation Amendment Bill (No 1) 2014

Thank you for the opportunity to make a submission to this inquiry. We do so in our capacity as members of the Gilbert + Tobin Centre of Public Law at the Faculty of Law, University of New South Wales. We are solely responsible for the views and content in this submission.

Many of the reforms contained in the National Security Legislation Amendment Bill (No 1) 2014 ('the Bill') are welcome. The Bill aims to modernise the law to reflect developments in communications technology, to streamline the processes for intelligence agencies to apply for various types of warrants and also to provide some clarification as to the scope of the powers that these agencies possess.

We have had insufficient time to prepare detailed submissions on each and every aspect of the Bill. It totals more than 120 pages and purports to implement – amongst other important matters – about 20 recommendations of the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') in its 2013 Inquiry into Potential Reforms of Australia's National Security Legislation ('2013 Inquiry'). However, in spite of this complexity, the Committee has been granted only two months from the date that the Bill was introduced into the

SYDNEY 2052 AUSTRALIA
Telephone: +61 (2) 9385 9654
Facsimile: +61 (2) 9385 1175
www.gtcentre.unsw.edu.au

Commonwealth Parliament to table its report. It has therefore been necessary for the period for public submissions to be limited to less than three weeks.

In light of this, our submission concentrates on four areas of the Bill about which we have particular concerns. These are:

1. Amending the provisions with respect to computer access warrants (Schedule 2).
2. Establishing a special intelligence operations regime (Schedule 3).
3. Changing the rules under which the Australian Security Intelligence Service ('ASIS') may cooperate with the Australian Security Intelligence Organisation ('ASIO') in the performance of its functions (Schedule 5).
4. Creating new disclosure offences for ASIO employees and contractors and increasing the maximum penalties for the existing offences (Schedule 6).

There is a need, in the intelligence context, to maintain a strong accountability framework so as to ensure that corruption and abuses of power do not occur (or are at least can be detected and minimised). Our concerns about the Bill are driven by a perception that it will adversely affect this framework by establishing vague and unduly broad criteria for the issue of a warrant, internalising the process for authorising intelligence-gathering activities and cloaking these activities in even greater secrecy than that which they have historically enjoyed.

1. Amending the provisions with respect to computer access warrants (Schedule 2)

a. The definition of a 'computer'

Currently, s 25A of the *Australian Security Intelligence Organisation Act 1979* (Cth) ('ASIO Act') empowers the Commonwealth Attorney-General to issue a computer access warrant when requested by the Director-General of Security. A warrant may be issued if the Minister is satisfied that there are reasonable grounds for believing that access to data 'held in a particular computer' would substantially assist in the collection of intelligence that is important in relation to security. ASIO officers may then undertake a number of covert activities to access that data, such as entering specified premises and doing any other thing reasonably necessary to conceal their actions. For the purposes of s 25A, 'computer' is currently defined in s 22 as 'a computer, a computer system or part of a computer system'.

The Bill proposes to amend this definition and also to remove the word 'particular' from s 25A, with the effect that a single computer access warrant may apply to more than one

computer. ‘Computer’ would instead be defined as (a) one or more computers, (b) one or more computer systems, (c) one or more computer networks, or any combination thereof. The Bill would also define ‘target computer’ as a particular computer, a computer located on particular premises, or ‘a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known)’. The Commonwealth Attorney-General explained in his Second Reading speech that the purpose of these amendments is to ‘ensure that ASIO’s intelligence-collection and related powers keeps pace with technological developments, particularly the use of online communications by persons of security interest’.¹ This is a commendable goal. However, we are concerned that the proposed amendments are overbroad and may result in undue and unnecessary intrusions upon the right to privacy.

There are two main problems with the proposed changes. The first is that the Bill offers no definition of a ‘computer network’. The Explanatory Memorandum gives only the vague explanation that this phrase is used ‘in the sense of a group of linked computers’.² It is unclear what would constitute a relevant ‘link’ between computers and, in any event, this explanation is not incorporated into the text of the Bill. At its broadest, a computer network could plausibly refer to all computers that have a connection to the Internet.³ It is certainly the case that the Internet is ‘likely to be used’ by the subject of the intelligence gathering operation, as specified in the proposed definition of ‘target computer’.

While we accept that this is almost certainly not the intended meaning of the provisions, there is nothing in the legislation to prevent such a broad reading being relied upon by a government. Large numbers of innocent persons could therefore be exposed to potentially severe invasions of their privacy. Even if the proposed warrant provisions were used responsibly by ASIO, such broad drafting undermines the rationale for the computer access warrant regime, namely, that intelligence-gathering powers are constrained within clearly defined and appropriate limits. For these reasons, we believe that the Bill should include a definition of ‘computer network’ that places clear restrictions on the power to access multiple computers. The definition of a ‘computer network’ should require a group of computers to be linked in some substantive way, such as by having shared storage drives, and not merely by virtue of being connected to the Internet or by some other telecommunications technology.

The second problem is that the Bill offers no higher or additional standard for accessing multiple computers as compared to a single computer. If the proposed changes to the warrant

¹ Commonwealth Parliament, *Parliamentary Debates*, 16 July 2014, 66 (George Brandis).

² Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014 (Cth) 63.

³ See Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of National Security Legislation* (2013) 87.

provisions are adopted, ASIO will be able to access entire computer networks (such as those of a workplace where a person of security interest is employed or a university where the person is studying) in the same way as they are currently able to access a single target computer. This means that ASIO could access and copy the files of other users on a network, such as those of colleagues or other university students, where this would ‘substantially assist’ in the collection of intelligence in relation to the person.

Given the potentially severe privacy implications of the proposed amendments, we believe that an additional burden of proof should be imposed where ASIO requests access to multiple computers or a computer network. One option is for the legislation to specify that ASIO may access computers on a network other than a specified computer only if there are reasonable grounds for believing that the person had access to those other computers (either directly or by virtue of access to shared storage drives). Or, in the alternative, that accessing those other computers must be reasonably necessary to collect intelligence in relation to the person and that ASIO must previously have exhausted other means of obtaining that intelligence. This would be consistent with the current restriction on the interception of third-party communications under s 9(3)(a) of the *Telecommunications (Interception and Access) Act 1979* (Cth).⁴

b. Altering data on the target computer

The Bill also proposes to amend the restriction on the addition, deletion or alteration of data on a target computer. Currently, s 25A(5) of the ASIO Act provides that ASIO officers cannot do any of these things while executing a computer access warrant if it would either interfere with the ‘lawful use’ of the target computer or cause ‘any loss or damage’ to other persons lawfully using the target computer.

The Bill proposes to amend this section to provide first that ASIO officers cannot add, delete or alter data in ways that are likely to *materially* interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless it is necessary to execute the warrant. And, secondly, ASIO will be prohibited from doing any of these things if it would be likely to cause ‘other material loss or damage to other persons lawfully using the computer’. By implication, ASIO officers will be permitted to add, delete or alter data in ways that do not constitute material interference and which are not likely to cause material loss of damage.

⁴ See *ibid* 93-94.

The purpose of this amendment is to allow ASIO to perform certain actions that are necessary in order to obtain data from a computer but which are currently prohibited. Section 25A(5) has been described as operating as a blanket prohibition preventing ASIO from interfering with the target computer even in a ‘minor or inconsequential’ way, such as by temporarily slowing its function.⁵ We agree that the provision should be relaxed to allow for minor disruptions or alterations that are necessary in order to obtain data held on a computer. However, we are concerned by the prospect of allowing ASIO officers to materially interfere with, interrupt or obstruct multiple computers and even computer networks. The scale of this is limited only by the two provisos set out above. The vague wording of these – for example, the lack of any definition of ‘material’, the reference to lawful use ‘by *other* persons’ and causing any ‘*other* material loss or damage to *other* persons’ – means that it is not clear that they would be sufficient to protect against significant delays or interruptions to the use of computer networks by third parties.

c. Access to the target computer via third party computers and communications in transit

Finally, the Bill proposes to allow access to a target computer via third-party computers and communications in transit. This has been said to be necessary because people are becoming increasingly ‘security conscious and ASIO must consider “innovative methods” to access the target computer’.⁶ Assuming that such methods are necessary in at least some cases (which is difficult to assess without further information), this still does not justify the broad wording of the provisions. The proposed amendments would allow ASIO to access the computers of third parties where it is ‘reasonable in all the circumstances to do so’.⁷ This is a very low threshold given the severe implications for privacy that access to a person’s computer entails. The wording suggests that ASIO would be able to access the computers or communications of third parties, such as the friends and colleagues of a person of security interest, if doing so was simply one amongst many viable options of obtaining that intelligence. A higher burden of proof should be imposed before the privacy of non-suspect third parties is intruded upon. We support the submission of the Victorian Privacy Commissioner and the Inspector-General of Intelligence and Security (‘IGIS’) to the 2013 Inquiry that third-party access should be limited to cases where doing so is: (a) necessary to obtain intelligence in relation to the person; and (b) all other methods of obtaining that intelligence have been exhausted by ASIO.⁸ These criteria should be made explicit in the text of the Bill.

⁵ See Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of National Security Legislation* (2013) 90 (submission by Attorney-General’s Department).

⁶ *Ibid* 92.

⁷ National Security Legislation Amendment Bill (No 1) 2014 (Cth) Schedule 2 item 23.

2. Establishing a special intelligence operations regime (Schedule 3)

The Bill proposes to establish a special intelligence operations ('SIO') regime. This regime would operate to give immunity to ASIO employees and affiliates from criminal and civil liability for certain conduct where an SIO has been authorised. It is ostensibly modelled upon the Australian Federal Police ('AFP') controlled operations regime in the *Crimes Act 1914* (Cth) ('Crimes Act').

In the first place, the onus is upon the government to justify why the SIO regime is required. Caution should be exercised before expanding the powers of intelligence – and especially domestic intelligence – agencies. The Second Reading speech states that '[i]t is appropriate that corresponding protections [to those available to the AFP] are extended to participants in cover intelligence operations'.⁹ However, such an explanation is insufficient. ASIO is not a law enforcement agency and should not automatically be given the same powers as such an agency. In particular, it is 'not accountable through the criminal trial process in the way that a law enforcement agency is. ... It is in a very different constitutional position, a very different administrative position and a very different policy position, and it is essentially secret'.¹⁰ The striking difference between law enforcement and domestic intelligence agencies is reflected in the fact that comparable nations – such as the United Kingdom, New Zealand and Canada – have not given their like agencies a general immunity from criminal and civil liability.¹¹

The Explanatory Memorandum states that 'some significant covert operations do not commence or are ceased' because of the lack of immunity for domestic intelligence officers.¹² We are unable to comment upon this except to say that 38 people have been charged with terrorism offences in Australia and 26 of that number have been convicted. These statistics by themselves do not suggest that there have been significant gaps in the ability to gather intelligence about potential risks to national security.

⁸ Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of National Security Legislation* (2013) 93-94.

⁹ Commonwealth Parliament, *Parliamentary Debates*, 16 July 2014, 66 (George Brandis).

¹⁰ Quoted in Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of National Security Legislation* (2013) 110.

¹¹ See *Intelligence Services Act 1994* (UK); *New Zealand Security Intelligence Service Act 1969* (NZ) s 4A; *Canadian Security Intelligence Service Act 1985* (Can) s 20; *Criminal Code 1985* (Can) s 25(1).

¹² Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014 (Cth) 97.

Our strong preference is to rely upon cooperation between intelligence and law enforcement agencies rather than creating a new legislative regime which gives ASIO officers immunity from civil and criminal liability. ASIO always has the ability to request the AFP to exercise its existing powers under the Crimes Act. This is nothing out of the ordinary. The terrorism investigations conducted in Australia to date have been characterised by a high – and commendable – level of cooperation between intelligence and federal, state and territory law enforcement agencies. We acknowledge that there may be some rare instances in which law enforcement agencies are unable to exercise these powers, for example, where there is insufficient evidence to indicate the commission of an offence. In these circumstances, it would still be open to ASIO to direct its employees and affiliates to engage in an undercover operation. It may simply instruct those taking part not to engage in any illegal activities or, in the alternative, rely upon the discretion of the Commonwealth Director of Public Prosecutions whether to prosecute in circumstances where such illegality was unavoidable.

Despite these concerns expressed by ourselves and others, the establishment of an SIO regime was supported by the PJCIS in the 2013 Inquiry.¹³ Importantly, however, the Committee noted that this regime should be ‘subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the Crimes Act’.¹⁴ We are concerned that the safeguards contained in the Bill fall short of this in at least two key respects. The first relates to the period for which an authorisation has effect. The Bill provides that authorisation for an SIO would expire after 12 months. This is considerably longer than the period under the Crimes Act. A controlled operation certificate lasts only three months unless it is renewed in three month increments (up to a total of 24 months).

Secondly, the Bill provides that authorisation for an SIO would be issued by the Director-General or Deputy Director-General of Security. This is similar to the process for authorising a ‘major controlled operation’ under the Crimes Act whereby certification may only be given by the Commissioner or Deputy Commissioner of the AFP. The critical difference, however, is that the decision whether to renew a controlled operations certificate – after it has been in effect for three months – lies with the Administrative Appeals Tribunal. This represents an important limitation upon the discretion of the Commissioner or Deputy Commissioner to authorise unlawful conduct by AFP employees. In *A v Hayden*, the High Court considered the immunity of ASIS officers from the criminal law. Justice Brennan stressed that ‘[t]he incapacity of the executive to dispense its servants from obedience to laws made by Parliament is the cornerstone of a parliamentary democracy’.¹⁵ If the SIO regime goes ahead,

¹³ Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of Australia’s National Security Legislation* (2013) 111-112.

¹⁴ Ibid 112, Recommendation 28.

the power to issue (or at least to renew or issue subsequent) authorisations should at the very least be given to an independent body. This would operate as an important safeguard against – the currently unchecked possibility – of rolling SIO authorisations being issued on an annual basis.

The previous proposal considered by the PJCIS included a provision for mandatory review after five years. We recommended that this should be supplemented by a sunset clause. The value of such a clause is that the Commonwealth Parliament is forced, in light of any recommendations made by the review body, to directly address whether to allow the SIO regime to lapse or to enact new legislation in the same terms. We commend the government for including in this Bill a requirement that the Director-General of Security must report to the Minister and the Inspector-General of Intelligence and Security on the operation of the SIO regime. However, it has unfortunately failed to include either a requirement for mandatory review or a sunset clause. We believe that both of these are appropriate given the unprecedented and exceptional nature of the SIO regime.

Our final point of concern relates to the two offences for the unauthorised disclosure of information in the proposed s 35P. These were not part of the SIO regime that was examined in the 2013 Inquiry. We appreciate that there are equivalent offences applying to controlled operations under the Crimes Act. However, the new offences must be considered on their own merits. This is not only for the simple reason that they concern the activities of an intelligence – rather than a law enforcement agency – but also because the scope of the new offences is potentially much greater than those contained in the controlled operations regime. An SIO may be authorised where it would assist ASIO in the performance of one or more very broadly defined special intelligence functions, for example, the collection of intelligence relevant to security. A controlled operation, in contrast, may only be authorised where the authorising officer is satisfied that there are reasonable grounds that a serious offence has been, is being, or is likely to be committed.

The first offence provides that a person may be imprisoned for a maximum of five years for disclosing any information relating to an SIO. This offence is exceptionally broad. In contrast to the offences that will be discussed in the next section of this submission, it applies to *any* person (and not simply someone in a position of privilege, such as an ASIO employee or contractor). There is no requirement that the person is aware that an SIO has been authorised. And, in fact, such knowledge is highly unlikely given the secrecy which surrounds the authorisation process. It is enough that the person is reckless, that is, aware of a substantial risk, that the disclosed information is connected in even some minor way with an SIO. This is

¹⁵ (1984) 156 CLR 532, 580.

a very low standard. A journalist might, for example, be subject to up to five years imprisonment where they publish an article containing any – even very vague – information about an ongoing terrorism investigation that relates to an SIO. A teacher who subsequently uses this article as a discussion aid in a legal studies class might also be caught by the offence. This first disclosure offence therefore has the potential to have a considerable chilling effect upon public debate about matters that are clearly of national interest.

