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 United States ('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 that 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 US military

* 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: David Leigh and Luke Harding, *WikiLeaks: Inside Julian Assange's War on Secrecy* (The Guardian, 2011) 53–6. Manning's actions were discovered not because the Tor encryption failed, but because he confessed his actions to a hacker friend (Adrian Lamo): at 72–87.

2 Leigh and Harding, above n 1, 116–44; 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>.

court of multiple offences under the US *Espionage Act*[3] and sentenced to 35 years' imprisonment, but was acquitted of a charge of aiding the enemy.[4]

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.[5]

The saga took on a new dimension when Edward Snowden released details of PRISM, a worldwide data mining program conducted by the US government's National Security Agency ('NSA').[6] Snowden was an employee of Booz Allen Hamilton, a technology consulting firm, and was contracted to work for the NSA.[7] He has since applied for political asylum in Russia, where he continues to justify his actions via the internet.[8]

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'.[9] US Vice-President Joe Biden

---

3 18 USC §§ 791–9.

4 See Paul Lewis, 'Bradley Manning to Request Pardon from Obama over 35-year Jail Sentence', *The Guardian* (London), 22 August 2013. 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.

5 See David Crouch and Robert Booth, 'Julian Assange's Lawyers Will Appeal against Ruling to Uphold Arrest Warrant', *The Guardian* (London), 17 July 2014.

6 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', *The Sydney Morning Herald* (Sydney), 12 June 2013; Nick Perry and Paisley Dodds, 'Five Eyes Spying Alliance will Survive Edward Snowden: Experts', *The Sydney Morning Herald* (Sydney), 18 July 2013; Philip Dorling, 'Australia gets "Deluge" of US Secret Data, Prompting a New Data Facility', *The Sydney Morning Herald* (Sydney), 13 June 2013.

7 See Greenwald, MacAskill and Poltras, above n 6.

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

9 'Gillard Fires at 'Illegal' WikiLeaks Dump', *ABC News* (online), 2 December 2010 <http://www.abc.net.au/news/2010-12-02/gillard-fires-at-illegal-wikileaks-dump/2359304>; 'Julia Gillard Can't Say How WikiLeaks Founder Julian Assange Has Broken the Law', *The Australian* (online), 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>; 'WikiLeaks Acting Illegally, Says Gillard', *The Sydney Morning Herald* (online), 2 December 2010 <http://www.smh.com.au/technology/technology-news/wikileaks-acting-illegally-says-gillard-20101202-18hb9.html>.

labelled Assange a 'hi-tech terrorist'.[10] Former US Secretary of State Hillary Clinton described Assange's actions as an 'attack on the international community'.[11] 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.'[12]

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.[13] The cyber-activist group 'Anonymous' launched denial-of-service attacks against MasterCard and PayPal for refusing to process donations to the WikiLeaks website.[14] Amnesty International has created an online petition calling for Manning's release, arguing that the sentence imposed was more severe than some soldiers have received for rape and war crimes.[15] Slavoj Žižek has called for an international network to protect whistleblowers,[16] describing Manning, Assange and Snowden as 'our new heroes, exemplary cases of the new ethics that befits our era of digitalised control'.[17]

Debates about whether these leaks were morally or ethically justified will continue, without the prospect of a definitive resolution. Our purpose in this

---

10 Ewen MacAskill, 'Julian Assange Like a Hi-Tech Terrorist, Says Joe Biden', *The Guardian* (London), 19 December 2010.

11 Mary Beth Sheridan, 'Hillary Clinton: WikiLeaks Release an "Attack on International Community"', *The Washington Post* (Washington DC), 29 November 2010.

12 Jeffrey T Kuhner, 'Kuhner: Assassinate Assange?', *The 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: *Flanagan Regrets WikiLeaks Assassination Remark* (1 December 2010) CBC News <http://www.cbc.ca/news/politics/flanagan-regrets-wikileaks-assassination-remark-1.877548>; *Assange Lawyer Condemns Calls for Assassination of WikiLeaks' Founder* (28 June 2013) NBC News <http://www.nbcnews.com/id/40467957/ns/us_news-wikileaks_in_security/t/assange-lawyer-condemns-calls-assassination-wikileaks-founder/#.UzCt36Wz5lI>.

13 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; *Wikileaks Protests in Spain over Julian Assange Arrest* (12 December 2010) BBC News <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; 'Hong Kong Protestors Rally in Support of US Spy Whistleblower Edward Snowden', *ABC News* (online), 16 June 2013 <http://www.abc.net.au/news/2013-06-15/hong-kong-protest-in-support-of-snowden/4756572>.

14 These attacks were known as 'Operation Payback': 'European Amazon Websites Down after Attack by WikiLeaks Supporters', *The Australian* (online), 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 Laville, 'Anonymous Cyber-Attacks Cost PayPal £3.5m, Court Told', *The Guardian* (London), 22 November 2013.

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

16 Slavoj Žižek, 'Edward Snowden, Chelsea Manning and Julian Assange: Our New Heroes', *The Guardian* (London), 3 September 2013.

17 Ibid.

article is narrower and focused on Australia.[18] 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,[19] 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) ('*NSIA*') 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.[20] 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.[21] Under the PSPF, national security information is classified to four levels ('Protected', 'Confidential',

18 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?'(Research Paper No 14/09, Sydney Law School Legal Studies, January 2014).

19 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', *The Sydney Morning Herald* (Sydney), 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.