The Explanatory Memorandum justifies the offences as ‘creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation’.¹⁶ However, the first offence clearly goes well beyond this purpose as it does not require any evidence as to the adverse consequences – or even possible consequences – of disclosure. The second aggravated offence, in contrast, is enlivened only where the person *intends* or the disclosure *will* endanger the health or safety of any person or prejudice the conduct of a special intelligence operation. Whilst the penalty for this offence is arguably excessive, our main objection is to the very limited excuses in subsection (3) and, in particular, the lack of a public interest defence. The submission of the Attorney-General’s Department to this inquiry refers to the *Public Interest Disclosure Act 2013* (Cth) (‘PID Act’).¹⁷ However, this Act has very limited application here. It applies only to disclosures by public officials and, furthermore, as will be discussed in the next section of this submission, it places special restrictions on the disclosure of information connected with intelligence agencies. Under the proposed SIO regime, a journalist could still be subject to up to ten years imprisonment for publishing an article which reveals the abuse of that regime, such as, for example, the general surveillance of non-suspect Muslim communities.

3. Changing the rules under which ASIS may cooperate with ASIO in the performance of its functions (Schedule 5)

Item 11 of the Bill proposes to insert a new s 13B into the *Intelligence Services Act 2001* (Cth) (‘IS Act’). The Commonwealth Attorney-General stated in the Second Reading speech that this amendment ‘enhances the capacity of ASIS [Australia’s foreign intelligence gathering agency] to cooperate with ASIO, by improving the statutory arrangements for the collection and sharing of certain security related intelligence’.¹⁸ We are concerned, however, that the principal effect of this amendment would not be to improve cooperation between the

¹⁶ Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014 (Cth) 111.

¹⁷ Attorney-General’s Department, Submission No 1, Parliamentary Joint Committee on Intelligence and Security, Inquiry into the National Security Legislation Amendment Bill (No 1) 2014 (Cth), July 2014, 10.

¹⁸ Commonwealth Parliament, *Parliamentary Debates*, 16 July 2014, 67 (George Brandis).

agencies but rather to internalise the processes for applying for and authorising surveillance of Australians overseas by ASIS. This would have a significant and detrimental effect upon the accountability framework under which this agency operates.

Currently, the circumstances in which such surveillance may occur are limited by the ministerial authorisation process. Section 9(1) requires that the Minister be satisfied that:

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

The *Telecommunications Interception and Intelligence Services Amendment Act 2011* (Cth) inserted into the IS Act a provision explicitly allowing ASIS, DSD and DIGO – when requested by the Director-General of Security – to cooperate with and assist ASIO in the performance of its very broad-ranging security functions. Section 13A did not, however, have the effect of circumventing the overarching requirement of ministerial authorisation. The Replacement Explanatory Memorandum to the Act instead stated that ‘ASIS DSD and DIGO will retain their obligation to obtain a Ministerial Authorisation ... when they undertake an activity for the purpose of collecting new intelligence on an Australian person even if they are solely performing the activity for the purpose of assisting another agency’.¹⁹ This provision was simply intended to clarify the ability – and indeed desirability – of Australia's domestic and foreign intelligence agencies to cooperate with one another in the exercise of their functions, for example, to share staff and resources.

The proposed inclusion of s 13B in the IS Act *would* circumvent the requirement of ministerial authorisation in some circumstances. This requirement would continue to apply to particularly intrusive intelligence-gathering (as defined in proposed s 13D). However, a new parallel regime would be created for all other forms of intelligence-gathering, such as human

¹⁹ Replacement Explanatory Memorandum to the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 (Cth) 33-34.

surveillance. ASIS would be permitted to collect intelligence on an Australian or class of Australians overseas wherever the Director-General of Security or a person authorised by him or her gives written notification to that agency that this intelligence is required by ASIO. In contrast to the rigorous criteria for ministerial authorisation, the only real limitation under the new regime is that the activity or series of activities must be undertaken to support ASIO in the performance of its functions. These are extremely broad-ranging. Of even greater concern is that the requirement of written notification may be dispensed with if an authorised staff member of ASIS believes that it is not practicable in the circumstances for it to be provided in advance of the activity. In such circumstances, it would simply be necessary for ASIS to notify ASIO and the IGIS after the fact. This goes against the clear recommendation of the 2013 Inquiry that ‘where ASIS proposes to collect intelligence on an Australian person ..., this would still need to be at the request of ASIO’.²⁰

The underlying premise for the amendments proposed in the Bill is that ‘[t]he differences in the legislative regimes that apply to ASIO when it produces intelligence on Australian persons who are overseas have led to situations that limit the extent of cooperation between the agencies’.²¹ It is said to follow from this that a blanket approach should be taken to the collection of intelligence about Australians by ASIO and the collection of intelligence about Australians by ASIS when it is cooperating with that agency in the performance of its functions. This, however, ignores the fact that ASIS and ASIO have different functions, operate under different accountability frameworks and with different levels of transparency. It was the recognition of these differences that led the 2004 Inquiry into Australian Intelligence Agencies (the Flood Inquiry) to conclude that it was appropriate for these agencies to remain separate.²² We believe that the current legislative arrangements strike an appropriate balance between the distinct characteristics of ASIS as a foreign intelligence agency and the need in some circumstances for it to assist ASIO to collect intelligence about Australians overseas.

4. Creating new disclosure offences that apply to ASIO employees and contractors and increasing the maximum penalties for the existing offences (Schedule 6)

²⁰ Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of Australia’s National Security Legislation* (2013) 136.

²¹ Attorney-General’s Department, Submission No 1, Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the National Security Legislation Amendment Bill (No 1) 2014* (Cth), July 2014, 20.

²² Inquiry into Australian Intelligence Agencies, *Report of the Inquiry into Australian Intelligence Agencies* (2004) 81.

The Bill proposes to strengthen and modernise the current offences for disclosing information in the national security context. Two of the authors of this submission have recently written an article (forthcoming in the *University of New South Wales Law Journal*) which examines the offences and protections under Australian law for people who disclose classified information.²³ The article is attached as Appendix 1. On the basis of our previous analysis, we believe that the Bill would exacerbate a number of problems with the existing legislation.

First, the Bill proposes to increase the penalties in both the ASIO Act and the IS Act for intelligence employees who disclose confidential information, and to introduce new disclosure offences so that these are standardised across the intelligence agencies. Importantly, the existing offences do not require any intention to prejudice security or defence. There is a strong argument to be made that the criminal law should be reserved for those cases where a person intends by disclosing classified information to harm the public interest – and not merely because he or she breached statutory or common law duties.²⁴ As such, the existing offences (which impose a maximum penalty of two years imprisonment) are already problematic in terms of whether criminal penalties should apply. The Bill ignores this and simply proposes to increase the penalties for these offences by a further eight years.

Secondly, the proposed 10 year penalties for disclosing national security information would far exceed the penalties found in other legislation. Section 79 of the Crimes Act provides for a maximum penalty of seven years imprisonment where a person discloses official secrets ‘with the intention of prejudicing the security or defence of the Commonwealth’.²⁵ This offence applies to intelligence officers and other individuals who are entrusted with classified information. It is not clear why the offences in the ASIO Act and IS Act should carry a greater maximum penalty where there is *no* such intention to prejudice security or defence.

Thirdly, the proposed strengthening of the disclosure offences would exacerbate an existing problem, which is that the offences apply to any person who has entered into an ‘agreement or arrangement’ with an intelligence agency.²⁶ While there is a strong case to be made that these offences should apply to government contractors (as evidenced by the case of Edward Snowden), it is not clear that the offences should extend this far beyond intelligence employees. The wording suggests that an informal arrangement or other relationship with an

²³ Keiran Hardy and George Williams, ‘Terrorist, Traitor or Whistleblower? Offences and Protections for Disclosing National Security Information’ (2014) 37(2) *University of New South Wales Law Journal* (forthcoming).

²⁴ Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, December 2009) 9 (Recommendation 5-1), 138, 160, 324.

²⁵ *Crimes Act 1914* (Cth) s 79(2).

²⁶ *Intelligence Services Act 2001* (Cth) ss 39, 39A, 40; *Australian Security Intelligence Organisation Act 1979* (Cth) s 18.

intelligence agency would be sufficient to attract criminal penalties. This is problematic because it is not clear that such individuals would understand the special responsibilities associated with handling classified information to the same degree as intelligence employees. Because of this, it would be preferable for the offences to apply only to intelligence employees and contractors or, at the very least, for higher penalties to be stipulated for employees and contractors as compared to other persons.

Fourthly, the Bill proposes to create new offences for ‘unauthorised dealing with records’ which would carry a maximum penalty of three years imprisonment. These offences would apply as soon as an entrusted person copies or records classified information, regardless of what he or she intends to do or indeed ultimately does with that information. If authorised dealing offences are to be created, we believe that they should – at the very least – require that the person’s conduct ‘is likely to result in ... the information being communicated or made available’ to another person.²⁷ This would ensure that there is at least some risk that the information would be disclosed to another before a criminal penalty may be imposed.

These issues are particularly concerning given the lack of protection for whistleblowers in the national security context. The PID Act provides immunity for public officials who disclose misconduct by government agencies in specified circumstances.²⁸ However, as a result of exemptions for intelligence information and information related to intelligence agencies,²⁹ there is virtually no protection for intelligence employees who disclose information obtained in the course of their duties (even where such a disclosure would expose gross misconduct or unlawful activities in which an intelligence agency was involved).³⁰ If the proposed disclosure offences are to be enacted, the government should consider whether some relaxation of the exemptions for intelligence information under the PID Act would help to lessen the potentially severe impact of these offences.

A final overarching point is that the government’s claim that there are ‘significant gaps’ in the law is simply not supported.³¹ There is a wide range of existing offences that could apply to the disclosure of classified information, including severe penalties for terrorism, espionage

²⁷ As in the espionage offence in the *Criminal Code Act 1995* (Cth) s 91.1(1)(c).

²⁸ *Public Interest Disclosure Act 2013* (Cth) ss 26, 29. See Keiran Hardy and George Williams, ‘Terrorist, Traitor or Whistleblower? Offences and Protections for Disclosing National Security Information’ (2014) 37(2) *University of New South Wales Law Journal* (forthcoming) Pt IV.

²⁹ *Public Interest Disclosure Act 2013* (Cth) ss 26(1), 41.

³⁰ See Keiran Hardy and George Williams, ‘Terrorist, Traitor or Whistleblower? Offences and Protections for Disclosing National Security Information’ (2014) 37(2) *University of New South Wales Law Journal* (forthcoming) Pt IV.

³¹ Commonwealth Parliament, *Parliamentary Debates*, 16 July 2014, 67 (George Brandis).

and treason,³² as well as other penalties for disclosing official secrets and the disclosure of information by Commonwealth officers.³³ And, contrary to the government's suggestion that 'no such offences exist',³⁴ many of these offences would also apply to the situation where a person merely possesses or retains information. Section 79 of the Crimes Act provides for a maximum penalty of seven years imprisonment where a person retains a classified document 'when it is contrary to his or her duty to retain it'.³⁵ Given this comprehensive array of existing offences, there is no demonstrable need to create a new 'three tier structure' for regulating the disclosure of classified information.³⁶

Yours sincerely

Mr Keiran Hardy

Doctoral Candidate, Gilbert + Tobin Centre of Public Law, University of New South Wales

Dr Nicola McGarrity

Lecturer and Director, Terrorism Law Reform Project, Gilbert + Tobin Centre of Public Law, University of New South Wales

Professor George Williams AO

Anthony Mason Professor and Foundation Director, Gilbert + Tobin Centre of Public Law, University of New South Wales

³² See Keiran Hardy and George Williams, 'Terrorist, Traitor or Whistleblower? Offences and Protections for Disclosing National Security Information' (2014) 37(2) *University of New South Wales Law Journal* (forthcoming) Pt II.

³³ See *ibid* Pt III.

³⁴ Commonwealth Parliament, *Parliamentary Debates*, 16 July 2014, 67 (George Brandis).

³⁵ *Crimes Act 1914* (Cth) s 79(5).

³⁶ Commonwealth Parliament, *Parliamentary Debates*, 16 July 2014, 68 (George Brandis).

Forthcoming in the University of New South Wales Journal: non-final draft

**TERRORIST, TRAITOR, OR WHISTLEBLOWER? OFFENCES AND
PROTECTIONS IN AUSTRALIA FOR DISCLOSING NATIONAL SECURITY
INFORMATION**

KEIRAN HARDY* AND GEORGE WILLIAMS**

I INTRODUCTION

Whether Chelsea (formerly Bradley) Manning, Julian Assange, and Edward Snowden are heroes or traitors is a divisive question. As is now well known, the WikiLeaks saga began in 2010 when Manning, who worked as an intelligence analyst for the US military in Iraq, downloaded the contents of a secure military database and sent them to WikiLeaks. WikiLeaks is a not-for-profit media organisation which specialises in protecting sources who leak classified information. It does so by providing a ‘high security anonymous drop box fortified by cutting-edge cryptographic information technologies’.¹ The documents that Manning leaked to WikiLeaks included more than 250 000 diplomatic cables from the US State Department, around 500 000 secret military documents linked to the wars in Iraq and Afghanistan, confidential files relating to nearly 800 detainees at Guantanamo Bay, and videos of US forces killing Iraqi and Afghani civilians.² The leaked documents were published in stages on the WikiLeaks website and by newspapers including *The Guardian*, the *New York Times*, and *Der Spiegel*. Manning has since been convicted by a United States military court of multiple offences under the US Espionage Act and sentenced to 35 years’ imprisonment, but was acquitted of a charge of aiding the enemy.³

Julian Assange, an Australian citizen and the founder of WikiLeaks, remains in the Ecuadorean Embassy in London. Assange sought asylum in June 2012 to evade sexual assault charges in Sweden, although his larger concern is to avoid extradition to the United States and possible reprisals from the US government.

The saga took on a new dimension when Edward Snowden released details of PRISM, a worldwide data mining program conducted by the United States’ National Security Agency (NSA).⁴ Snowden was an employee of Booz Allen Hamilton, a technology consulting

* PhD Candidate, Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales.

** Anthony Mason Professor, Scientia Professor and Foundation Director, Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales; Australian Research Council Laureate Fellow; Barrister, New South Wales Bar.

¹ WikiLeaks, *WikiLeaks* (15 January 2014) <<https://wikileaks.org>>. The main technology used by WikiLeaks is the ‘Tor’ encryption program, which was originally developed by the US Navy: see David Leigh and Luke Harding, *WikiLeaks: Inside Julian Assange’s War on Secrecy* (The Guardian, 2011) 53-56. Manning’s actions were discovered not because the Tor encryption failed, but because he confessed his actions to a hacker friend (Adrian Lamo): see Leigh and Harding, 72-87.

² See Leigh and Harding, above n 1, 116-144; Jane Cowan, ‘Bradley Manning found guilty of espionage, not guilty of aiding enemy over WikiLeaks release’, *ABC News* (Online), 31 July 2013 <<http://www.abc.net.au/news/2013-07-31/bradley-manning-found-guilty-of-espionage/4854798>>.

³ Cowan, *ibid*. Manning’s experience suggests that a member of the Australian Defence Force might be tried in a military tribunal under the *Defence Force Discipline Act 1982* (Cth). This article focuses on employees of the Commonwealth public service, particularly those of intelligence agencies. We do not consider the implications for military law.

⁴ See, eg, Glenn Greenwald, Ewen MacAskill and Laura Poltras, ‘Edward Snowden: the whistleblower behind the NSA surveillance revelations’, *The Guardian* (London), 10 June 2013; Spencer Ackerman, ‘US tech giants knew of NSA data collection, agency’s top lawyer insists’, *The Guardian* (London), 19 March 2014; David Wroe, ‘Government refuses to say if it receives PRISM data’, *Sydney Morning*

firm, and was contracted to work for the NSA. He has since applied for political asylum in Russia, where he continues to justify his actions via the Internet.⁵

The WikiLeaks and Snowden affairs raise fundamental questions about the balance to be struck between the transparency of government and the protection of classified information. On the one hand, many view the leaking of classified information as an irresponsible and illegal act which endangers lives and national security. Former Australian Prime Minister Julia Gillard described Assange's actions as 'illegal' and 'grossly irresponsible'.⁶ US Vice-President Joe Biden labelled Assange a 'hi-tech terrorist'.⁷ Former US Secretary of State Hillary Clinton described Assange's actions as an 'attack on the international community'.⁸ Some have even called for Assange's assassination, arguing that he should be considered an enemy combatant and treated 'the same way as other high-value terrorist targets'.⁹

On the other hand, Manning, Assange and Snowden have been cast by others as champions of government accountability in the digital age. Large protests have been held and support groups established in honour of all three.¹⁰ The cyber-activist group 'Anonymous' launched denial-of-service attacks against MasterCard and PayPal for refusing to process donations to the WikiLeaks website.¹¹ Amnesty International has created an online petition

Herald, 12 June 2013; Nick Perry and Paisley Dodds, 'Five Eyes spying alliance will survive Edward Snowden: experts', *Sydney Morning Herald*, 18 July 2013; Phillip Dorling, 'Australia gets "deluge" of US secret data, prompting a new data facility', *Sydney Morning Herald*, 13 June 2013.