20 *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) s 7 (definition of 'national security information'; 'national security'). The definition of 'national security' in the *NSIA* relies on the definition of 'security' in the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*') s 4. Part 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.

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

'Secret', and 'Top Secret') according to the potential damage that could be caused by its release.[22]

Part II of this article 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 Part 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) schedule 1 ('*Criminal Code*'),[23] 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.[24] 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.[25] 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

22 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 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'.

23 *Criminal Code* s 100.1.

24 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).

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

to terrorist acts.[26] 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.[27]

Most of these counter-terrorism laws hinge on a statutory definition of terrorism that was inserted in section 100.1 of the *Criminal Code*.[28] Section 100.1 was closely modelled on the United Kingdom's (UK) 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.[29] 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'.[30] 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.[31] 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.[32] The list includes death and

26 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).

27 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: Kent Roach, *The 9/11 Effect* (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*. However, the *Act* also expanded the scope of Australia's anti-terror laws by granting police a power to conduct warrantless searches: *National Security Legislation Amendment Act 2010* (Cth) schs 1, 3, 4.

28 *Criminal Code* s 100.1. The definition of terrorism in Pt 5.3 of the *Criminal Code* was inserted by *Security Legislation Amendment (Terrorism) Act 2002* (Cth) sch 1 item 3. For a more detailed evaluation of the statutory definition of terrorism, see Keiran Hardy and George Williams, 'What is "Terrorism"? Assessing Domestic Legal Definitions' (2011) 16 *UCLA Journal of International Law and Foreign Affairs* 77, 130–7.

29 *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: 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, 375.

30 *Criminal Code* 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 *University of New South Wales Law Journal* 333.

31 *Criminal Code* s 100.1(1)(a).

32 *Criminal Code* s 100.1(2).

serious bodily injury,[33] 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.[34] Subsection (3) of the definition sets out an exemption for protest, dissent or industrial action that is intended only to cause serious property damage,[35] 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.[36]

A number of criminal offences stem from this definition of terrorism. Most obviously, section 101.1 creates the offence of committing a terrorist act,[37] 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.[38] In the context of releasing national security information, the most relevant of these offences would be:

- possessing things connected with terrorist acts (section 101.4);
- collecting or making documents likely to facilitate terrorist acts (section 101.5); and
- doing any other act in preparation for a terrorist act (section 101.6)[39]

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,[40] or 10 years where the person is reckless as to the existence of the connection.[41] The penalty for doing any other act in preparation for terrorism is life imprisonment.[42]

In addition, division 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,

33 *Criminal Code* ss 100.1(2)(a), (c).
34 *Criminal Code* ss 100.1(2)(d)–(f).
35 *Criminal Code* s 100.1(3). See Keiran Hardy, 'Operation Titstorm: Hacktivism or Cyber-Terrorism?' (2010) 33 *University of New South Wales Law Journal* 474, 489–92.
36 *Criminal Code* s 100.1(3)(b)(iv).
37 *Criminal Code* s 101.1. It has a maximum penalty of life imprisonment.
38 See, eg, *R v Lodhi* (2006) 163 A Crim R 448; *R v Elomar* (2010) 264 ALR 759; *Khazaal v The Queen* (2011) 265 FLR 27. 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: 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 Futures of Criminal Law* (Hart Publishing, 2008) 35–58; Lucia Zedner, 'Preventive Justice or Pre-Punishment? The Case of Control Orders' (2007) 60 *Current Legal Problems* 174; Jude McCulloch and Sharon Pickering, 'Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror"' (2009) 49 *British Journal of Criminology* 628.
39 *Criminal Code* ss 101.4–101.6.
40 *Criminal Code* ss 101.4(1), 101.5(1).
41 *Criminal Code* ss 101.4(2), 101.5(2).
42 *Criminal Code* s 101.6(1).

prepare, assist in or foster the doing of a terrorist act.[43] The penalty is 25 years' imprisonment where the person knows the organisation is a terrorist organisation,[44] and 15 years' imprisonment where the person is reckless as to the fact that the organisation is a terrorist organisation.[45]

Given the scope of the definition of terrorism in section 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.[46] The definition of terrorism does not require any higher intention standard, such as the conduct or threat being designed to strike immense fear or terror in the population.[47]

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.[48] Indeed, given that the definition extends to acts that seriously interfere with electronic systems,[49] it is possible that the harm requirement could be satisfied by the act of hacking into a secure database to obtain national security information, even if no such additional or subsequent harm was caused.[50] In addition, because the scope of section 100.1 extends explicitly to the threat of action,[51] 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

---

43 *Criminal Code* s 102.7. This offence requires that the Attorney-General has previously proscribed the organisation as a 'terrorist organisation'. Alternatively, it may be proved in court that the organisation is a terrorist organisation: see definition of a terrorist organisation in *Criminal Code* s 102.1. See *Benbrika v The Queen* (2010) 29 VR 593. 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 *Legal History* 25; Andrew Lynch, Nicola McGarrity and George Williams, 'The Proscription of Terrorist Organisations in Australia' (2009) 37 *Federal Law Review* 1; Nicola McGarrity, 'Review of the Proscription of Terrorist Organisations: What Role for Procedural Fairness?' (2008) 16 *Australian Journal of Administrative Law* 45.

44 *Criminal Code* s 102.7(1).

45 *Criminal Code* s 102.7(2).

46 *Criminal Code* ss 100.1(1)(a)–(b).

47 This higher intention standard is included as one in a list of alternatives in the New Zealand and South African statutory definitions of terrorism: *Terrorism Suppression Act 2002* (NZ) s 5(2)(a) ('to induce terror in a civilian population'); *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').