⁵ *Sydney Morning Herald* (online), 'Edward Snowden: NSA setting fire to the internet', 11 March 2014 <<http://www.smh.com.au/it-pro/security-it/edward-snowden-nsa-setting-fire-to-the-internet-20140311-hvh7m.html>>; *The Guardian* (online), 'Edward Snowden talks NSA and internet surveillance at SXSW – video' <<http://www.theguardian.com/world/video/2014/mar/10/edward-snowden-talks-nsa-internet-surveillance-sxsw-video>>.

⁶ ABC News (online), 'Gillard fires at "illegal" WikiLeaks dump', 2 December 2010 <<http://www.abc.net.au/news/2010-12-02/gillard-fires-at-illegal-wikileaks-dump/2359304>>; *The Australian*, 'Julia Gillard can't say how WikiLeaks founder Julian Assange has broken the law', 7 December 2010 <<http://www.theaustralian.com.au/national-affairs/julia-gillard-cant-say-how-wikileaks-founder-julian-assange-has-broken-the-law/story-fn59niix-1225966954147>>; *Sydney Morning Herald*, 'WikiLeaks acting illegally, says Gillard', 2 December 2010 <<http://www.smh.com.au/technology/technology-news/wikileaks-acting-illegally-says-gillard-20101202-18hb9.html>>.

⁷ Ewen MacAskill, 'Julian Assange like a hi-tech terrorist, says Joe Biden', *The Guardian* (London), 19 December 2010.

⁸ Mary Beth Sheridan, 'Hillary Clinton: WikiLeaks release an "attack on international community"', *Washington Post*, 29 November 2010.

⁹ Jeffrey T Kuhner, 'Kuhner: Assassinate Assange?', *Washington Times*, 2 December 2010. Similar comments were made by Tom Flanagan, a former aide to the Canadian Prime Minister, and then potential Republican presidential candidate Sarah Palin: see CBC News (online), 'Flanagan regrets WikiLeaks assassination remark'; NBC News (online), 'Assange lawyer condemns calls or assassination of WikiLeaks' founder' <http://www.nbcnews.com/id/40467957/ns/us_news-wikileaks_in_security/t/assange-lawyer-condemns-calls-assassination-wikileaks-founder/#.UzCt36Wz5II>.

¹⁰ Chelsea Manning Support Network, *Pvt. Manning Support Network* (26 March 2014) <<http://www.bradleymanning.org>>; David Batty, 'Julian Assange supporters plan protests worldwide', *The Guardian* (London), 11 December 2010; BBC News (online), 'Wikileaks protests in Spain over Julian Assange arrest', 12 December 2010 <<http://www.bbc.co.uk/news/world-europe-11977406>>; Jim Newell, 'Thousands gather in Washington for anti-NSA "Stop Watching Us" rally', *The Guardian* (London), 26 October 2013; ABC News (online), 'Hong Kong protestors rally in support of US spy whistleblower Edward Snowden', 16 June 2013 <<http://www.abc.net.au/news/2013-06-15/hong-kong-protest-in-support-of-snowden/4756572>>.

¹¹ These attacks were known as 'Operation Payback': see *The Australian* (online), 'European Amazon websites down after attack by Wiki-Leaks supporters', 13 December 2010 <<http://www.theaustralian.com.au/news/world/european-amazon-websites-down-after-attack-by-wikileaks-supporters/story-e6frg6so-1225970194135>>; Lauren Turner, 'Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and Paypal', *The Independent* (London), 24 January 2013; Sandra

calling for Manning's release, arguing that the sentence imposed was more severe than some soldiers have received for rape and war crimes.¹² Slavoj Žižek has called for an international network to protect whistleblowers,¹³ describing Manning, Assange and Snowden as 'our new heroes, exemplary cases of the new ethics that befits our era of digitalised control'.¹⁴

Debates about whether these leaks were morally or ethically justified will continue, without the prospect of a definitive resolution. Our purpose in this paper is narrower and focused on Australia.¹⁵ We examine how Australian law would deal with the actions of people such as Assange, Manning and Snowden if undertaken with regard to Australian interests and information. This has not before been examined,¹⁶ but is a question of significant public interest. Specifically, we consider the offences and protections available under the law where an Australian citizen discloses sensitive government information. In doing so, we also evaluate whether that law provides an adequate, or overbroad, means of dealing with such situations.

Because recent events have focused on military and intelligence activities, our focus is on government information that is relevant to national security. There is no single definition of national security information in the Australian context, although the most commonly used definitions are broad and encompass a range of political threats to the state. 'National security information' is defined in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) as any information which if disclosed would affect the protection of the Commonwealth from a range of threats including espionage, sabotage, politically motivated violence, attacks on Australia's defence system, acts of foreign interference, and serious threats to border security.¹⁷ According to the Australian *Protective Security Policy Framework* (PSPF), a set of guidelines for managing information security within the Commonwealth government, national security information is defined as 'any official resource' that records information about, or is associated with, Australia's security, defence, international relations, or the national interest.¹⁸ Under the PSPF, national security information is classified to four levels ('Protected', 'Confidential', 'Secret', and 'Top Secret') according to the potential damage that could be caused by its release.¹⁹

Laville, 'Anonymous cyber-attacks cost PayPal £3.5m, court told', *The Guardian* (London), 22 November 2013.

¹² Amnesty International, *Support the Release of Chelsea Manning* (15 November 2013) <<http://www.amnesty.org/en/appeals-for-action/chelseamanning>>.

¹³ Slavoj Žižek, 'Edward Snowden, Chelsea Manning and Julian Assange: our new heroes', *The Guardian* (London), 3 September 2013.

¹⁴ Ibid.

¹⁵ Cf Ben Saul, who focuses more heavily on moral questions about whether Assange's actions were justified, as well as questions surrounding the right to asylum in international law: Ben Saul, 'WikiLeaks: Information Messiah or Global Terrorist?', Sydney Law School Legal Studies Research Paper No. 14/09 (January 2014).

¹⁶ The Australian Federal Police (AFP) did launch an investigation into Assange, which concluded that he had not committed any offence under Australian law: Dylan Welch, 'Julian Assange has committed no crime in Australia: AFP', *Sydney Morning Herald*, 17 December 2010. To be clear, our purpose is not to consider whether Assange or any other person has violated Australian law, but rather to explore the scope of the law in this area by considering how the laws would apply to a range of possible scenarios.

¹⁷ *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ('NSIA'), s 7. The definition of national security in the NSIA relies on the definition of 'security' in the *Australian Security Intelligence Organisation Act 1979* (Cth), s 4. Pt 5 of the NSIA includes a range of offences for disclosing national security information, but these apply within criminal and civil proceedings when an individual fails to comply with specified procedures for handling national security information in the courtroom. Our focus in this article is on the situation where a person comes across classified information in the course of their employment or otherwise and decides to publish that information or communicate it to another person, as in the WikiLeaks and Snowden scenarios.

¹⁸ Australian Government, *Information Security Management Guidelines: Australian Government Security Classification System* (2013) 8.

¹⁹ See *ibid* 9-10. 'Protected' means that disclosure of the information 'could cause damage to the Australian Government, commercial entities or members of the public'; 'Confidential' means that

Part II of this paper considers the most serious offences that could apply to an individual who discloses national security information: terrorism, espionage and treason. Part III considers a range of secrecy offences for Commonwealth employees and others, including specific offences which apply to employees of Australia's intelligence agencies. Part IV considers the circumstances in which individuals who disclose national security information might be protected by the new Commonwealth whistleblower scheme set out in the *Public Interest Disclosure Act 2013* (Cth).

II TERRORISM AND RELATED OFFENCES

This section considers three categories of offences that could apply to an individual who discloses national security information. These are serious offences which criminalise politically motivated action against the state. First, given the broad statutory definition of terrorism in the *Criminal Code Act 1995* (Cth) ('Criminal Code'),²⁰ the disclosure of national security information could qualify under Australia's counter-terrorism laws as a terrorist act or related offence. Secondly, the disclosure of national security information could constitute an act of treason. Thirdly, the disclosure of national security information could constitute an act of espionage.

A Terrorism Offences

The Howard government's main legislative response to the 9/11 attacks was a package of five Bills enacted in March 2002.²¹ When introducing the legislation into Parliament, Attorney-General Daryl Williams explained that the 9/11 attacks signalled 'a profound shift in the international security environment' and that Australia faced a 'higher level of terrorist threat' as a result.²² The five Bills were passed quickly by the Australian Parliament and included new offences for terrorist bombings and financing, increased surveillance powers, improved border security measures, and a range of pre-emptive criminal offences relating to terrorist acts.²³ In the years since this initial legislative response to 9/11, the Howard government's counter-terrorism laws have continually been supplemented with additional powers.²⁴

disclosure of the information 'could cause damage to national security'; 'Secret' means that disclosure of the information 'could cause serious damage to national security'; 'Top Secret' means that disclosure of the information 'could cause exceptionally grave damage to national security'.

²⁰ *Criminal Code Act 1995* (Cth), s 100.1

²¹ The five Bills were enacted as the following: *Security Legislation Amendment (Terrorism) Act 2002* (Cth); *Suppression of the Financing of Terrorism Act 2002* (Cth); *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* (Cth); *Border Security Legislation Amendment Act 2002* (Cth); *Telecommunications Interception Legislation Amendment Act 2002* (Cth).

²² Commonwealth, *Parliamentary Debates*, House of Representatives, 12 March 2002, 1040 (Daryl Williams).

²³ See *Security Legislation Amendment (Terrorism) Act 2002* (Cth); *Suppression of the Financing of Terrorism Act 2002* (Cth); *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* (Cth); *Border Security Legislation Amendment Act 2002* (Cth); *Telecommunications Interception Legislation Amendment Act 2002* (Cth).

²⁴ Indeed, Australia's response to terrorism since 9/11 has been described as one of 'hyper-legislation' with 61 separate pieces of anti-terror legislation being passed since 9/11: see Kent Roach, *The 9/11 Effect* (Cambridge: Cambridge University Press, 2011) 309; George Williams, 'The Legal Legacy of the War on Terror' (2013) 12 *Macquarie Law Journal* 3, 7; George Williams, 'A Decade of Australian Anti-Terror Laws' (2011) 35 *Melbourne University Law Review* 1136, 1144. Only occasionally have Australia's counter-terrorism laws been reduced in scope. For example, the *National Security Legislation Amendment Act 2010* (Cth) amended the 'dead-time' provisions in Pt IC of the *Crimes Act 1914* (Cth) and the controversial sedition offences in pt 5.1 of the *Criminal Code Act 1995* (Cth). However, the act also expanded the scope of by granting police a power to conduct warrantless searches: see *National Security Legislation Amendment Act 2010* (Cth), schs 1,3,4.

Most of these counter-terrorism laws hinge on a statutory definition of terrorism that was inserted in s 100.1 of the Criminal Code.²⁵ Section 100.1 was closely modelled on the UK's definition of terrorism in the *Terrorism Act 2000* (UK) and, as such, it sets out three requirements for an act or threat to qualify as terrorism.²⁶ First, the definition includes a motive requirement: it provides that the action must be done or threat made 'with the intention of advancing a political, religious or ideological cause'.²⁷ Secondly, the definition includes an intention requirement: it provides that the action must be done or threat made with the intention of coercing a government, influencing a government by intimidation, or intimidating a section of the public.²⁸ Thirdly, the definition includes a harm requirement: it sets out a list of possible harms that the conduct must cause or the threat must specify.²⁹ The list includes death and serious bodily injury,³⁰ but it also extends to a range of vaguer and less serious harms, such as endangering life, creating a serious risk to public health or safety, and seriously disrupting or interfering with electronic systems.³¹ Sub-section (3) of the definition sets out an exemption for protest, dissent or industrial action that is intended only to cause serious property damage,³² although the precise scope of this exemption remains unclear. Conduct will fall outside the political protest exemption if it is intended at a minimum to create a serious risk to public health or safety.³³

A number of criminal offences stem from this definition of terrorism. Most obviously, s 101.1 creates the offence of committing a terrorist act,³⁴ although in practice this has proved less relevant than a range of pre-emptive offences which apply to the early stages of preparing for a terrorist act.³⁵ In the context of releasing national security information, the most relevant of these offences would be:

²⁵ *Criminal Code Act 1995* (Cth), s 100.1. The definition of terrorism was inserted by *Security Legislation Amendment (Terrorism) Act 2002* (Cth), Pt 5.3. See generally Keiran Hardy and George Williams, 'What is "Terrorism"? Assessing Domestic Legal Definitions' (2011) 16(1) *UCLA Journal of International Law and Foreign Affairs* 77, 130-136; Ben Golder and George Williams, 'What is "Terrorism"? Problems of Legal Definition' (2004) 27(2) *University of New South Wales Law Journal* 270-95; Kent Roach, 'Defining Terrorism: The Need for a Restrained Definition' in Nicola LaViolette and Craig Forcece (eds), *The Human Rights of Anti-Terrorism* (Irwin Law, 2008) 97; Cathleen Powell, 'Defining Terrorism: Why and How' in Nicola LaViolette and Craig Forcece (eds), *The Human Rights of Anti-Terrorism* (Irwin Law, 2008) 128.

²⁶ *Terrorism Act 2000* (UK) c 11, s 1. The UK counter-terrorism laws, and particularly the statutory definition of terrorism, were highly influential in Commonwealth countries that had not enacted counter-terrorism laws prior to 9/11: see Kent Roach, 'The Post-9/11 Migration of Britain's Terrorism Act 2000', in Sujit Choudhry (ed), *The Migration of Constitutional Ideas* (Cambridge University Press, 2006) 374.

²⁷ *Criminal Code Act 1995* (Cth), s 100.1(1)(b). On the motive requirement in the definition of terrorism, see Ben Saul, 'The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalising Thought?' in Andrew Lynch, Edwina Macdonald and George Williams (eds), *Law and Liberty in the War on Terror* (Federation Press, 2007) 28; Kent Roach, 'The Case for Defining Terrorism With Restraint and Without Reference to Political or Religious Motive' in Andrew Lynch, Edwina Macdonald and George Williams (eds), *Law and Liberty in the War on Terror* (Federation Press, 2007) 39; Keiran Hardy, 'Hijacking Public Discourse: Religious Motive in the Australian Definition of a Terrorist Act' (2011) 34(1) *University of New South Wales Law Journal* 333.

²⁸ *Criminal Code Act 1995* (Cth), s 100.1(1)(a).

²⁹ *Criminal Code Act 1995* (Cth), s 100.1(2).

³⁰ *Criminal Code Act 1995* (Cth), s 100.1(2)(a),(c).

³¹ *Criminal Code Act 1995* (Cth), s 100.1(2)(d)-(f).

³² *Criminal Code Act 1995* (Cth), s 100.1(3). See Keiran Hardy, 'Operation Titstorm: Hacktivism or Cyber-Terrorism?' (2010) 33(2) *University of New South Wales Law Journal* 474, 489-492.

³³ *Criminal Code Act 1995* (Cth), s 100.1(3)(b)(iv).

³⁴ *Criminal Code Act 1995* (Cth), s 101.1 (maximum penalty is life imprisonment).

³⁵ See, eg, *R v Lodhi* [2006] NSWSC 571; *R v Elomar* [2010] NSWSC 10; *R v Khazaal* [2011] NSWCCA 129. These offences have been described and critiqued as a form of 'pre-crime' because they impose serious criminal penalties on the basis of unpredictable predictions of future conduct: see Lucia Zedner, 'Pre-Crime and Post-Criminology?' (2007) 11 *Theoretical Criminology* 261; Lucia Zedner, 'Fixing the Future? The Pre-Emptive Turn in Criminal Justice', in Bernadette McSherry, Alan Norrie and Simon Bronitt (eds), *Regulating Deviance: The Redirection of Criminalisation and the*

- Possessing things connected with terrorist acts (s 101.4);
- Collecting or making documents likely to facilitate terrorist acts (s 101.5); and
- Doing any other act in preparation for a terrorist act (s 101.6)³⁶

The penalty for possessing things or collecting documents connected with preparation for a terrorist act is 15 years where the person is aware of the relevant connection,³⁷ or 10 years where the person is reckless as to the existence of the connection.³⁸ The penalty for doing any other act in preparation for terrorism is life imprisonment.³⁹

In addition, div 102 of the Criminal Code makes it an offence to intentionally provide support or resources to a terrorist organisation where the support or resources would help the organisation to directly or indirectly plan, prepare, assist in or foster the doing of a terrorist act.⁴⁰ The penalty is 25 years' imprisonment where the person knows the organisation is a terrorist organisation,⁴¹ and 15 years' imprisonment where the person is reckless as to the fact that the organisation is a terrorist organisation.⁴²

Given the scope of the definition of terrorism in s 100.1 and these related offences, it is possible to describe the circumstances in which the disclosure of national security information could constitute an offence under Australia's counter-terrorism laws. Assuming that a person had classified national security information in his or her possession, the release of this information could constitute an act of terrorism if its release was designed to advance a political cause and to intimidate the government into changing its policy stance on a particular issue.⁴³ There is no additional requirement, as in some other countries' definitions of terrorism, that the conduct or threat be designed to strike immense fear or terror in the population.⁴⁴

The harm requirement would be satisfied if releasing the information endangered the lives of intelligence agents or soldiers in the field, or if releasing the information led to protests or riots which created a serious risk to public health or safety.⁴⁵ Indeed, given that the definition extends to acts that seriously interfere with electronic systems,⁴⁶ it is possible that the harm requirement could be satisfied by the act of hacking into a secure database to obtain

Futures of Criminal Law (Oxford: Hart, 2008) 35-58; Lucia Zedner, 'Preventive Justice or Pre-Punishment? The Case of Control Orders' (2007) 60(1) *Current Legal Problems* 174; Jude McCulloch and Sharon Pickering, 'Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror"' (2009) 49(5) *British Journal of Criminology* 628.

³⁶ *Criminal Code Act 1995* (Cth), ss 101.4-101.6.

³⁷ *Criminal Code Act 1995* (Cth), ss 101.4(1), 101.5(1).

³⁸ *Criminal Code Act 1995* (Cth), ss 101.4(2), 101.5(2).

³⁹ *Criminal Code Act 1995* (Cth), s 101.6(1).

⁴⁰ *Criminal Code Act 1995* (Cth), s 102.7. This offence requires that the Attorney-General has previously proscribed the organisation as a 'terrorist organisation'. Alternatively, it may be proven in court that the organisation is a terrorist organisation: see definition of a terrorist organisation in *Criminal Code Act 1995* (Cth), s 102.1. See *Benbrika v The Queen* [2010] VSCA 281. See generally Andrew Lynch, Nicola McGarrity and George Williams, 'Lessons From the History of the Proscription of Terrorist and Other Organisations by the Australian Parliament' (2009) 13(1) *Legal History* 25; Andrew Lynch, Nicola McGarrity and George Williams, 'The Proscription of Terrorist Organisations in Australia' (2009) 37(1) *Federal Law Review* 1; Nicola McGarrity, 'Review of the Proscription of Terrorist Organisations: What Role for Procedural Fairness?' (2008) 16(1) *Australian Journal of Administrative Law* 45.

⁴¹ *Criminal Code Act 1995* (Cth), s 102.7(1).

⁴² *Criminal Code Act 1995* (Cth), s 102.7(2).

⁴³ *Criminal Code Act 1995* (Cth), s 100.1(1)(a)-(b).

⁴⁴ See, eg, statutory definitions of terrorism in New Zealand and South Africa: *Terrorism Suppression Act 2002* (NZ), s 5(2)(a) ('induce terror in a civilian population'); South Africa, *Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004* (RSA), s 1(1)(xxv)(b)(ii) ('to induce fear or panic in a civilian population').

⁴⁵ *Criminal Code Act 1995* (Cth), s 100.1(2)(e).

⁴⁶ *Criminal Code Act 1995* (Cth), s 100.1(2)(f).

national security information, even if no such additional or subsequent harm was caused.⁴⁷ In addition, because the scope of s 100.1 extends explicitly to the threat of action,⁴⁸ the classified information would not even need to be released for the person's conduct to qualify as an act of terrorism.

For example, one could imagine a cyber-activist group hacking into a secure military database and downloading information about the complicity of Australian soldiers in the torture of detainees in the Middle East.⁴⁹ The group might then intimidate the Australian government by threatening to release the identities of the soldiers involved, so that the families of their victims could seek reprisals. The scope of s 100.1 would certainly extend to such a scenario. Indeed, the group might even be bluffing about the fact that they obtained the information, but the mere threat of releasing such information could be sufficient to constitute an act of terrorism. The political protest exemption would not apply in such a scenario if the act of releasing the information would be intended to endanger the lives of those soldiers.⁵⁰

In addition, the possession of national security information for purposes similar to those described above could trigger the pre-emptive terrorism offences. This could lead to severe penalties where no direct harm has been caused, and indeed where no final decision has even been made to release the information. For example, a person could be charged with possessing a thing connected with terrorism,⁵¹ or collecting or making a document connected with terrorism,⁵² if he or she downloaded classified material from a secure database in circumstances similar to those described above. If the person intended to release the information in a scenario that would fall under the statutory definition of terrorism, such as the threat by a cyber-activist group outlined above, any preparatory acts done to obtain the information could attract life imprisonment under s 101.6.⁵³ Given this possibility, it is curious that a person would receive a maximum penalty of only 25 years' imprisonment for intentionally giving the information to a terrorist organisation (s 102.7(1)) where that information could help to plan a terrorist act on Australian soil.⁵⁴ Arguably this is one of the most serious possible scenarios that could occur in the context of releasing national security information, and yet it would attract a significantly lower penalty than a person who intended to influence government policy through intimidation.

A related possibility is that a person who released national security information could be charged under Division 115 of the Criminal Code with intentionally or recklessly causing harm to Australians overseas. These offences were enacted in November 2002 in response to the Bali bombings.⁵⁵ Section 115.1 provides a maximum penalty of life imprisonment where a person engages in conduct outside Australia, the conduct causes the death of an Australian citizen or resident, and the person intended to cause death or was reckless as to that possibility.⁵⁶ Section 115.2 is the equivalent offence for manslaughter; it provides a maximum penalty of 25 years' imprisonment where death is caused and the person intended to cause (or

⁴⁷ See Keiran Hardy, 'WWMDs: Cyber-Attacks Against Infrastructure in Domestic Anti-Terror Laws' (2011) 27(2) *Computer Law & Security Review* 152; Hardy, 'Operation Titstorm', above n 32.

⁴⁸ *Criminal Code Act 1995* (Cth), s 100.1 (defined as 'action or threat of action').

⁴⁹ Similar revelations were made by the Public Interest Advocacy Centre in 2012: Public Interest Advocacy Centre, 'Australia complicit in military detention' (2 September 2012) <<http://www.piac.asn.au/news/2012/02/australia-complicit-illegal-military-detention>>; Public Interest Advocacy Centre, 'US report confirms Australian involvement in capture and transport of Iraqi prisoners' (2 September 2012) <<http://www.piac.asn.au/news/2012/02/us-report-confirms-australian-involvement-capture-and-transport-iraqi-prisoners>>; Dylan Welch, 'Australia's link to secret Iraq prisons', *Sydney Morning Herald*, 9 February 2012.

⁵⁰ *Criminal Code Act 1995* (Cth), s 100.1(3)(b)(iv).

⁵¹ *Criminal Code Act 1995* (Cth), s 101.4.

⁵² *Criminal Code Act 1995* (Cth), s 101.5.

⁵³ *Criminal Code Act 1995* (Cth), s 101.6.

⁵⁴ *Criminal Code Act 1995* (Cth), s 102.7(1).

⁵⁵ See Commonwealth, *Parliamentary Debates*, House of Representatives, 12 November 2002, 8797 (Daryl Williams).

⁵⁶ *Criminal Code Act 1995* (Cth), s 115.1(1).

was reckless as to the possibility of causing) serious harm.⁵⁷ Sections 115.3 and 115.4 apply in the case of serious harm rather than death, providing maximum penalties of 20 and 15 years' imprisonment respectively.⁵⁸ The cause element will be satisfied if the person's conduct 'substantially contributes' to the death or harm of an Australian citizen.⁵⁹

These offences could apply in a scenario, similar to the circumstances of Assange and Snowden, where a person sought refuge in a foreign country and released national security information that led to the death of or serious harm to Australian citizens. This might occur if the person failed to exercise due care in protecting the identities of Australian intelligence officers operating overseas. Another possibility is that revelations about national security issues could cause harm to Australians overseas by damaging Australia's reputation and causing foreign individuals or groups to seek reprisals. For example, relationships between the Australian and Indonesian governments were strained when Edward Snowden revealed that the Australian intelligence agencies had spied on the wife of the Indonesian Prime Minister and leading members of the Indonesian government.⁶⁰ One could imagine a similar scenario in which damaging revelations about national security issues led to reprisals causing serious harm to Australian citizens overseas.

B *Treason*

A second category of relevant offences is the treason offences in Division 80 of the Criminal Code. The offence of treason existed in the original version of the *Crimes Act 1914* (Cth) ('Crimes Act'), but this was revised after 9/11.⁶¹ The revised version of the offence included acts of violence against the Sovereign, Governor-General or Prime Minister (death, harm, imprisonment or restraint); levying war against the Commonwealth; assisting an enemy at war with the Commonwealth; assisting a country or organisation engaged in armed hostilities against the Australian Defence Force (ADF); and instigating a foreign person to invade Australia.⁶² In 2005, the offence was supplemented with new sedition offences,⁶³ which included the offences of 'urging' a person to assist an enemy at war or to engage in armed hostilities with the ADF.⁶⁴

The sedition offences attracted significant criticism on the grounds that they unduly restricted free speech, leading to an inquiry by the Australian Law Reform Commission (ALRC) that recommended their repeal and replacement.⁶⁵ In response, the current wording of the treason offences was introduced in 2010.⁶⁶ The amendments repealed the sedition offences and amended the basic offence of treason by creating a separate offence of 'materially assisting the enemy'.⁶⁷ The offence of treason, in s 80.1 of the Criminal Code, now provides a maximum penalty of life imprisonment where a person commits acts of violence against the Sovereign, Governor-General or Prime Minister (death, harm,

⁵⁷ *Criminal Code Act 1995* (Cth), s 115.2(1).

⁵⁸ *Criminal Code Act 1995* (Cth), ss 115.3(1), 115.4(1).

⁵⁹ *Criminal Code Act 1995* (Cth), s 115.9.

⁶⁰ See Peter Alford and Paul Maley, 'Let's restore trust to relationship, says Indonesia's Susilo Bambang Yudhoyono', *The Australian* (Sydney), 27 November 2013; Michelle Grattan, 'Phone spying rocks Australian-Indonesian relationship', *The Conversation* (Melbourne), 18 November 2013; George Roberts, 'Spying row: Julie Bishop says Australia setting up hotline with Indonesia to repair damage', ABC News (online), 6 December 2013 <<http://www.abc.net.au/news/2013-12-06/indonesia-tells-region-to-prepare-for-more-spying-leaks/5139110>>.

⁶¹ *Security Legislation Amendment (Terrorism) Act 2002* (Cth) Pt 5.1. See Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Review of Security and Counter Terrorism Legislation* (December 2006) 39 [4.3].

⁶² *Security Legislation Amendment Act 2002* (Cth), Item 2.

⁶³ *Anti-Terrorism Act (No 2) 2005* (Cth) sch 7.

⁶⁴ *Criminal Code Act 1995* (Cth), s 80.2(7)-(9) (now repealed).

⁶⁵ Australian Law Reform Commission (ALRC), *Fighting Words: A Review of Sedition Laws in Australia* (Report 104, July 2006) 158.

⁶⁶ *National Security Legislation Amendment Act 2010* (Cth) sch 1.

⁶⁷ *Criminal Code Act 1995* (Cth), s 80.1AA.

imprisonment or restraint); levies war against the Commonwealth; or instigates a foreign person to make an armed invasion of Australia.⁶⁸ The separate offence for materially assisting the enemy is now found in s 80.1AA.⁶⁹ It provides a maximum penalty of life imprisonment where a person engages in conduct that is intended to ‘materially assist’ an enemy at war with the Commonwealth or a country or organisation that is engaged in armed hostilities with the ADF.⁷⁰ In contrast to this fault element, the physical element of the offence requires only that the conduct assist (but not materially assist) the enemy, country or organisation.⁷¹ The higher fault element (of intending ‘material’ assistance) followed a recommendation by the ALRC, which suggested that an intention to ‘assist’ the enemy could encompass ‘merely dissenting opinions about government policy’, such as criticism of Australia’s contribution to the war in Iraq.⁷²

It is possible that the release of national security information could fall under the treason offence in s 80.1. For example, a person could release information about Australia’s military defences to a foreign intelligence service for the purpose of instigating an armed invasion of Australia. More likely, however, the disclosure of national security information would fall under the related offence of materially assisting the enemy. Manning was charged with a similar offence in the United States,⁷³ although she was found not guilty of aiding the enemy because prosecutors could not prove that she expected al-Qaeda would see the WikiLeaks material.⁷⁴ If a similar scenario occurred in Australia and the person expected that a terrorist organisation would see the leaked information, then s 80.1AA could be triggered.

Importantly, s 80.3 of the Criminal Code includes a defence for acts done in good faith.⁷⁵ This is available for the offence of materially assisting the enemy, but not for the basic offence of treason.⁷⁶ Section 80.3 provides that the defence will be made out where the person ‘tries in good faith’ to show that the Sovereign, Governor-General or Prime Minister is ‘mistaken in any of his or her counsels, policies or actions’.⁷⁷ In considering such a defence, the court may consider whether the acts were done for purposes ‘intended to be prejudicial to the safety or defence of the Commonwealth’, or ‘with the intention of causing violence or creating public disorder or a public disturbance’.⁷⁸ Given the wide variety of opinions about whether the actions of Manning, Assange and Snowden are justifiable, this would likely prove a difficult issue to resolve in any prosecution. If a court considered that the defence was not available because the person intended to ‘create public disorder or a public disturbance’,⁷⁹ then arguably s 80.1AA would go too far in criminalising legitimate behaviour. Many political protests are designed to create a public disturbance but should still be considered legitimate behaviour in a contemporary democratic society.

Section 80.1AA may also go beyond its intended purposes by failing to adequately distinguish the different ways in which a person might assist an enemy. In a submission to the

⁶⁸ *Criminal Code Act 1995* (Cth), s 80.1(1).

⁶⁹ *Criminal Code Act 1995* (Cth), s 80.1AA.

⁷⁰ *Criminal Code Act 1995* (Cth), s 80.1AA(1)(d), (4)(c).

⁷¹ *Criminal Code Act 1995* (Cth), s 80.1AA(1)(e), (4)(d).

⁷² ALRC, *Fighting Words*, above n 65, 15-16.

⁷³ See the crime of treason in 18 USC §2381: ‘Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death’.

⁷⁴ *Criminal Code Act 1995* (Cth), s 80.3.

⁷⁵ See Reuters (online), ‘Manning not guilty of aiding the enemy, faces 130+ yrs in jail on other charges’, 31 July 2013 <<http://rt.com/usa/manning-not-guilty-aiding-enemy-805/>>.

⁷⁶ *Criminal Code Act 1995* (Cth), s 80.3.

⁷⁷ *Criminal Code Act 1995* (Cth), s 80.3(1)(a). Sub-s (1)(b) provides a similar exemption where the person: ‘points out in good faith errors or defects’ in the Government, Constitution, legislation or the administration of justice ‘with a view to reforming those errors or defects’. The evidential burden to establish the defence lies with the defendant: *Criminal Code Act 1995* (Cth), ss 13.3(3), 80.3.