48 *Criminal Code* s 100.1(2)(e).

49 *Criminal Code* s 100.1(2)(f).

50 See Keiran Hardy, 'WWWMDs: Cyber-Attacks Against Infrastructure in Domestic Anti-Terror Laws' (2011) 27 *Computer Law & Security Review* 152; Hardy, above n 35.

51 *Criminal Code* s 100.1 (defined as 'action or threat of action').

Australian soldiers in the torture of detainees in the Middle East.[52] 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 section 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.[53]

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,[54] or collecting or making a document connected with terrorism,[55] 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 section 101.6.[56] 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 (section 102.7(1)) where that information could help to plan a terrorist act on Australian soil.[57] 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.[58] Section

52 Similar revelations were made by the Public Interest Advocacy Centre in 2012: Public Interest Advocacy Centre, 'Australia Complicit in Illegal 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', *The Sydney Morning Herald* (Sydney), 9 February 2012.

53 *Criminal Code* s 100.1(3)(b)(iv).

54 *Criminal Code* s 101.4.

55 *Criminal Code* s 101.5.

56 *Criminal Code* s 101.6.

57 *Criminal Code* s 102.7(1).

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

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.[59] 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 was reckless as to the possibility of causing) serious harm.[60] 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.[61] The causal element will be satisfied if the person's conduct 'substantially contributes' to the death or harm of an Australian citizen.[62]

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.[63] 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.[64] 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

59 *Criminal Code* s 115.1(1).
60 *Criminal Code* s 115.2(1).
61 *Criminal Code* ss 115.3(1), 115.4(1).
62 *Criminal Code* s 115.9.
63 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* (online), 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>.
64 *Security Legislation Amendment (Terrorism) Act 2002* (Cth) sch 1 item 2. See Parliamentary Joint Committee on Intelligence and Security, *Review of Security and Counter Terrorism Legislation* (2006) 39 [4.3] ('*Review of Security Report*').

Commonwealth; assisting a country or organisation engaged in armed hostilities against the Australian Defence Force ('ADF'); and instigating a foreign person to invade Australia.[65] In 2005, the offence was supplemented with new sedition offences,[66] which included the offences of 'urging' a person to assist an enemy at war or to engage in armed hostilities with the ADF.[67]

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.[68] In response, the current wording of the treason offences was introduced in 2010.[69] The amendments repealed the sedition offences and amended the basic offence of treason by creating a separate offence of 'materially assisting the enemy'.[70] The offence of treason, in section 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, imprisonment or restraint); levies war against the Commonwealth; or instigates a foreign person to make an armed invasion of Australia.[71] The separate offence for materially assisting the enemy is now found in section 80.1AA.[72] 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.[73] 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.[74] 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.[75]

It is possible that the release of national security information could fall under the treason offence in section 80.1 of the *Criminal Code*. 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

65 *Security Legislation Amendment (Terrorism) Act 2002* (Cth) sch 1 item 2.
66 *Anti-Terrorism Act (No 2) 2005* (Cth) sch 7.
67 *Criminal Code* ss 80.2(7)–(9) (now repealed).
68 ALRC, *Fighting Words: A Review of Sedition Laws in Australia,* Report No 104 (2006) 158 ('*Fighting Words Report*').
69 *National Security Legislation Amendment Act 2010* (Cth) sch 1.
70 *Criminal Code* s 80.1AA.
71 *Criminal Code* s 80.1(1).
72 *Criminal Code* s 80.1AA.
73 *Criminal Code* ss 80.1AA(1)(d), (4)(c).
74 *Criminal Code* ss 80.1AA(1)(e), (4)(d).
75 *Fighting Words Report*, above n 68, 15–16.

charged with a similar offence in the US,[76] 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.[77] If a similar scenario occurred in Australia and the person expected that a terrorist organisation would see the leaked information, then section 80.1AA of the *Criminal Code* could be triggered.

Importantly, section 80.3 of the *Criminal Code* includes a defence for acts done in good faith.[78] This is available for the offence of materially assisting the enemy, but not for the basic offence of treason.[79] 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'.[80] 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'.[81] 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',[82] then arguably section 80.1AA of the *Criminal Code* 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 Sheller Committee, which reviewed Australia's counter-terrorism laws in 2006,[83] 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:

---

76 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, or shall be imprisoned not less than five years and fined under this title but not less than $10,000; and shall be incapable of holding any office under the United States.

77 *Manning Not Guilty of Aiding the Enemy, Faces 130+ Yrs in Jail on Other Charges* (31 July 2013) Reuters <http://rt.com/usa/manning-not-guilty-aiding-enemy-805/>.

78 *Criminal Code* s 80.3.

79 *Criminal Code* s 80.3.

80 *Criminal Code* s 80.3(1)(a). Section 80.3(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* ss 13.3(3), 80.3.

81 *Criminal Code* s 80.3(2).

82 *Criminal Code* s 80.3(2)(f).

83 Security Legislation Review Committee, Parliament of Australia, *Report of the Security Legislation Review Committee* (2006).

> 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.[84]

It is clear that section 80.1AA can apply to very serious conduct, such as directly assisting al-Qaeda in a foreign insurgency. However, section 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 section 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.[85] 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.[86] 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 section 91.1 of the *Criminal Code*. Like the other offences outlined above, the espionage offences were updated after 9/11.[87] 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.[88] The main offence in section 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

---

84 Australian Federal Police, Submission No 12 to Security Legislation Review Committee, 8 February 2006, 5, cited in *Review of Security Report*, above n 64, 40.