⁷⁸ *Criminal Code Act 1995* (Cth), s 80.3(2).

⁷⁹ *Criminal Code Act 1995* (Cth), s 80.3(2)(f).

Sheller Committee, which reviewed Australia's counter-terrorism laws in 2006,⁸⁰ the Australian Federal Police (AFP) explained that the purpose of updating the treason offence was to ensure that Australian citizens could be punished for fighting alongside al-Qaeda, either in Australia or overseas:

The enhanced treason offence is required to ensure that Australians in armed conflict with a terrorist organisation, such as Al-Qa'ida, can be dealt with under Australian law, where life imprisonment is the penalty. The extended jurisdiction of the offence means that an Australian committing treason as a member of a terrorist organisation against the Commonwealth of Australia, whether within or outside of Australia can be captured under the legislation.⁸¹

It is clear that s 80.1AA can apply to very serious conduct, such as directly assisting al-Qaeda in a foreign insurgency. However, s 80.1AA may also apply to the release of national security information which indirectly assisted an enemy. These are two very different scenarios – one involving direct participation in armed hostilities against Australia, and the other involving the leaking of classified information which indirectly assists a foreign country or organisation – and yet both could constitute the same offence under s 80.1AA and attract a maximum penalty of life imprisonment. The higher fault element of intending 'material' assistance goes some way to focusing the provision on the most serious conduct, but the fact that the conduct need only 'assist' the enemy sets a relatively low physical element for the offence.⁸² Section 80.1AA would align more closely with its intended purposes if it required both that the person intended to materially assist the enemy and that the conduct did *in fact* materially assist the enemy. Another possibility would be to specify that the person 'directly' assisted the enemy, as described in the AFP's submission to the Sheller Committee.⁸³ In the latter case, a separate, lesser offence for indirectly assisting the enemy might be required.

C *Espionage*

A third possibility is that the disclosure of national security information could constitute an act of espionage under s 91.1 of the Criminal Code. Like the other offences outlined above, the espionage offences were updated after 9/11.⁸⁴ Section 91.1 replaced a range of outdated espionage offences in Part VII of the Crimes Act (such as 'harbouring spies' and the 'illegal use of uniforms'), and raised the maximum penalty from seven to 25 years' imprisonment.⁸⁵ The main offence in s 91.1 applies where (1) a person communicates or makes available information concerning the security or defence of the Commonwealth or another country, (2) the person does so 'intending to prejudice the Commonwealth's security or defence', and (3) the information is communicated or made available to a foreign country or organisation, or to a person acting on behalf of a foreign country or organisation.⁸⁶ An equivalent offence applies where the person obtains the information 'without lawful authority' and intends to 'give an advantage to another country's security or defence'.⁸⁷ This means that the offences could apply either to a Commonwealth employee who obtained national security information in the

⁸⁰ Security Legislation Review Committee, *Report of the Security Legislation Review Committee* (June 2006).

⁸¹ Australian Federal Police, Submission No 5 to Security Legislation Review Committee, cited in PJCIS, above n 61, 40.

⁸² *Criminal Code Act 1995* (Cth), s 80.1AA(1)(e), (4)(d).

⁸³ Australian Federal Police, Submission No 5 to Security Legislation Review Committee, cited in PJCIS, above n 61, 40.

⁸⁴ *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth).

⁸⁵ Including 'harbouring spies' and the 'illegal use of uniforms': *Crimes Act 1914* (Cth), ss 81, 83A (now repealed). See *Criminal Code Amendment (Espionage and Related Matters) Bill 2002* (Cth), Explanatory Memorandum, 5-6.

⁸⁶ *Criminal Code Act 1995* (Cth), s 91.1(1).

⁸⁷ *Criminal Code Act 1995* (Cth), s 91.1(2).

course of his or her employment, or to another person who illegally obtained classified information, such as by hacking into a secure database. In the latter case, the person would not need to intend to prejudice Australia's security or defence, so long as he or she intended to advantage the security or defence of another country.⁸⁸

As with the terrorism offences,⁸⁹ the espionage offences apply where a person downloads and possesses national security information without disclosing it to others. This is because they apply not only where a person communicates the information to a foreign country or organisation, but also where the person's conduct 'is likely to result in' the information being so communicated.⁹⁰ In addition, s 91.1 provides separate offences where a person makes, obtains or copies a record of information concerning the Commonwealth's security or defence.⁹¹ The same maximum penalty of 25 years' imprisonment applies. The person must intend that the record 'will, or may, be delivered to a foreign country or organisation' or to a person acting on their behalf.⁹² In such a case, the person need not have a 'particular country, foreign organisation or person in mind' when they make, obtain or copy a record of the information.⁹³ The broad wording of these provisions suggest that the offence would be made out where a person downloaded national security information, such as that contained in the WikiLeaks material, and the person seriously contemplated the possibility of releasing that information to another country or organisation for the purposes of prejudicing Australia's security or defence.

The espionage offences also rely on a broad definition of the type of information that might be communicated. Section 90.1 defines 'information' as information 'of any kind, whether true or false and whether in material form or not', including opinions and reports of conversations.⁹⁴ Information concerning the 'security or defence' of a country includes the methods, sources, operations, capabilities and technologies of the country's intelligence and security agencies.⁹⁵ The information might be communicated 'in whole or part', including not only the information itself but also the substance or effect or a description of the information.⁹⁶ As such, a person could be charged with espionage not only for passing on classified documents containing information about national security, but also by describing their content in general terms or by offering an opinion about them. On its face, s 91.1 could therefore apply to journalists who received classified material from a source and described that material in general terms or offered an opinion about it, even if the specific contents of the material were not revealed. The offence does not require that the person communicating or making available the information is an intelligence officer or other Commonwealth employee. It would need to be proven that the journalist intended to prejudice the Commonwealth's security or defence by doing so,⁹⁷ but considering the seriousness of recent revelations in the WikiLeaks and Snowden material, it does appear that this would be a difficult requirement to satisfy.

This shows how broadly the espionage offences might operate in the context of releasing classified information, and this broad scope is clearly guided by national security concerns. The offences are designed to have a preventive effect: they are designed to stop individuals from releasing national security information in the first place, rather than punishing individuals after the fact once a foreign country has already learned secrets about Australia's security or defence. In a submission to the ALRC's inquiry on secrecy offences,

⁸⁸ *Criminal Code Act 1995* (Cth), s 91.1(2)(b)(ii).

⁸⁹ *Criminal Code Act 1995* (Cth), ss 101.4, 101.5.

⁹⁰ *Criminal Code Act 1995* (Cth), s 91.1(1)(c), (2)(c).

⁹¹ *Criminal Code Act 1995* (Cth), s 91.1(3)-(4).

⁹² *Criminal Code Act 1995* (Cth), s 91.1(3)(b)(i), (4)(b)(ii) (or person acting on their behalf). Sub-s (4) is the equivalent offence where the information is obtained 'without lawful authority': *Criminal Code Act 1995* (Cth), s 91.1(4)(b)(i).

⁹³ *Criminal Code Act 1995* (Cth), s 91.1(5).

⁹⁴ *Criminal Code Act 1995* (Cth), s 90.1(1).

⁹⁵ *Criminal Code Act 1995* (Cth), s 90.1(1).

⁹⁶ *Criminal Code Act 1995* (Cth), s 90.1(2)(a).

⁹⁷ *Criminal Code Act 1995* (Cth), s 91.1(1)(b).

representatives from the Australian intelligence agencies explained the rationale of having broadly drafted espionage offences which encompassed the copying or recording of information:

This formulation provides scope to prevent espionage activities or possible unauthorised disclosures of national security-classified information that would not be possible if the provision was limited to the disclosure itself. Without the current formulation, a person could only be prosecuted after they had committed the act of espionage or unauthorised disclosure of information. By that time, any damage to national security would have occurred.⁹⁸

These are important considerations, but it is also a serious concern that the legislation imposes the same penalty on those who intentionally disclose national security information to prejudice security and defence and those who possess national security information without disclosing it. If the espionage offences for merely possessing classified information are retained, then the penalties for possession and retention of information should be significantly lower than that for disclosure. Some protection against the misuse of the current provisions is provided by s 93.1, which requires prior consent from the Attorney-General for the prosecution of any espionage offence,⁹⁹ although it is doubtful whether this provides much protection in a context where it would be the interests of the executive branch of government being harmed.

III SECRECY OFFENCES

This section details two categories of secrecy offences which apply to Commonwealth officers (and, in certain circumstances, other individuals). First, ss 70 and 79 of the Crimes Act set out general secrecy offences that apply to Commonwealth officers and others. Secondly, the *Intelligence Services Act 2001* (Cth) and the *Australian Security Intelligence Organisation Act 1979* (Cth) set out offences where employees of intelligence agencies release information obtained by virtue of their employment.

A *Secrecy Offences in the Crimes Act*

1. Section 70

Section 70 of the Crimes Act makes it an offence for current or former Commonwealth officers to disclose any facts they have learned or documents they have obtained by virtue of being a Commonwealth officer and which it is their 'duty not to disclose'.¹⁰⁰ The maximum penalty is two years' imprisonment and there is an exception where the person is authorised to publish or communicate the information.¹⁰¹ A 'Commonwealth officer' is defined as a person who is appointed or engaged under the *Public Service Act 1999* (Cth), the Commissioners and employees of the Australian Federal Police and, for the purposes of s 70, any other person who 'performs services for or on behalf of' the Commonwealth government.¹⁰² A version of s 70 was included in the original Crimes Act but this was replaced in 1960 to extend the prohibition to former Commonwealth officers.¹⁰³ Section 70 has been used to prosecute employees from a range of government departments, including

⁹⁸ Australian Law Reform Commission (ALRC), *Secrecy Laws and Open Government in Australia* (Report 112, December 2009) 324 [9.52] ('*Secrecy Laws*').

⁹⁹ *Criminal Code Act 1995* (Cth), s 93.1.

¹⁰⁰ *Crimes Act 1914* (Cth), s 70(1),(2).

¹⁰¹ *Crimes Act 1914* (Cth), s 70(1),(2) ('except to some person to whom he or she is authorized to publish or communicate it').

¹⁰² *Crimes Act 1914* (Cth), s 3.

¹⁰³ ALRC, *Secrecy Laws*, above n 98, 43, 87.

employees of Centrelink and the Australian Tax Office.¹⁰⁴ The offence has proved less relevant in the national security context where prosecutions have been instituted under the espionage offences and s 79 of the Crimes Act,¹⁰⁵ although in one prominent case a customs officer was found guilty under s 70 for disclosing the contents of two secret reports detailing lax security procedures at Sydney airport.¹⁰⁶

As the ALRC has noted, the duty not to disclose the information is not contained within s 70 itself but can be sourced elsewhere.¹⁰⁷ Potential common law sources include the duty of confidentiality, as considered in *Commonwealth v Fairfax*,¹⁰⁸ a duty of loyalty and fidelity arising from the contract of employment, and potential fiduciary obligations if an employee is placed in a special position of trust and confidence.¹⁰⁹ Employees of the Australian Public Service (APS) are also placed under statutory duties according to the *Public Service Act 1999* (Cth) ('Public Service Act') and its regulations.¹¹⁰ Section 13 of the Public Service Act creates the APS Code of Conduct, which includes such requirements that employees must 'maintain appropriate confidentiality' and 'not make improper use of ... inside information'.¹¹¹ In particular, reg 2.1(3) of the *Public Service Regulations 1999* (Cth) ('APS Regulations') specifies that APS employees must not disclose information where this would prejudice the effective working of government or the development of policy:

An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs¹¹²

The extent to which these duties apply to contracted service providers is less clear. Given that s 3 of the Crimes Act defines Commonwealth officers to include any person who 'performs services for or on behalf of' the government,¹¹³ it seems that s 70 could extend to a scenario, such as the Snowden affair, where a government contractor leaked classified information that they obtained by virtue of their employment contract. To clarify this issue, the ALRC recommended that the definition of Commonwealth officer in s 3 should explicitly reference 'contracted service providers' as well as the 'officers or employees of a contracted service provider'.¹¹⁴ The ALRC also emphasised the importance of including confidentiality provisions in employment contracts so that contractors are aware of their secrecy obligations.¹¹⁵ Overall, the ALRC recognised the importance of extending the same restrictions, including the criminal law where appropriate, to government contractors:

The reality [is] that contracted service providers are increasingly involved in the business of government, including the provision of government services. They collect and generate large amounts of information, which would clearly be Commonwealth information if it were collected or generated by an Australian Government agency, and has the potential to cause the same kind and degree of harm if disclosed without

¹⁰⁴ Ibid 87.

¹⁰⁵ See, eg, *R v Lappas* (2003) 152 ACTR 7; *R v Lappas & Dowling* [2001] ACTSC 115; *Grant v Headland* (1977) 17 ACTR 29.

¹⁰⁶ *R v Kessing* (2008) 73 NSWLR 22.

¹⁰⁷ ALRC, *Secrecy Laws*, above n 98, 88-89, 119-20.

¹⁰⁸ (1980) 147 CLR 39 ('*Fairfax*').

¹⁰⁹ See ALRC, *Secrecy Laws*, above n 98, 65-69. See, eg, *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [117].

¹¹⁰ *Public Service Regulations 1999* (Cth).

¹¹¹ *Public Service Act 1999* (Cth), s 13 (6),(10).

¹¹² *Public Service Regulations 1999* (Cth), reg 2.1.

¹¹³ *Crimes Act 1914* (Cth), s 3.

¹¹⁴ ALRC, *Secrecy Laws*, above n 98, 9-10 (Recommendation 6-1).

¹¹⁵ Ibid 16 (Recommendation 13-3), 480 [13.103]-[13.104].

authority. This information should be protected in the same way by the criminal law, whether it happens to be held by the public or private sector.¹¹⁶

Equally, however, the ALRC recommended that government contracts ‘should expressly permit the disclosure of confidential Commonwealth information where this would amount to public interest disclosure’.¹¹⁷ The availability of whistleblower protections under public interest disclosure legislation is considered in Part IV.

The important question, as raised by the ALRC in its inquiry into Commonwealth secrecy offences,¹¹⁸ is whether breach of these common law and statutory duties should give rise to the intervention of the criminal law as found in s 70. Because s 70 fails to specify the type of information that is prohibited from disclosure, or an express requirement that the person intends to cause harm, s 70 could apply on its face to the ‘disclosure of any information regardless of its nature of sensitivity’.¹¹⁹ In this regard, the ALRC believed that there were ‘real concerns about the way that s 70 of the Crimes Act is framed’.¹²⁰ The ALRC recommended that a new general secrecy offence should be drafted, and that this offence should be confined to specified categories which reflect an ‘essential public interest’.¹²¹ By considering various exceptions to the *Freedom of Information Act 1982* (Cth), the ALRC recommended that the general secrecy offence should be limited to cases where an unauthorised disclosure did, or was likely to, or was intended to:

- (a) damage the security, defence or international relations of the Commonwealth;
- (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;
- (c) endanger the life or physical safety of any person; or
- (d) prejudice the protection of public safety.¹²²

Such an amendment would represent a significant improvement on the current wording of s 70, which imposes criminal liability for acts that are merely prejudicial to the effective working of government.¹²³ If such an amendment were adopted, there would still be remedies available to government departments whose employees leaked information that impacted negatively on the development of policy: a government department would still be able to suspend the person, terminate their employment, or seek civil remedies for breach of contract or a duty of confidentiality.¹²⁴ However, the wording suggested by the ALRC would restrict the application of the offence to those cases which are sufficiently serious to warrant the intervention of the criminal law.

¹¹⁶ Ibid 190 [6.25].

¹¹⁷ Ibid 478 [13.95].

¹¹⁸ Ibid 89.

¹¹⁹ Ibid 89 [3.100]. In *Commissioner of Taxation v Swiss Aluminium Australia Ltd* (1986) 10 FCR 321, Bowen CJ (at 325) described the content as ‘virtually irrelevant’. In *Deacon v Australian Capital Territory* [2001] ACTSC 8, Higgins J (at [87]-[88]) took a different view, arguing that the public interest was a relevant concern: see *ibid* 89-90.

¹²⁰ ALRC, *Secrecy Laws*, above n 98, 122, [4.100].

¹²¹ Ibid 9 (Recommendation 5-1), 138, 160, 324. The duty not to disclose information would be confined to these specified categories and included within the offence itself, rather than being sourced in common law and statutory duties: *ibid* 123 [4.102].

¹²² Ibid 9 (Recommendation 5-1). The ALRC (at *ibid*, 161-181) considered that disclosures of information in the following categories should not be criminalised if they do not also fall under one of the public interest categories listed above: Cabinet documents, information communicated in confidence by a foreign government, information communicated in confidence by a State or Territory government, material obtained in breach of the duty of confidentiality, personal and commercial information, information affecting the financial or property interests of the Commonwealth, or information affecting the economy.

¹²³ Through the duty imposed by *Public Service Regulations 1999* (Cth), reg 2.1.

¹²⁴ See, eg, *Public Service Act 1999* (Cth), ss 28 (suspension), 29 (termination of employment).

The broad drafting of s 70 raises the possibility of a constitutional challenge on the grounds that it infringes the implied freedom of political communication, although it appears unlikely such a challenge would succeed. The relevant test, as adopted by the High Court in *Lange v Australian Broadcasting Corporation*¹²⁵ and later modified in *Coleman v Power*,¹²⁶ has two limbs. First, the court must determine whether the law effectively burdens communication about government and political matters, either in its terms, operation or effect.¹²⁷ Secondly, the court must determine whether the law is reasonably appropriate and adapted to serving a legitimate end in a manner that is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government.¹²⁸ In *Levy v Victoria*,¹²⁹ the High Court emphasised that the freedom was not absolute, and extended only to ‘what is necessary to the effective working of the *Constitution*’s system of representative and responsible government’.¹³⁰

In *Bennett v President, Human Rights and Equal Opportunity Commission*,¹³¹ the Federal Court upheld a challenge to a previous version of reg 2.1 on the grounds that it infringed the implied freedom. Regulation 7(13) previously provided that an APS employee must not disclose ‘any information about public business or anything of which the employee has official knowledge’.¹³² Finn J held that reg 7(13) infringed the implied freedom because it did not specify the types of information to which the duty applied or the consequences of disclosure.¹³³ As a result of *Bennett*, reg 7(13) was replaced with the current reg 2.1, which, as above, places a duty on APS employees not to disclose information where it is ‘reasonably foreseeable that the disclosure could be prejudicial to the effective working of government’.¹³⁴ It is doubtful whether this wording remedies the failure of reg 7(13) to specify the types of information or the consequences of disclosure, but in 2008 the ACT Supreme Court nonetheless upheld the constitutionality of reg 2.1 on this ground.¹³⁵ Even if s 70 were to survive constitutional challenge in other courts, it raises an important question about the circumstances in which it is appropriate to impose criminal sanctions for releasing sensitive government information. It is not a question of whether sanctions should be imposed on an individual who releases information in circumstances that prejudice government or the development of policy, but whether civil and administrative remedies provide a more appropriate avenue than the criminal law.

2. Section 79

Section 79 of the Crimes Act sets out multiple offences where a person communicates official secrets.¹³⁶ A version of s 79 was included in the original Crimes Act and was based on a similar provision in the *Official Secrets Act 1911* (UK).¹³⁷ Few prosecutions have been instituted under s 79, although a key example is *Lappas*,¹³⁸ where an employee of the Defence Intelligence Organisation (DIO) was charged under s 79 and a previous version of the

¹²⁵ (1997) 189 CLR 520 (*‘Lange’*).

¹²⁶ (2004) 220 CLR 1.

¹²⁷ *Lange* (1997) 189 CLR 520, 567; *Coleman v Power* (2004) 220 CLR 1, 50 (McHugh J).

¹²⁸ *Lange* (1997) 189 CLR 520, 567; *Coleman v Power* (2004) 220 CLR 1, 50 (McHugh J). The latter judgment added the words ‘in a manner’ to the second limb.

¹²⁹ (1997) 189 CLR 579

¹³⁰ *Levy v Victoria* (1997) 189 CLR 579, 595 (Brennan CJ).

¹³¹ (2003) 134 FCR 334.

¹³² *Public Service Regulations 1999* (Cth), reg 7(13) (now repealed). See ALRC, *Secrecy Laws*, above n 98, 55-56.

¹³³ *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [98]–[99], [101]. Finn J described the regulation (at [98]) as imposing an ‘almost impossible demand’ on Commonwealth employees. See ALRC, *Secrecy Laws*, 56.

¹³⁴ *Public Service Regulations 1999* (Cth), reg 2.1. See ALRC, *Secrecy Laws*, above n 98, 56 [2.60].

¹³⁵ *R v Goreng Goreng* [2008] ACTSC 74.

¹³⁶ *Crimes Act 1914* (Cth), s 79.

¹³⁷ ALRC, *Secrecy Laws*, above n 98, 93 [3.115].

¹³⁸ *R v Lappas* (2003) 152 ACTR 7. See ALRC, *Secrecy Laws*, above n 98, 94.

espionage offence in s 91.1 of the Criminal Code. Lappas received 2 years' imprisonment for passing classified intelligence documents to a prostitute so that she could sell them to a foreign country.¹³⁹

Section 79 overlaps to some degree with s 70, but applies beyond Commonwealth officers to other categories of people, and contains a higher maximum penalty (up to 7 years' imprisonment) where there is an intention to cause harm. The offence applies to 'prescribed information', being a 'sketch, plan, photograph, model, cipher, note, document, or article' that has been received in one of three possible scenarios.¹⁴⁰ First, prescribed information is information received in contravention of s 79 or the espionage offence in the Criminal Code.¹⁴¹ Secondly, prescribed information is information entrusted to the person by a Commonwealth officer, or which the person has obtained by virtue of his or her position as a Commonwealth officer.¹⁴² This limb also refers to individuals who hold contracts made on behalf of the Commonwealth, suggesting that the offences could equally apply to contracted service providers.¹⁴³ Thirdly, prescribed information is information relating to a prohibited place (or anything in a prohibited place) and the person 'ought to know' by the circumstances in which he or she received the information that it should not be communicated to a person other than those authorised to see it.¹⁴⁴ The definition of 'prohibited place' includes defence premises, ships, aircraft and any other infrastructure that is proclaimed to be a prohibited place because its 'destruction or obstruction ... would be useful to an enemy power'.¹⁴⁵

Sub-section (2) of s 79 provides a maximum penalty of 7 years' imprisonment where the person communicates the information to another person 'with the intention of prejudicing the security or defence of the Commonwealth'.¹⁴⁶ While this is a significantly higher penalty than that imposed by s 70,¹⁴⁷ the inclusion of an express intention requirement is a notable improvement. It restricts the application of the 7-year penalty to disclosures of information that are intended to cause harm. By contrast, sub-s (3) provides a maximum penalty of 2 years' imprisonment where there is no intention to prejudice security or defence.¹⁴⁸ In this respect, s 79(3) raises a similar issue to s 70 about whether the criminal law is an appropriate remedy in cases where the person discloses sensitive information but does not intend to cause harm.¹⁴⁹

For both these offences under s 79, there is an exemption where disclosure would be 'in the interest of the Commonwealth'.¹⁵⁰ As with the good faith defence to the treason offences above, it is likely that this would prove a difficult issue to resolve given the wide variety of views on whether recent disclosures of national security information were made in the public interest. However, considering previous court decisions on public interest disclosure,¹⁵¹ it seems unlikely that a court would find a disclosure to be in the public interest if it revealed the contents of any intelligence reports or similar documents. It is possible that protection might be available if the person disclosed the nature of classified documents in very general terms to promote discussion on current affairs without revealing any details or

¹³⁹ Transcript of Proceedings, *R v Dowling* (Supreme Court of the Australian Capital Territory, Gray J, 9 May 2003). See ALRC, *Secrecy Laws*, above n 98, 94.

¹⁴⁰ *Crimes Act 1914* (Cth), s 79(1).

¹⁴¹ *Crimes Act 1914* (Cth), s 79(1)(a).

¹⁴² *Crimes Act 1914* (Cth), s 79(1)(b).

¹⁴³ *Crimes Act 1914* (Cth), s 79(1)(b)(iii).

¹⁴⁴ *Crimes Act 1914* (Cth), s 79(1)(c).

¹⁴⁵ *Crimes Act 1914* (Cth), s 80.

¹⁴⁶ *Crimes Act 1914* (Cth), s 79(2).

¹⁴⁷ *Crimes Act 1914* (Cth), s 70 (maximum penalty 2 years' imprisonment).

¹⁴⁸ *Crimes Act 1914* (Cth), s 79(3).

¹⁴⁹ ALRC, *Secrecy Laws*, 117 [4.76], 138 [4.157].

¹⁵⁰ *Crimes Act 1914* (Cth), s 79(2)(a)(ii), (3)(b).

¹⁵¹ See, eg, *Fairfax* (1980) 147 CLR 39; *R v Kessing* (2008) 73 NSWLR 22 ('Kessing'). In *Fairfax*, Mason CJ held (at 52) that disclosure would be against the public interest if 'it appears that ... national security, relations with foreign countries or the ordinary business of government will be prejudiced'. However, he noted (at 52) that this can often be 'difficult to decide'.

particulars about their content.¹⁵² For example, in *R v Kessing*, a customs officer was found guilty under s 70 of the Crimes Act for revealing the contents of two classified reports that revealed lax airport security procedures.¹⁵³ Kessing was considered a hero by many because his acts led to a major review of airport security.¹⁵⁴ The court suggested that Kessing might have been protected if he had revealed that the reports had been inadequately addressed by customs management, without revealing the substance of the reports.¹⁵⁵

Like the terrorism and espionage offences, s 79 applies not only to the disclosure of information but also to its possession. A maximum penalty of 7 years' imprisonment applies where the person retains prescribed information 'when he or she has no right to retain it', or fails to dispose of the information in accordance with an order to do so, and does so with the intention of prejudicing the Commonwealth's security or defence.¹⁵⁶ An offence also applies where the information is retained without an intention to prejudice security or defence, although in that case a significantly lower penalty (of 6 months' imprisonment) applies.¹⁵⁷ The latter offence also applies where the person fails to take reasonable care of the information.¹⁵⁸

A key issue raised by s 79, which is not contemplated by any of the other offences detailed above, is the idea of 'subsequent disclosures'. A subsequent disclosure occurs where one person (Person A) discloses information to a second person (Person B) in circumstances that would amount to a criminal offence, such as espionage, and then Person B subsequently discloses that information to a third person (Person C) or to the public at large. This describes the WikiLeaks scenario, where Manning (Person A) communicated information to Assange (Person B), who released the information to journalists (Persons C, D, etc) and the general population.

Given the contemporary relevance of the subsequent disclosure scenario it is important that legislation should address it, although the scope of s 79 is strikingly broad in this regard. If Person B communicates the information to Person C, he or she could be prosecuted under s 79 according to the offences outlined above.¹⁵⁹ However, s 79 also extends to circumstances where Person B has received information from Person A, but has not yet communicated that information to Person C. Indeed, in such a case, s 79 applies the same penalty to Person B as to Person A, even where Person B has not yet formed an intention to communicate the information to Person C. This offence is made available through sub-s (5), which provides a maximum penalty of 7 years' imprisonment where a person receives prescribed information in circumstances contrary to s 91.1 of the Criminal Code (espionage) or sub-s (2) of s 79 (i.e. where Person A intends to prejudice security or defence).¹⁶⁰ Alternatively, sub-s (6) provides a maximum penalty of 2 years' imprisonment where a

¹⁵² See, eg, *Fairfax* (1980) 147 CLR 39, 52: 'The court will not prevent the publication of information which merely throws light on the past workings of government, even if it be not public property, so long as it does not prejudice the community in other respects. Then disclosure will itself serve the public interest in keeping the community informed and in promoting discussion of public affairs' (Mason CJ).

¹⁵³ *R v Kessing* (2008) 73 NSWLR 22.

¹⁵⁴ ALRC, *Secrecy Laws*, 58 [2.63]; Paul Latimer and A J Brown, 'Whistleblower Laws: International Best Practice' (2008) 31(3) *University of New South Wales Law Journal* 766, 783.

¹⁵⁵ See *Kessing* (2008) 73 NSWLR 22, 30 [33]. On appeal, the court considered that it was a matter of degree when a report would be 'communicated' to another person, but it held that defendant had communicated the documents in question because journalists working for *The Australian* had drawn on 'material portions' of the reports. The trial judge had earlier suggested that it would be in the public interest 'to expose the inadequacy of an agency or government manifested by its failure to respond in a timely fashion to an internal report generated at the lower levels of the organisation': see ALRC, *Secrecy Laws*, above n 98, 57-58.

¹⁵⁶ *Crimes Act 1914* (Cth), s 79(2)(b)-(c).

¹⁵⁷ *Crimes Act 1914* (Cth), s 79(4)(a)-(b).

¹⁵⁸ *Crimes Act 1914* (Cth), s 79(4)(c).

¹⁵⁹ *Crimes Act 1914* (Cth), s 79(1)(a) defines prescribed information as information received in contravention of this part of in contravention of espionage offence in s 91.1.

¹⁶⁰ *Crimes Act 1914* (Cth), s 79(5).

person receives prescribed information in circumstances contrary to sub-s (3) of s 79 (i.e. where Person A does not intend to prejudice security or defence).¹⁶¹ In either case, Person B must have reasonable grounds for believing that the information was received in contravention of the relevant offence.¹⁶² It is a defence if Person B received the prescribed information in circumstances ‘contrary to his or her desire’, although the burden to prove this lies with the defendant.¹⁶³ This means that journalists, for example, could receive the same penalty for receiving prescribed information as the person who communicated that information to them, even where the journalist has not yet formed an intention to publish or otherwise communicate the information to another person. As with the terrorism and espionage offences, which provide serious criminal penalties for possessing information, these offences remove a window of moral opportunity in which a journalist or other person might receive national security information from another person and then decide not to publish that information.

To clarify the confusion surrounding subsequent disclosures in s 79, and to ensure that the ‘mere receipt or possession’ of information does not receive the same penalty as an initial disclosure,¹⁶⁴ the ALRC recommended that a separate offence for subsequent disclosures be created.¹⁶⁵ For the same penalty as the main offence to apply, the subsequent disclosure offence should require that Person B communicated the information to Person C and had the same intention as Person A (to prejudice the Commonwealth’s security or defence), or that Person B was reckless as to the possibility that disclosing the information to Person C would cause such harm.¹⁶⁶ Given the importance of subsequent disclosures to recent events, a separate offence along these lines would be a valuable amendment to help clarify the law in this area.

B *Offences for Employees of Intelligence Organisations*

In addition to the general secrecy offences outlined above, specific secrecy offences apply to the employees of intelligence agencies who release information obtained in the course of their employment. Sections 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth) set out offences for the employees of the Australian Secret Intelligence Service (ASIS), Defence Imagery and Geospatial Organisation (DIGO) and the Australian Signals Directorate (ASD) respectively.¹⁶⁷ Section 39 featured in public debate after a former ASIS officer alleged that the Howard government spied on the Timor-Leste government to advantage commercial negotiations.¹⁶⁸ Each of the three offences provides a maximum of 2 years’ imprisonment where an employee of the intelligence agency ‘communicates any information or matter that was prepared by or on behalf of [the agency] in connection with its functions, or relates to the performance by [the agency] of its functions’.¹⁶⁹ An equivalent offence for employees of the Australian Security Intelligence Organisation (ASIO) can be found in s 18 of the *Australian Security Intelligence Organisation Act 1979* (Cth).¹⁷⁰

Like s 70 of the Crimes Act,¹⁷¹ these offences apply regardless of the type of information communicated by the person or any intention on behalf of the person to prejudice security or defence. However, this may be less problematic in the intelligence context where the communication of *any* classified information could harm national security. In its inquiry

¹⁶¹ *Crimes Act 1914* (Cth), s 79(6).

¹⁶² *Crimes Act 1914* (Cth), s 79(5)-(6).

¹⁶³ *Crimes Act 1914* (Cth), s 79(5)-(6).

¹⁶⁴ ALRC, *Secrecy Laws*, above n 98, 203 [6.82].