85 *Criminal Code* ss 80.1AA(1)(e), (4)(d).

86 Australian Federal Police, above n 84, 40.

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

88 Including 'harbouring spies' and the 'illegal use of uniforms': *Crimes Act 1914* (Cth) ss 81, 83A (now repealed). See Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Matters) Bill 2002 (Cth) 5–8.

behalf of a foreign country or organisation.[89] 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'.[90] This means that the offences could apply either to a Commonwealth employee who obtained national security information in the 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.[91]

As with the terrorism offences,[92] 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.[93] In addition, section 91.1 provides separate offences where a person makes, obtains or copies a record of information concerning the Commonwealth's security or defence.[94] 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.[95] 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.[96] 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.[97] 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.[98] The information might be communicated 'in whole or part', including not only

89 *Criminal Code* s 91.1(1).
90 *Criminal Code* s 91.1(2).
91 *Criminal Code* s 91.1(2)(b)(ii).
92 *Criminal Code* ss 101.4–101.5.
93 *Criminal Code* ss 91.1(1)(c), (2)(c).
94 *Criminal Code* ss 91.1(3)–(4).
95 *Criminal Code* ss 91.1(3)(b)(i), (4)(b)(ii) (or person acting on their behalf). Subsection (4) is the equivalent offence where the information is obtained 'without lawful authority': *Criminal Code* s 91.1(4)(b)(i).
96 *Criminal Code* s 91.1(5).
97 *Criminal Code* s 90.1(1).
98 *Criminal Code* s 90.1(1).

the information itself but also the substance or effect or a description of the information.[99] 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, section 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,[100] but considering the seriousness of recent revelations in the WikiLeaks and Snowden material, it does not 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, 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.[101]

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 in order 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 section 93.1, which requires prior consent from the Attorney-General for the prosecution of any espionage offence,[102] although it is doubtful whether this provides much protection in a context where it would be in the interests of the executive branch of government being harmed.

---

99 *Criminal Code* s 90.1(2)(a).

100 *Criminal Code* s 91.1(1)(b).

101 ALRC, *Secrecy Laws and Open Government in Australia*, Report No 112 (2009) 324 [9.52] ('*Secrecy Laws Report*').

102 *Criminal Code* s 93.1.

III SECRECY OFFENCES

This Part details two categories of secrecy offences which apply to Commonwealth officers (and, in certain circumstances, other individuals). First, sections 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) ('*Intelligence Services Act*') and the *ASIO Act* 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'.[103] The maximum penalty is two years' imprisonment and there is an exception where the person is authorised to publish or communicate the information.[104] A 'Commonwealth officer' is defined as a person who is appointed or engaged under the *Public Service Act 1999* (Cth) ('*Public Service Act*'), the Commissioners and employees of the AFP and, for the purposes of section 70, any other person who 'performs services for or on behalf of' the Commonwealth government.[105] A version of section 70 was included in the original *Crimes Act* but this was replaced in 1960 to extend the prohibition to former Commonwealth officers.[106] Section 70 has been used to prosecute employees from a range of government departments, including employees of Centrelink and the Australian Tax Office.[107] The offence has proved less relevant in the national security context where prosecutions have been instituted under the espionage offences and section 79 of the *Crimes Act*,[108] although in one prominent case a customs officer was found guilty under section 70 for disclosing the contents of two secret reports detailing lax security procedures at Sydney airport.[109]

As the ALRC has noted, the duty not to disclose the information is not contained within section 70 itself but can be sourced elsewhere.[110] Potential common law sources include the duty of confidentiality, as considered in

103 *Crimes Act 1914* (Cth) ss 70(1)–(2).
104 *Crimes Act 1914* (Cth) ss 70(1)–(2) ('except to some person to whom he or she is authorised to publish or communicate it').
105 *Crimes Act 1914* (Cth) s 3.
106 *Secrecy Laws Report*, above n 101, 43, 87.
107 Ibid 87.
108 See, eg, *R v Lappas* (2003) 152 ACTR 7; *R v Lappas* [2001] ACTSC 115; *Grant v Headland* (1977) 17 ACTR 29.
109 *R v Kessing* (2008) 73 NSWLR 22.
110 *Secrecy Laws Report*, above n 101, 88–9, 119–20.

Commonwealth v Fairfax,[111] 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.[112] Employees of the Australian Public Service ('APS') are also placed under statutory duties according to the *Public Service Act* and its regulations.[113] 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'.[114] In particular, regulation 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 programs.[115]

The extent to which these duties apply to contracted service providers is less clear. Given that section 3 of the *Crimes Act* defines Commonwealth officers to include any person who 'performs services for or on behalf of' the government,[116] it seems that section 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 section 3 should explicitly reference 'contracted service providers' as well as the 'officers or employees of a contracted service provider'.[117] The ALRC also emphasised the importance of including confidentiality provisions in employment contracts so that contractors are aware of their secrecy obligations.[118] 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 authority. This information should be protected in the

111 (1980) 147 CLR 39 ('*Fairfax*').
112 See *Secrecy Laws Report*, above n 101, 65–9. See, eg, *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [117].
113 *Public Service Regulations 1999* (Cth).
114 *Public Service Act 1999* (Cth) ss 13(6), (10).
115 *Public Service Regulations 1999* (Cth) reg 2.1.
116 *Crimes Act 1914* (Cth) s 3.
117 *Secrecy Laws Report*, above n 101, 9–10 (Recommendation 6-1).
118 Ibid 16 (Recommendation 13-3), 480 [13.103]–[13.104].

> same way by the criminal law, whether it happens to be held by the public or private sector.[119]

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'.[120] 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,[121] is whether breach of these common law and statutory duties should give rise to the intervention of the criminal law as found in section 70. Because section 70 fails to specify the type of information that is prohibited from disclosure, or an express requirement that the person intends to cause harm, section 70 could apply on its face to the 'disclosure of any information regardless of its nature of sensitivity'.[122] In this regard, the ALRC believed that there were 'real concerns about the way that section 70 of the *Crimes Act* is framed'.[123] 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'.[124] 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.[125]

Such an amendment would represent a significant improvement on the current wording of section 70, which imposes criminal liability for acts that are

---

119 Ibid 190 [6.25].

120 Ibid 478 [13.95].

121 Ibid 89.

122 Ibid 89 [3.100]. In *Commissioner of Taxation v Swiss Aluminium Australia Ltd* (1986) 10 FCR 321, Bowen CJ described the content as 'virtually irrelevant': at 325. In *Deacon v Australian Capital Territory* (2001) 147 ACTR 1, 13 [87]–[89], Higgins J took a different view, arguing that the public interest was a relevant concern.

123 *Secrecy Laws Report*, above n 101, 122 [4.100].

124 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: at 123 [4.102].

125 Ibid 9 (Recommendation 5-1). The ALRC 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: at 161–81.

merely prejudicial to the effective working of government.[126] 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.[127] 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.

The broad drafting of section 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*[128] and later modified in *Coleman v Power*,[129] 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.[130] 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.[131] In *Levy v Victoria*,[132] 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'.[133]

In *Bennett v President, Human Rights and Equal Opportunity Commission*,[134] the Federal Court upheld a challenge to a previous version of regulation 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'.[135] Justice Finn held that regulation 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.[136] As a result of *Bennett*, regulation 7(13) was replaced with the current regulation 2.1, which, as above, places a duty on APS employees not to

126 Through the duty imposed by *Public Service Regulations 1999* (Cth) reg 2.1.
127 See, eg, *Public Service Act 1999* (Cth) ss 28 (suspension), 29 (termination of employment).
128 (1997) 189 CLR 520 ('*Lange*').
129 (2004) 220 CLR 1.
130 *Lange* (1997) 189 CLR 520, 567; *Coleman v Power* (2004) 220 CLR 1, 50 (McHugh J).
131 Ibid. The latter judgment added the words 'in a manner' to the second limb.
132 (1997) 189 CLR 579.
133 *Levy v Victoria* (1997) 189 CLR 579, 624 (Brennan CJ).
134 (2003) 134 FCR 334 ('*Bennett*').
135 *Public Service Regulations 1999* (Cth) reg 7(13) (now repealed). See *Secrecy Laws Report*, above n 101, 55–6.
136 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [98]–[99], [101]. Justice Finn described the regulation as imposing an 'almost impossible demand' on Commonwealth employees: at [98]. See *Secrecy Laws Report*, above n 101, 56.

disclose information where it is 'reasonably foreseeable that the disclosure could be prejudicial to the effective working of government'.[137] It is doubtful whether this wording remedies the failure of regulation 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 regulation 2.1 on this ground.[138] Even if section 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.[139] A version of section 79 was included in the original *Crimes Act* and was based on a similar provision in the *Official Secrets Act 1911* (UK).[140] Few prosecutions have been instituted under section 79, although a key example is *R v Lappas*,[141] where an employee of the Defence Intelligence Organisation ('DIO') was charged under section 79 and a previous version of the espionage offence in section 91.1 of the *Criminal Code*. Lappas received two years' imprisonment for passing classified intelligence documents to a sex worker so that she could sell them to a foreign country.[142]

Section 79 overlaps to some degree with section 70, but applies beyond Commonwealth officers to other categories of people, and contains a higher maximum penalty (up to seven 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.[143] First, prescribed information is information received in contravention of section 79 or the espionage offence in the *Criminal Code*.[144] 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.[145] This limb also refers to individuals who hold contracts made on behalf of the

137 *Public Service Regulations 1999* (Cth) reg 2.1. See *Secrecy Laws Report*, above n 101, 56 [2.60].
138 *R v Goreng Goreng* (2008) 220 FLR 21.
139 *Crimes Act 1914* (Cth) s 79.
140 *Secrecy Laws Report*, above n 101, 93 [3.115].
141 (2003) 152 ACTR 7. See *Secrecy Laws Report*, above n 101, 94.
142 Transcript of Proceedings, *R v Dowling* (Supreme Court of the Australian Capital Territory, Gray J, 9 May 2003), cited in *Secrecy Laws Report*, above n 101, 94.
143 *Crimes Act 1914* (Cth) s 79(1).
144 *Crimes Act 1914* (Cth) s 79(1)(a).
145 *Crimes Act 1914* (Cth) s 79(1)(b).