¹⁶⁵ Ibid 10-11 (Recommendations 6-6, 6-7), 13 (Recommendation 9-7).

¹⁶⁶ See ibid 10-11 (Recommendations 6-6, 6-7), 13 (Recommendation 9-7), 341-342.

¹⁶⁷ *Intelligence Services Act 2001* (Cth), ss 39, 39A, 40.

¹⁶⁸ See, Tom Allard, ‘Australia accused of playing dirty in battle with East Timor over oil and gas reserves’, *Sydney Morning Herald*, 28 December 2013.

¹⁶⁹ *Intelligence Services Act 2001* (Cth), ss 39(1)(a), 39A(1)(a), 40A(1)(a).

¹⁷⁰ *Australian Security Intelligence Organisation Act 1979* (Cth), s 18(2).

¹⁷¹ *Crimes Act 1914* (Cth), s 70.

into secrecy offences in Australia, the ALRC accepted the ‘mosaic theory’ put forward in submissions from representatives of the Australian intelligence agencies (who are collectively referred to as the ‘Australian Intelligence Community’ or ‘AIC’).¹⁷² The mosaic theory suggests that any one piece of intelligence on its own might not be very useful to a foreign country or terrorist organisation, but these small pieces of information can be combined with other pieces to create a relatively comprehensive picture of the agencies’ sources and methods.¹⁷³ As such, the ALRC did not feel that the offences should include an express requirement that the officer intended to cause harm by his or her conduct:

The ‘mosaic approach’ argument put by the AIC—the argument that isolated disclosures of seemingly innocuous information, when combined with other information, together disclose sensitive information that could cause harm to national security—suggests that a secrecy offence that included an express requirement of harm would be insufficient to protect against harm to national security.¹⁷⁴

The ALRC supported the current wording of the intelligence offences, which extend both to government contractors and any person entering into an ‘agreement or arrangement’ with an intelligence agency,¹⁷⁵ by arguing that it is ‘appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive intelligence information’.¹⁷⁶ However, in considering the scope of a general secrecy offence to replace ss 70 and 79 of the Crimes Act, the ALRC recommended that such an offence should extend only to government contractors and not to any person who enters into an ‘agreement or arrangement’ with a government department.¹⁷⁷ This raises an important question about the limits to be placed on the criminal law with regard to *who releases* national security information. On the one hand, given that the purpose of these provisions is to prevent the release of information that can harm national security, the formal employment status of the person who releases that information should be irrelevant. On the other hand, it is arguable that those entering into an ‘arrangement or agreement’ with the AIC would not understand the special obligations surrounding the handling of intelligence to the same degree as intelligence officers and those contracted to work for the intelligence agencies. To this extent, the intelligence offences may go too far in applying a criminal penalty to any person who comes across and discloses classified information.

The intelligence legislation also includes offences for making public the identities of ASIS and ASIO officers.¹⁷⁸ These offences could apply not only to individuals who are employed by or enter into an arrangement with an intelligence agency, but also to any person who reveals the identity of an intelligence officer. For example, if an intelligence officer leaked information to a journalist and the journalist learned of the true identity of that officer, the journalist could be prosecuted for publishing that information. The maximum penalty is imprisonment for 1 year.¹⁷⁹

IV WHISTLEBLOWER PROTECTIONS

¹⁷² See ALRC, *Secrecy Laws*, above n 98, 289.

¹⁷³ *Ibid.*

¹⁷⁴ *Ibid* 289 [8.63].

¹⁷⁵ *Intelligence Services Act 2001* (Cth), ss 39(1)(b)(ii)-(iii), 39A(1)(b)(ii)-(iii), 40 (1)(b)(ii)-(iii); *Australian Security Intelligence Organisation Act 1979* (Cth), s 18(2).

¹⁷⁶ *Ibid* 289 [8.62].

¹⁷⁷ ALRC, *Secrecy Laws*, above n 98, 190.

¹⁷⁸ *Intelligence Services Act 2001* (Cth), s 41; *Australian Security Intelligence Organisation Act 1979* (Cth), s 92.

¹⁷⁹ *Intelligence Services Act 2001* (Cth), s 41(1); *Australian Security Intelligence Organisation Act 1979* (Cth), s 92(1).

This section considers whether individuals who commit the above offences for disclosing national security information would be protected from criminal liability by the *Public Interest Disclosure Act 2013* (Cth) ('PID Act'). The PID Act came into force on 15 January 2014. It was a product of the Rudd government's election commitments, which led to an inquiry into existing whistleblower protections by the House of Representatives Standing Committee on Legal and Constitutional Affairs.¹⁸⁰ The move was aided by former intelligence whistleblower Andrew Wilkie, who introduced his own private member's Bill alongside the main legislation.¹⁸¹

The term 'whistleblower' is not used in the PID Act but in common usage it refers to individuals who by speak out about wrongdoing or illegal conduct by an organisation or its members.¹⁸² Whistleblowing should be distinguished from 'leaking', where a person 'covertly provides information directly to the media, "to seek support and vindication in the court of public opinion"'.¹⁸³ As a result of its inquiry, the Legal and Constitutional Affairs Committee recommended that a comprehensive scheme for protecting whistleblowers should be enacted at the national level 'as a matter of priority'.¹⁸⁴ The Committee emphasised the importance of whistleblowing in contributing to the integrity and accountability of government:

Public interest disclosure legislation has an important role in protecting the interests of those who speak out about what they consider to be wrongdoing in the workplace, encouraging responsive action by public agencies, strengthening public integrity and accountability systems and supporting the operation of government ... Facilitating public interest disclosures is part of a broader public integrity framework that is considered to be an essential feature of modern accountable and transparent democracies.¹⁸⁵

The PID Act establishes a whistleblowing scheme by protecting public officials who disclose information according to a specified process.¹⁸⁶ The stated objectives of the scheme are to 'promote the integrity and accountability of the Commonwealth public sector' and to ensure that 'public officials who make public interest disclosures are supported and protected from adverse consequences'.¹⁸⁷ The definition of 'public official' extends beyond APS employees to other individuals including any person employed by the Commonwealth government and any person exercising powers under Commonwealth legislation.¹⁸⁸ The definition also includes contracted service providers,¹⁸⁹ meaning that the protections could be available in a similar scenario to the Snowden affair, provided that the other requirements below were also satisfied.

The starting point for the PID scheme is s 10, which provides that public officials who make public interest disclosures are protected from civil, criminal and administrative

¹⁸⁰ House of Representatives Standing Committee on Legal and Constitutional Affairs ('Standing Committee'), *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (February 2009). See also A J Brown and Paul Latimer, 'Symbols or Substance? Priorities for the Reform of Australian Public Interest Disclosure Legislation' (2008) 17(1) *Griffith Law Review* 223.

¹⁸¹ Public Interest Disclosure (Whistleblower Protection) Bill 2012 (Cth). See Commonwealth, *Parliamentary Debates*, House of Representatives, 29 October 2012, 14-15.

¹⁸² See *ibid* 24 [2.16].

¹⁸³ *Ibid* 24 [2.18].

¹⁸⁴ *Ibid* xix (Recommendation 1), 10 [1.38], 32 [2.50].

¹⁸⁵ *Ibid* 1 [1.3]-[1.4].

¹⁸⁶ The PID Act repealed s 16 of the Public Service Act, which previously provided limited protections for APS employees who disclosed breaches of the APS Code of Conduct: *Public Service Act 1999* (Cth), s 16 (now repealed). See *ibid* 5 [1.19].

¹⁸⁷ *Public Interest Disclosure Act 2013* (Cth), s 6(a),(c). Its other objectives are 'encouraging and facilitating the making of public interest disclosures' (s 6(b)) and 'ensuring that disclosures by public officials are properly investigated and dealt with' (s 6(d)).

¹⁸⁸ *Public Interest Disclosure Act 2013* (Cth), s 69, Items 2, 13, 17.

¹⁸⁹ *Public Interest Disclosure Act 2013* (Cth), s 69, Items 15-16. See also s 30, which specifies the definition of a contracted service provider in greater detail.

liability, including disciplinary action by the department in which they are employed.¹⁹⁰ This protection is not available where the disclosure contravenes a ‘designated publication restriction’ such as a suppression order issued by a court.¹⁹¹ While the protection in s 10 is broadly worded, there are two key requirements which public officials must satisfy in order to be immune from liability.

The first is that the information being disclosed must satisfy the definition of ‘disclosable conduct’.¹⁹² Immunity is provided only if the information falls within a range of specified categories. These categories include information about conduct which:

- Contravenes a law of the Commonwealth, a State or a Territory
- Perverts the course of justice or involves corruption of any kind
- Constitutes maladministration (including conduct that is based on improper motives; is unreasonable, unjust or oppressive; or is negligent)
- Is an abuse of public trust
- Results in the wastage of public money or property
- Unreasonably results in a danger to the health or safety of one or more persons
- Results in an increased risk of danger to the environment¹⁹³

The PID Act states that the information will not qualify as disclosable conduct if it relates only to a policy with which a person disagrees.¹⁹⁴ In the national security context, this would mean, for example, that a person could disclose the fact that Australia’s foreign intelligence services were acting contrary to their statutory mandate – such as by conducting illegal surveillance of Australian citizens.¹⁹⁵ However, the person could not disclose information about the conduct of intelligence agencies with which the person simply disagreed as a matter of moral principle.¹⁹⁶

In addition, the PID Act specifies that the person must not disclose any more information than is reasonably necessary to identify one or more instances of wrongdoing.¹⁹⁷ This means that a person would not be protected from liability if he or she disclosed an entire database of intelligence material that contained specific instances of wrongdoing. For example, the WikiLeaks material undoubtedly exposed some instances of serious wrongdoing, such as American soldiers killing civilians in Iraq and Afghanistan.¹⁹⁸ However, this material also included a large database of diplomatic cables that would not qualify under the categories above.¹⁹⁹ As such, a similar scenario in Australia would be protected under the PID Act only if the person limited disclosure to information that qualified under one of the categories specified above. As detailed below, there are additional considerations in the intelligence context which further limit the scope for public interest disclosures of this kind.

The second key requirement is that the process by which the public official discloses the information must satisfy the definition of a ‘public interest disclosure’.²⁰⁰ A public interest disclosure may be made orally or in writing, it may be made anonymously, and it may be

¹⁹⁰ *Public Interest Disclosure Act 2013* (Cth), s 10.

¹⁹¹ *Public Interest Disclosure Act 2013* (Cth), s 11A.

¹⁹² *Public Interest Disclosure Act 2013* (Cth), s 29.

¹⁹³ See *Public Interest Disclosure Act 2013* (Cth), s 29.

¹⁹⁴ *Public Interest Disclosure Act 2013* (Cth), s 31.

¹⁹⁵ See, eg, *Intelligence Services Act 2001* (Cth) s 6(1)(a), which provides that the functions of the Australian Secret Intelligence Service (ASIS) are ‘to obtain ... intelligence about the capabilities, intentions or activities of people or organisations outside Australia’.

¹⁹⁶ *Public Interest Disclosure Act 2013* (Cth), s 31.

¹⁹⁷ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Items 2(f), 3(b).

¹⁹⁸ The key example is the video showing US troops in an Apache helicopter killing civilians in Iraq: see Leigh and Harding, above n 1, 65-71; Chris McGreal, ‘Wikileaks reveals video showing US air crew shooting down Iraqi civilians’, *The Guardian* (London), 5 April 2010.

¹⁹⁹ See Leigh and Harding, above n 1, 135-144.

²⁰⁰ *Public Interest Disclosure Act 2013* (Cth), s 26.

made without the person asserting that they are seeking immunity from liability under the PID Act.²⁰¹ However, the information cannot simply be leaked to the media or the public at large. The first step is that the person needs to disclose the information internally – that is, to the person’s supervisor or to an authorised recipient within the organisation.²⁰² Alternatively, the information may be communicated where appropriate to the Ombudsman, the Inspector-General for Intelligence and Security (IGIS), or another investigative agency specified under the PID Regulations.²⁰³ Only when the person reasonably believes that this internal review process has been inadequate can the information be released externally to a person outside the organisation.²⁰⁴ Even then, the information will only have been validly disclosed if its disclosure is not contrary to the public interest.²⁰⁵ In weighing up whether the disclosure is in the public interest, the court may have regard to a range of factors, including whether the disclosure would promote integrity and accountability; the extent to which the disclosure would address serious wrongdoing; and whether the disclosure could cause damage to security, defence, international relations, or relations between the Commonwealth and a State or Territory government.²⁰⁶ The only circumstance in which a person can bypass this process is if he or she believes on reasonable grounds that there is a ‘substantial and imminent danger to the health and safety of one or more persons or to the environment’.²⁰⁷ In such a case, there must also be ‘exceptional circumstances’ to justify why the person did not first make an internal disclosure to a supervisor or investigative agency.²⁰⁸ The person may also release the information to an Australian legal practitioner, but only for the purpose of obtaining advice about making a disclosure under the Act.²⁰⁹

These requirements under the PID Act will be particularly difficult to satisfy where the information being disclosed relates to the conduct of intelligence agencies. This is because the PID Act places special restrictions on information connected with intelligence agencies due to the greater risk involved to national security.²¹⁰ There are two exemptions for information connected with intelligence agencies, one applying to the definition of disclosable conduct and the other applying to the definition of a public interest disclosure.²¹¹ First, conduct will not qualify as disclosable conduct if it is ‘conduct that an intelligence agency engages in in the proper performance of its functions or the proper exercise of its power’.²¹² Several witnesses to the Senate Legal and Constitutional Affairs Legislation Committee (LCA Committee) expressed concern that this provided a blanket exemption for intelligence agencies, although the IGIS gave evidence that the exemption would operate more narrowly.²¹³ The narrower view, supported by the Explanatory Memorandum, is that the exemption only encompasses a limited range of overseas activities for which intelligence officers receive immunity from liability; in other words, activities that are necessary for intelligence agencies to perform their functions properly but would otherwise be contrary to foreign or domestic law.²¹⁴ On this narrower view, an intelligence officer would not receive protection for revealing the ordinary activities of intelligence agencies – such as intercepting communications or entering private premises – which would be considered unlawful if performed by any other person or organisation. However, it is possible that an intelligence officer could receive protection for revealing conduct that was technically lawful but highly

²⁰¹ *Public Interest Disclosure Act 2013* (Cth), s 28.

²⁰² *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 1; s 34.

²⁰³ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Items 1, 2(b).

²⁰⁴ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 2(c).

²⁰⁵ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 2(e).

²⁰⁶ *Public Interest Disclosure Act 2013* (Cth), s 26(3)(aa)-(ab),(a).

²⁰⁷ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 3(a).

²⁰⁸ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 3(d).

²⁰⁹ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 4.

²¹⁰ Standing Committee, *Whistleblower Protection*, above n 180, 149 [8.31].

²¹¹ In *Public Interest Disclosure Act 2013* (Cth), ss 26 and 29.

²¹² *Public Interest Disclosure Act 2013* (Cth), s 33.

²¹³ Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Public Interest Disclosure Bill 2013 [Provisions]* (June 2013) 21-22.

²¹⁴ Ibid 22. See Explanatory Memorandum, *Public Interest Disclosure Bill 2013* (Cth) 17.

improper.²¹⁵ It is not clear whether a court would adopt this narrower view, as the provision on its face could extend to any conduct by the intelligence agencies that is within their statutory powers.

Secondly, in accordance with s 41 of the PID Act, the disclosure will not qualify as a public interest disclosure if it contains ‘intelligence information’.²¹⁶ The definition of intelligence information includes information that might reveal the sources, technologies, or operations of an intelligence agency,²¹⁷ but it also extends more broadly to any ‘information that has originated with, or been received from, an intelligence agency’.²¹⁸ The definition also includes a summary or extract of any such information.²¹⁹ The government justified this broad exemption by explaining that the ‘inappropriate disclosure of intelligence information may compromise national security and potentially place lives at risk’.²²⁰ Many witnesses to the LCA Committee were nonetheless critical of the broad scope of the exemption.²²¹ AJ Brown has likewise criticised the breadth of s 41, arguing that such a ‘blanket carve-out’ may not satisfy ‘constitutional tests of proportionality, if challenged on constitutional or rights-protection grounds’.²²² In the absence of relevant human rights protections in the *Constitution*, however, it is difficult to see how such a challenge could succeed.