Commonwealth, suggesting that the offences could equally apply to contracted service providers.[146] 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.[147] 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'.[148]

Subsection (2) of section 79 provides a maximum penalty of seven years' imprisonment where the person communicates the information to another person 'with the intention of prejudicing the security or defence of the Commonwealth'.[149] While this is a significantly higher penalty than that imposed by section 70,[150] the inclusion of an express intention requirement is a notable improvement. It restricts the application of the seven year penalty to disclosures of information that are intended to cause harm. By contrast, subsection (3) provides a maximum penalty of two years' imprisonment where there is no intention to prejudice security or defence.[151] In this respect, section 79(3) raises a similar issue to section 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.[152]

For both these offences under section 79, there is an exemption where disclosure would be 'in the interest of the Commonwealth'.[153] 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,[154] 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

146 *Crimes Act 1914* (Cth) s 79(1)(b)(iii).
147 *Crimes Act 1914* (Cth) s 79(1)(c).
148 *Crimes Act 1914* (Cth) s 80.
149 *Crimes Act 1914* (Cth) s 79(2).
150 *Crimes Act 1914* (Cth) s 70 (maximum penalty 2 years' imprisonment).
151 *Crimes Act 1914* (Cth) s 79(3).
152 *Secrecy Laws Report*, above n 101, 117 [4.76], 138 [4.157].
153 *Crimes Act 1914* (Cth) s 79(2)(a)(ii), (3)(b).
154 See, eg, *Fairfax* (1980) 147 CLR 39; *R v Kessing* (2008) 73 NSWLR 22 (*'Kessing'*). In *Fairfax*, Mason CJ held 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': at 52. However, he noted that this can often be 'difficult to decide'.

affairs without revealing any details or particulars about their content.[155] For example, in *Kessing*, a customs officer was found guilty under section 70 of the *Crimes Act* for revealing the contents of two classified reports that revealed lax airport security procedures.[156] Kessing was considered a hero by many because his acts led to a major review of airport security.[157] In upholding Kessing's conviction, the NSW Court of Criminal Appeal confirmed that the *entire* contents of a classified report need not be communicated for the offence to be made out, so long as the person communicates the 'substance or purport of the document or some part of it'.[158] This leaves open the possibility that a public servant might reveal, for example, that a classified report had been inadequately addressed by an agency's management, so long as he or she did not reveal the substance of those reports.[159]

Like the terrorism and espionage offences, section 79 applies not only to the disclosure of information but also to its possession. A maximum penalty of seven 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.[160] 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 six months' imprisonment) applies.[161] The latter offence also applies where the person fails to take reasonable care of the information.[162]

A key issue raised by section 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.

---

155 See, eg, *Fairfax* (1980) 147 CLR 39, 52 (Mason CJ): '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'.

156 *Kessing* (2008) 73 NSWLR 22.

157 *Secrecy Laws Report*, above n 101, 58 [2.63]; Paul Latimer and A J Brown, 'Whistleblower Laws: International Best Practice' (2008) 31 *University of New South Wales Law Journal* 766, 783.

158 *Kessing* (2008) 73 NSWLR 22, 30 [33] (Bell JA).

159 In sentencing, Bennett DCJ had suggested that this kind of a revelation would be in the public interest: *R v Kessing* [2007] NSWDC 138 [59]–[60].

160 *Crimes Act 1914* (Cth) ss 79(2)(b)–(c).

161 *Crimes Act 1914* (Cth) ss 79(4)(a)–(b).

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

Given the contemporary relevance of the subsequent disclosure scenario it is important that legislation should address it, although the scope of section 79 is strikingly broad in this regard. If Person B communicates the information to Person C, he or she could be prosecuted under section 79 according to the offences outlined above.[163] However, section 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, section 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 subsection 5, which provides a maximum penalty of seven years' imprisonment where a person receives prescribed information in circumstances contrary to section 91.1 of the *Criminal Code* (espionage) or subsection 2 of section 79 (ie, where Person A intends to prejudice security or defence).[164] Alternatively, subsection 6 provides a maximum penalty of two years' imprisonment where a person receives prescribed information in circumstances contrary to subsection 3 of section 79 (ie, where Person A does not intend to prejudice security or defence).[165] In either case, Person B must have reasonable grounds for believing that the information was received in contravention of the relevant offence.[166] 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.[167] 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 section 79, and to ensure that the 'mere receipt or possession' of information does not receive the same penalty as an initial disclosure,[168] the ALRC recommended that a separate offence for subsequent disclosures be created.[169] 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

163 *Crimes Act 1914* (Cth) s 79(1)(a) defines prescribed information as information received in contravention of this part or in contravention of espionage offence in s 91.1 of the *Criminal Code*.
164 *Crimes Act 1914* (Cth) s 79(5).
165 *Crimes Act 1914* (Cth) s 79(6).
166 *Crimes Act 1914* (Cth) ss 79(5)–(6).
167 *Crimes Act 1914* (Cth) ss 79(5)–(6).
168 *Secrecy Laws Report*, above n 101, 203 [6.82].
169 Ibid 10–11 (Recommendations 6-6, 6-7), 13 (Recommendation 9-7).

that Person B was reckless as to the possibility that disclosing the information to Person C would cause such harm.[170] 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* 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.[171] 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.[172] Each of the three offences provides a maximum of two 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'.[173] An equivalent offence for employees of the Australian Security Intelligence Organisation ('ASIO') can be found in section 18 of the *ASIO Act*.[174]

Like section 70 of the *Crimes Act*,[175] 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 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').[176] 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.[177] 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:

---

170 See ibid 10–11 (Recommendations 6-6, 6-7), 13 (Recommendation 9-7), 341–2.
171 *Intelligence Services Act 2001* (Cth) ss 39, 39A, 40.
172 See, Tom Allard, 'Australia Accused of Playing Dirty in Battle with East Timor over Oil and Gas Reserves', *The Sydney Morning Herald* (Sydney), 28 December 2013.
173 *Intelligence Services Act 2001* (Cth) ss 39(1)(a), 39A(1)(a), 40A(1)(a).
174 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(2).
175 *Crimes Act 1914* (Cth) s 70.
176 *Secrecy Laws Report*, above n 101, 289.
177 Ibid.

> 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.[178]

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,[179] by arguing that it is 'appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive intelligence information'.[180] However, in considering the scope of a general secrecy offence to replace sections 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.[181] 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.[182] 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 one year.[183]

---

178 Ibid 289 [8.63].

179 *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).

180 *Secrecy Laws Report*, above n 101, 289 [8.62].

181 Ibid 190.

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

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

IV WHISTLEBLOWER PROTECTIONS

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 ('Standing Committee').[184] The move was aided by former intelligence whistleblower Andrew Wilkie, who introduced his own private member's Bill alongside the main legislation.[185]

The term 'whistleblower' is not used in the *PID Act* but in common usage it refers to individuals who speak out about wrongdoing or illegal conduct by an organisation or its members.[186] 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".'[187] As a result of its inquiry, the Standing Committee recommended that a comprehensive scheme for protecting whistleblowers should be enacted at the national level 'as a matter of priority'.[188] The Standing 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.[189]

The *PID Act* establishes a whistleblowing scheme by protecting public officials who disclose information according to a specified process.[190] 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

---

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

185 Public Interest Disclosure (Whistleblower Protection) Bill 2012 (Cth). See Commonwealth, *Parliamentary Debates*, House of Representatives, 29 October 2012, 12181.

186 See *Whistleblower Protection Report*, above n 184, 24–5.

187 Ibid 24 [2.18].

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

189 Ibid 1 [1.3]–[1.4].

190 The *PID Act* repealed section 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 also ibid 5 [1.19].

adverse consequences'.[191] 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.[192] The definition also includes contracted service providers,[193] 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 Act* scheme is section 10, which provides that public officials who make public interest disclosures are protected from civil, criminal and administrative liability, including disciplinary action by the department in which they are employed.[194] This protection is not available where the disclosure contravenes a 'designated publication restriction' such as a suppression order issued by a court.[195] While the protection in section 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'.[196] 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 or one or more persons; and
- results in an increased risk of danger to the environment.[197]

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.[198] 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

191 *Public Interest Disclosure Act 2013* (Cth) ss 6(a), (c). Its other objectives are outlined in s 6(b) ('encouraging and facilitating the making of public interest disclosures') and s 6(d) ('ensuring that disclosures by public officials are properly investigated and dealt with').
192 *Public Interest Disclosure Act 2013* (Cth) s 69(1) items 2, 13, 17.
193 *Public Interest Disclosure Act 2013* (Cth) s 69(1) items 15–16. The definition of a contracted service provider in specified in greater detail: at s 30.
194 *Public Interest Disclosure Act 2013* (Cth) s 10.
195 *Public Interest Disclosure Act 2013* (Cth) s 11A.
196 *Public Interest Disclosure Act 2013* (Cth) s 29.
197 See *Public Interest Disclosure Act 2013* (Cth) s 29.
198 *Public Interest Disclosure Act 2013* (Cth) s 31.

contrary to their statutory mandate – such as by conducting illegal surveillance of Australian citizens.[199] 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.[200]

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.[201] 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.[202] However, this material also included a large database of diplomatic cables that would not qualify under the categories above.[203] 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'.[204] A public interest disclosure may be made orally or in writing, it may be made anonymously, and it may be made without the person asserting that they are seeking immunity from liability under the *PID Act*.[205] 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.[206] 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*.[207] 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.[208] Even then, the information will only have been validly disclosed

199 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'.

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

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

202 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.

203 See Leigh and Harding, above n 1, 135–44.

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

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

206 *Public Interest Disclosure Act 2013* (Cth) ss 26(1) item 1, 34.

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

208 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 2(c).

if its disclosure is not contrary to the public interest.[209] 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.[210] 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'.[211] 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.[212] 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 *PID Act*.[213]

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.[214] 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.[215] 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'.[216] 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.[217] 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.[218] 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

209 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 2(e).
210 *Public Interest Disclosure Act 2013* (Cth) ss 26(3)(aa)–(ab), (a).
211 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 3(a).
212 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 3(d).
213 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 4.
214 *Whistleblower Protection Report*, above n 184, 149 [8.31].
215 *Public Interest Disclosure Act 2013* (Cth) ss 26, 29.
216 *Public Interest Disclosure Act 2013* (Cth) s 33.
217 Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Public Interest Disclosure Bill 2013 [Provisions]* (2013) 21–2.
218 Ibid 22. See Explanatory Memorandum, Public Interest Disclosure Bill 2013 (Cth) 17.

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 improper.[219] 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 section 41 of the *PID Act*, the disclosure will not qualify as a public interest disclosure if it contains 'intelligence information'.[220] The definition of intelligence information includes information that might reveal the sources, technologies, or operations of an intelligence agency,[221] but it also extends more broadly to any 'information that has originated with, or been received from, an intelligence agency'.[222] The definition also includes a summary or extract of any such information.[223] 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'.[224] Many witnesses to the LCA Committee were nonetheless critical of the broad scope of the exemption.[225] Brown has likewise criticised the breadth of section 41, arguing that such a 'blanket carve-out' may not satisfy 'constitutional tests of proportionality, if challenged on constitutional or rights-protection grounds'.[226] In the absence of relevant human rights protections in the *Australian 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'.[227] In the latter case, information will relate to an intelligence agency if the agency 'engages in the conduct'.[228] 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,

---

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

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

221 *Public Interest Disclosure Act 2013* (Cth) s 41(1)(b).