The PID Act also draws a distinction between intelligence information as defined above and information which ‘relates to an intelligence agency’.²²³ In the latter case, information will relate to an intelligence agency if the agency ‘engages in the conduct’.²²⁴ The distinction is unclear, but on its face it suggests that conduct relates to an intelligence agency if it describes the actions of intelligence agencies in very general terms without revealing any sources, operations, methods or agents. As explained below, this distinction creates the possibility for intelligence officers to disclose national security information to the general public in very limited circumstances.

The effect of these requirements is that a person would receive protection for disclosing national security information about intelligence matters in three very limited scenarios. First, a person would be protected for disclosing intelligence information to his or her immediate supervisor, an authorised internal recipient, or the IGIS.²²⁵ In such a case, the information would need to demonstrate that the agency was operating outside ‘the proper performance of its functions or the proper exercise of its power’.²²⁶ In effect, the exemption of intelligence information from the definition of public interest disclosures means that the definition of disclosable conduct is limited to its first category (unlawful activity) with regard to national security information. For example, as above, an officer might reveal to the IGIS that Australia’s foreign intelligence agencies were conducting surveillance on Australian

²¹⁵ The IGIS suggested that the wording encompasses ‘both propriety and legality’, suggesting that improper conduct on behalf of the intelligence agencies could fall outside the exemption: *ibid* 22.

²¹⁶ *Public Interest Disclosure Act 2013* (Cth), s 41.

²¹⁷ *Public Interest Disclosure Act 2013* (Cth), 41 (1)(b).

²¹⁸ *Public Interest Disclosure Act 2013* (Cth), 41 (1)(a).

²¹⁹ *Public Interest Disclosure Act 2013* (Cth), 41 (1)(e).

²²⁰ Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Public Interest Disclosure Bill 2013 [Provisions]* (June 2013) 24.

²²¹ *Ibid* 23-24. See also House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, *Advisory Report: Public Interest Disclosure (Whistleblower Protection) Bill 2012; Public Interest Disclosure (Whistleblower Protection) (Consequential Amendments) Bill 2012; Public Interest Disclosure Bill 2013* (May 2013) 51.

²²² A J Brown, ‘Towards “Ideal” Whistleblowing Legislation? Some Lessons from Recent Australian Experience’ (2013) 2(3) *E-Journal of International and Comparative Labour Studies* 4, 31.

²²³ See *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 2(h)-(i).

²²⁴ *Public Interest Disclosure Act 2013* (Cth), s 35(1).

²²⁵ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 1.

²²⁶ *Public Interest Disclosure Act 2013* (Cth), s 33.

citizens when their statutory mandate is to collect intelligence on ‘people or organisations outside Australia’.²²⁷

Secondly, a person would be protected for disclosing information relating to intelligence agencies (but not intelligence information) where there is a substantial and imminent danger to health, safety or the environment.²²⁸ This suggests that an intelligence officer could disclose information about the conduct of intelligence agencies in very general terms for the purpose of protecting Australian citizens or the environment, but he or she could not disclose any operations, sources or methods for this purpose.²²⁹ This is the only possible scenario in which a person could receive protection for releasing national security information to the general public, including a specific person such as a journalist or Member of Parliament. Even in this case, however, it is not entirely clear that the protections would be available. On its face, the legislation does not appear to require that an emergency disclosure satisfy the definition of ‘disclosable conduct’.²³⁰ However, it is possible that a court could take into account the broad exemption for intelligence information as set out above, and thus that immunity from liability in such a case would not therefore be available.²³¹

Thirdly, a person would be protected for disclosing information relating to intelligence agencies to an Australian legal practitioner.²³² The legal practitioner would need to hold an appropriate security clearance, and the protection would not extend to intelligence information such as operations, sources and methods.²³³ Under no circumstances would a person receive protection for releasing intelligence information to the general public, even if an initial internal review by the person’s supervisor or the IGIS proved inadequate.²³⁴ For this reason, Brown has argued that ‘a workable solution in respect of the coverage of intelligence agencies is yet to be found’.²³⁵ He argues that the differential treatment of intelligence agencies under the PID Act has ‘the effect of undermining the credibility of the scheme as a whole’.²³⁶

These three scenarios demonstrate that the PID Act plays a very limited role with regard to the release of national security information. Given the sympathy of many for the actions of Manning, Assange, and Snowden, these limited protections would appear inadequate to a significant section of the community. It is conceivable, for example, that an Australian intelligence officer could become involved in conduct that they believed to be highly immoral – such as manipulating sources into providing intelligence by threatening to tell their children about their involvement in illegal activity. If the officer raised this within the agency or with the IGIS and no remedies were provided (for example, because the conduct fell within the agency’s statutory powers), the officer might feel compelled to disclose information about the agency’s conduct to a respected journalist or Member of Parliament. The officer could exercise the utmost care in protecting any operations, sources or methods and the identities of any officers involved, but the PID Act would still provide no

²²⁷ See *Intelligence Services Act 2001* (Cth) s 6(1)(a), which provides that functions of ASIS are ‘to obtain ... intelligence about the capabilities, intentions or activities of people or organisations outside Australia’

²²⁸ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 3.

²²⁹ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 3(f). That provision excludes intelligence information from the meaning of public interest disclosures in emergency situations, but there is no equivalent exclusion for information relating to intelligence agencies. Cf *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 2(h)-(i), which includes exemptions for both intelligence information and information relating to intelligence agencies in the case of an external disclosure.

²³⁰ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 3(a). Cf *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 2(a), which provides for an ordinary external disclosure that the information ‘tends to show ... one or more instances of disclosable conduct’

²³¹ Brown, ‘Towards “Ideal” Whistleblowing Legislation?’, above n 222, 29-30.

²³² *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 4.

²³³ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 4(b)-(c).

²³⁴ With regard to external disclosures, *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 4(h)(i) excludes both intelligence information and information relating to intelligence agencies.

²³⁵ Brown, ‘Towards “Ideal” Whistleblowing Legislation?’, above n 222, 30.

²³⁶ *Ibid.*

protection. A scenario along these lines could be protected if the PID Act were amended to allow the disclosure of information relating to intelligence agencies where the information suggested illegal conduct or a serious breach of public trust and an internal review had previously proved inadequate. Until then – and such an amendment seems unlikely given the important status that intelligence information holds within the PID Act – prosecution for a serious criminal offence may simply be the price that an intelligence officer must pay for revealing improper and immoral conduct in good conscience. It is doubtful whether this is an adequate result given that the explicit objectives of the PID Act are to contribute to the integrity and accountability of government.²³⁷

V CONCLUSIONS

Recent events surrounding Manning, Assange and Snowden raise important questions about balance to be struck in exposing abuses of power by government and protecting classified information for the purposes of national security. Moral questions about whether these leaks were justified or excusable will continue for the foreseeable future, and reasonable minds will disagree about the extent to which the public interest was served in publishing the WikiLeaks and Snowden material. In this article, we have addressed a narrower legal question by exploring the scope of Australian law with regard to the disclosure of national security information. This inquiry raises a number of important themes.

It is clear the Australian government has enacted a comprehensive scheme for regulating national security information. While the WikiLeaks and Snowden scenarios are very recent developments, there is certainly no absence of legislation to address this issue. The Commonwealth government has at its disposal not only serious criminal offences for political acts against the state (namely terrorism, treason and espionage), but also criminal offences which address the disclosure of information by Commonwealth officers, those contracted to work for government agencies, intelligence officers, and any person entering into an agreement or arrangement with the intelligence agencies. It is unlikely that any new scenario involving the release of national security information could arise that would not be addressed by one or more of these laws.

On the other hand, while there is certainly a wide variety of laws available to address the disclosure of national security information, in some cases these laws do not adequately address some more specific scenarios that are relevant to recent events. This is because existing laws would need to be applied to new purposes for which they were not originally designed. The terrorism, treason and espionage offences, for example, were introduced or remodelled in response to the 9/11 attacks. They were not designed specifically to address the release of national security information by the likes of individuals such as Assange or Snowden. In some cases this creates some curious anomalies and in others it means that the laws may not be sufficiently tailored to likely future scenarios. Under Australia's anti-terror laws,²³⁸ for example, a cyber-activist group could face a maximum penalty of life imprisonment for hacking into a secure database and threatening to release information in a way that would create a serious risk to health and safety – yet a person who intentionally provided that same information to a terrorist organisation would receive a lower penalty of 25 years' imprisonment.²³⁹ Another example is the offence of materially assisting the enemy: this offence would apply, as intended, to individuals who directly assist an enemy at war with the Commonwealth, but could apply the same maximum penalty to a person who indirectly assisted an enemy by disclosing classified information. Such examples suggest that new offences or amendments are needed to tailor existing laws more specifically to the disclosure of classified information.

²³⁷ *Public Interest Disclosure Act 2013* (Cth), s 6.

²³⁸ *Criminal Code Act 1995* (Cth), s 100.1.

²³⁹ *Criminal Code Act 1995* (Cth), s 102.7(1).

The laws examined above also involve important questions about the role of the criminal law. In particular, they raise three issues as to when the criminal law provides an appropriate remedy in this context. First, the terrorism and espionage offences and s 79 of the Crimes Act apply criminal penalties not only to the disclosure of information but also to the possession and retention of information.²⁴⁰ This raises an important question as to whether the criminal law should intervene before a person has formed an intention to release the information to others. In such cases, it may be more appropriate for the government to seek civil and administrative remedies.²⁴¹ Given that the purpose of the offences is to prevent the release of information that could harm national security, it seems unlikely that the government would restrict the offences so that they operate only once the information has been disclosed. However, a significant improvement would be to amend the espionage offences so that they provide significantly lower penalties for possession compared to disclosure.²⁴² This is the approach currently taken in the terrorism offences and s 79, and an amendment along these lines would ensure parity.

Secondly, most of the offences for possession – and in some cases disclosure – do not expressly require an intention to cause harm.²⁴³ In particular, ss 70 and 79(3) of the Crimes Act and the specific offences for intelligence officers all provide maximum penalties of 2 years' imprisonment where a person releases information – regardless of the type of information released and regardless of whether the person intends to harm the public interest.²⁴⁴ These offences provide significantly lower penalties compared to terrorism, espionage, or the release of official secrets to prejudice security or defence, but they nonetheless pose an important question as to whether the criminal law should be triggered by the breach of common law and statutory duties. As the ALRC has convincingly argued, the criminal law should apply only to the most serious cases of disclosure where a person intends to harm an essential public interest, such as security, defence or public safety.²⁴⁵

Thirdly, the offences raise important questions as to *whom* the criminal law should apply. In particular, the offences for intelligence officers raise an important question as to whether the criminal law should apply beyond contractors to any person who holds an 'agreement or arrangement' with the Commonwealth.²⁴⁶ In such cases it may be more appropriate for civil remedies to apply, as the individuals concerned may not be fully aware of the special responsibilities involved in handling classified information. In either case, the law surrounding government contractors and those holding agreements with government departments should be clarified in the legislation – such as by including clearer references to contractors in the statutory definition of a Commonwealth officer.²⁴⁷

Another area in which existing laws require further attention is with regard to the subsequent disclosure scenario. Where A commits a criminal offence by communicating information to B, and B communicates that information to C with the same intention as A, it is appropriate that B should receive the same penalty as A. However, s 79 of the Crimes Act applies the same penalty to B for the mere receipt of information from A, before B has formed an intention to communicate that information to C.²⁴⁸ Clearly Person A in this scenario (who has intentionally communicated classified information) is more at fault than Person B (who has merely received the information), and yet under s 79 the same penalties

²⁴⁰ See *Criminal Code Act 1995* (Cth), ss 91.1(3)-(4), 101.4, 101.5; *Crimes Act 1914* (Cth), s 79(2)(b)-(c), (4)-(6).

²⁴¹ See ALRC, *Secrecy Laws*, above n 98, 203 [6.82].

²⁴² Instead of providing 25 years for both: cf *Criminal Code Act 1995* (Cth), s 91.1(1)-(2) (disclosure) with (3)-(4) (possession/retention).

²⁴³ An exception are the espionage offences where information is recorded or copied with an intention to prejudice security or defence: *Criminal Code Act 1995* (Cth), s 91.1(3)-(4).

²⁴⁴ *Crimes Act 1914* (Cth), s 70, s 79(3); *Intelligence Services Act 2001* (Cth), ss 39, 39A, 40.

²⁴⁵ ALRC, *Secrecy Laws*, above n 98, 9 (Recommendation 5-1), 138, 160, 324.

²⁴⁶ *Intelligence Services Act 2001* (Cth), ss 39(1)(b)(ii), 39A(1)(b)(ii), 40(1)(b)(ii); *Australian Security Intelligence Organisation Act 1979* (Cth), s 18(2).

²⁴⁷ *Crimes Act 1914* (Cth), s 3. As suggested by ALRC: ALRC, *Secrecy Laws*, 9-10 (Recommendation 6-1), 16 (Recommendation 13-3), 480 [13.103]-[13.104].

²⁴⁸ *Crimes Act 1914* (Cth), s 79(5)-(6).

can apply. As with the offences for possession and retention of information, this formulation also removes a window of moral opportunity in which B may freely choose to dispose of or retain the information without communicating it to another person. A separate offence for subsequent disclosures, which stipulates the same fault and physical requirements for B as A, would help to remedy these problems.

It is clear that there are few protections under these laws for individuals who disclose national security information. There are some exemptions contained in the offences themselves: the political protest exemption in the definition of terrorism,²⁴⁹ the good faith defence for materially assisting the enemy,²⁵⁰ and the exemption in s 79 of the Crimes Act for disclosures made ‘in the interest of the Commonwealth’.²⁵¹ These are important inclusions, although their scope is relatively limited. The precise scope of the political protest exemption in the definition of terrorism is unclear, but it will not apply where the person intends to create a serious risk to health or safety.²⁵² This is a relatively low harm requirement which could be satisfied by many legitimate political protests, such as nurses striking or environmental activists protesting in treetops. Whether a person acted in good faith or in the interests of the Commonwealth by disclosing classified information would likely be difficult issues to resolve, although it seems unlikely that a court would hold disclosure to be in the public interest where the contents of intelligence reports or similar documents were revealed. There may be some scope for an individual to describe the conduct of an agency with regard to classified material in general terms – such as the fact that an agency’s management ignored an important report – so long as the content of that material was not disclosed.²⁵³

Protections for whistleblowers under the PID Act are severely limited in this context because of the special status given to intelligence information. Public officials will be protected for releasing classified material to their immediate supervisors, the IGIS, or a lawyer – but no protections are available for releasing intelligence information to the general public. The only circumstance in which a person could receive immunity for releasing national security information to the general public is where there is a substantial and imminent danger to health or safety and the person disclosed information relating to intelligence agencies in general terms (but not intelligence information that exposed any operations, methods, sources, or agents).²⁵⁴ In such a case, there would also need to be ‘exceptional circumstances’ justifying why the person bypassed the statutory requirement for internal review.²⁵⁵

The PID Act certainly would not extend to a WikiLeaks scenario where a person downloaded and published the content of an entire intelligence database, as any disclosures must be restricted only to that information necessary to demonstrate wrongdoing or illegal conduct.²⁵⁶ Even if an intelligence officer revealed a very limited range of information for the purposes of exposing highly immoral conduct, the protections of PID Act still would not be triggered. This reflects the higher risk that intelligence poses to national security compared to information held by other government departments, although it would likely be an inadequate result for the many thousands of individuals who believe that Manning, Assange and Snowden are the heroes of the digital age.

²⁴⁹ *Criminal Code Act 1995* (Cth), s 100.1(3).

²⁵⁰ *Criminal Code Act 1995* (Cth), s 80.3.

²⁵¹ *Crimes Act 1914* (Cth), s 79(2)(a)(ii), (3)(b).

²⁵² *Criminal Code Act 1995* (Cth), s 100.1(3)(b)(iv).

²⁵³ See Kessing (2008) 73 NSWLR 22, 30 [33]; ALRC, *Secrecy Laws*, above n 98, 57-58.

²⁵⁴ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 3.

²⁵⁵ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Item 3(d).

²⁵⁶ *Public Interest Disclosure Act 2013* (Cth), s 26(1), Items 2(f), 3(b).