222 *Public Interest Disclosure Act 2013* (Cth) s 41(1)(a).

223 *Public Interest Disclosure Act 2013* (Cth) s 41(1)(e).

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

225 Ibid 23–4. 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* (2013) 51.

226 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.

227 See *Public Interest Disclosure Act 2013* (Cth) s 26(1) items 2(h)–(i).

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

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.[229] 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'.[230] 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 citizens when their statutory mandate is to collect intelligence on 'people or organisations outside Australia'.[231]

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.[232] 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.[233] 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'.[234] However, it is possible that a court could take into account the broad exemption for intelligence information as set out above, and

229 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 1.

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

231 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'.

232 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 3.

233 *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) items 2(h)–(i), which includes exemptions for both intelligence information and information relating to intelligence agencies in the case of an external disclosure.

234 *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'.

thus that immunity from liability in such a case would not therefore be available.[235]

Thirdly, a person would be protected for disclosing information relating to intelligence agencies to an Australian legal practitioner.[236] 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.[237] 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.[238] For this reason, Brown has argued that 'a workable solution in respect of the coverage of intelligence agencies is yet to be found'.[239] 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'.[240]

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 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

235 Brown, above n 226, 29–30.
236 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 4.
237 *Public Interest Disclosure Act 2013* (Cth) s 26(1) items 4(b)–(c).
238 With regard to external disclosures, *Public Interest Disclosure Act 2013* (Cth) s 26(1) items 4(h)–(i) exclude both intelligence information and information relating to intelligence agencies.
239 Brown, above n 226, 30.
240 Ibid.

result given that the explicit objectives of the *PID Act* are to contribute to the integrity and accountability of government.[241]

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,[242] 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

241 *Public Interest Disclosure Act 2013* (Cth) s 6.
242 *Criminal Code* s 100.1.

to a terrorist organisation would receive a lower penalty of 25 years' imprisonment.[243] 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.

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 section 79 of the *Crimes Act* apply criminal penalties not only to the disclosure of information but also to the possession and retention of information.[244] 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.[245] 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.[246] This is the approach currently taken in the terrorism offences and section 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.[247] In particular, sections 70 and 79(3) of the *Crimes Act* and the specific offences for intelligence officers all provide maximum penalties of two 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.[248] 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

243 *Criminal Code* s 102.7(1).
244 See *Criminal Code* ss 91.1(3)–(4), 101.4, 101.5; *Crimes Act 1914* (Cth) ss 79(2)(b)–(c), (4)–(6).
245 See *Secrecy Laws Report*, above n 101, 203 [6.82].
246 Instead of providing 25 years for both: cf *Criminal Code* ss 91.1(1)–(2) (disclosure) with s 91.1(3)–(4) (possession/retention).
247 An exception are the espionage offences where information is recorded or copied with an intention to prejudice security or defence: *Criminal Code* ss 91.1(3)–(4)
248 *Crimes Act 1914* (Cth) ss 70, 79(3); *Intelligence Services Act 2001* (Cth) ss 39, 39A, 40.

where a person intends to harm an essential public interest, such as security, defence or public safety.[249]

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.[250] 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).[251]

Another area in which existing laws require further attention is with regard to the subsequent disclosure scenario. Where Person A commits a criminal offence by communicating information to Person B, and Person B communicates that information to Person C with the same intention as Person A, it is appropriate that Person B should receive the same penalty as Person A. However, section 79 of the *Crimes Act* applies the same penalty to Person B for the mere receipt of information from Person A, before Person B has formed an intention to communicate that information to Person C.[252] 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 section 79 the same penalties can apply. As with the offences for possession and retention of information, this formulation also removes a window of moral opportunity in which Person 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 Person B as for Person 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,[253] the good faith defence for materially assisting the enemy,[254] and the exemption in section 79 of the *Crimes Act* for disclosures made 'in the interest of the Commonwealth'.[255] These are important inclusions, although their scope is

249 *Secrecy Laws Report*, above n 101, 9 (Recommendation 5-1), 138, 160, 324.
250 *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).
251 *Crimes Act 1914* (Cth) s 3. As suggested by ALRC: ALRC, *Secrecy Laws*, above n 101, 9–10 (Recommendation 6-1), 16 (Recommendation 13-3), 480 [13.103]–[13.104].
252 *Crimes Act 1914* (Cth) ss 79(5)–(6).
253 *Criminal Code* s 100.1(3).
254 *Criminal Code* s 80.3.
255 *Crimes Act 1914* (Cth) ss 79(2)(a)(ii), (3)(b).

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.[256] 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.[257]

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).[258] In such a case, there would also need to be 'exceptional circumstances' justifying why the person bypassed the statutory requirement for internal review.[259]

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.[260] 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.

256 *Criminal Code* s 100.1(3)(b)(iv).
257 See *Kessing* (2008) 73 NSWLR 22, 30 [33]; *R v Kessing* [2007] NSWDC 138 [59]–[60] (Bennett DCJ); *Secrecy Laws Report*, above n 101, 57–8.
258 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 3.
259 *Public Interest Disclosure Act 2013* (Cth) s 26(1) item 3(d).
260 *Public Interest Disclosure Act 2013* (Cth) s 26(1) items 2(f), 3(b).