Griffith Journal
of Law & Human Dignity

GRIFFITH JOURNAL OF LAW & HUMAN DIGNITY

Volume 3(1) 2015

Published in May 2014, Gold Coast, Australia by the *Griffith Journal of Law & Human Dignity*
ISSN: 2203-3114

CONTENTS

NATIONAL SECURITY REFORMS AND FREEDOM OF THE PRESS

KEIRAN HARDY*

In October 2014, the Abbott government introduced a 'special intelligence operations' ('SIOs') regime which provides immunity for Australian Security Intelligence Organisation ('ASIO') officers who commit unlawful acts in the course of specially-approved undercover operations. Attached to this regime is a secrecy offence, in s 35P of the Australian Security Intelligence Organisation Act 1979 *(Cth), which prohibits the disclosure of any information relating to SIOs. This article considers the impact of s 35P on press freedom in Australia, and considers options for striking a more appropriate balance between secrecy and accountability. It suggests that a limited public interest exemption based on whistleblower protections in the* Public Interest Disclosure Act 2013 *(Cth) would provide the most viable solution for reducing the impact of s 35P on press freedom.*

* Keiran Hardy is working as a Research Fellow on the ARC Laureate Fellowship on Anti-Terrorism Laws at the Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales. The author would like to thank George Williams for his comments on a draft of this article.

CONTENTS

I INTRODUCTION

> It is our job to hold up to scrutiny the decisions made by those in power. Over the years it has become abundantly clear that highly secretive bodies can abuse their powers in the absence of accountability. It seems ludicrous to talk about fighting for freedom and democracy when journalists are not free to hold to account one of the powerful and secretive agencies in the country […][1]

The United Nations Human Rights Committee has described a 'free, uncensored and unhindered press… [as] one of the cornerstones of a democratic society'.[2] Press freedom is a measure of how much a society values the rights to freedom of opinion and expression. It is also necessary to ensure the enjoyment of other (perhaps all) human rights, as an uncensored press allows information and ideas about public policy to be communicated freely between citizens and their elected representatives.[3] A free press is necessary to maintain both an informed public and an accountable government.

Press freedom in Australia has recently come under threat with the enactment of the *National Security Legislation Amendment Act (No 1) 2014* (Cth) ('NSLAA'). The NSLAA modernises the intelligence-gathering powers of Australia's intelligence agencies and it strengthens criminal offences relating to the disclosure of classified information. It was

[1] Kate McClymont, 'Andrew Olle Media Lecture', *ABC Sydney* (online), 31 October 2014 <http://www.abc.net.au/local/stories/2014/10/31/4118651.htm>.
[2] Human Rights Committee, *General Comment No 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 3 [13].
[3] Ibid 3–4 [13].

the first of three tranches of national security legislation introduced by the Abbott government in 2014. In contrast to the second and third tranches, in which the Abbott government put its own stamp on counter-terrorism law, the NSLAA was the result of a parliamentary inquiry requested by the previous Labor government.[4]

The NSLAA passed both Houses of Parliament on 1 October 2014. The second tranche, which deals directly with the threat of foreign fighters returning from Iraq and Syria, was passed four weeks later.[5] A parliamentary inquiry into the Foreign Fighters legislation was heavily truncated due to that perceived threat.[6] The third tranche, which implements a mandatory data retention regime,[7] was introduced into the House of Representatives on the same day that the Foreign Fighters legislation was passed.

The rapid succession of these national security reforms made it extremely difficult for individuals and organisations to contribute meaningfully to the parliamentary and public debate on the legislation. This was especially concerning given that the legislation introduced some of the most significant and controversial anti-terrorism measures since those introduced in response to the London bombings in 2005.[8]

Of particular concern in the NSLAA is a new offence, found in s 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) ('ASIO Act'), which criminalises the disclosure of information relating to SIOs. SIOs are specially-approved undercover operations in which officers of the ASIO are granted immunity for most unlawful acts. Under s 35P, journalists will not be able to report on SIOs, even if this reveals substantial wrongdoing or unlawful conduct by the ASIO officers involved in an operation. The

[4] See Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (May 2013).
[5] *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (Cth).
[6] See Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (October 2014). Interested parties were given just eight days from the announcement of the inquiry to make submissions to the Committee.
[7] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth).
[8] In particular, the second tranche of national security legislation introduced a new offence of 'advocating' terrorism, and an offence of entering or remaining in a 'declared area': *Criminal Code Act 1995* (Cth) ss 80.2C, 119.2; see Keiran Hardy and George Williams, 'National Security Reforms Stage Two: Foreign Fighters' (2014) 1(7) *Law Society Journal;* Gilbert + Tobin Centre of Public Law, Submission No 3 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*, 1 October 2014, 8–11, 13–15.

offence has been criticised as 'an outrageous attack on press freedom' and 'not worthy of a healthy, functioning democracy'.[9]

The primary justification for s 35P is that the offence will prevent WikiLeaks and Snowden-style scenarios in which "whistleblowing" intelligence officers disclose information to journalists or others.[10] Understandably, governments need to prevent the disclosure of classified information where this would endanger lives or reveal the sources or methods of intelligence agencies. At the same time, there is a strong need to promote transparency and accountability by allowing media outlets to report on wrongdoings by government departments, including intelligence agencies.

This article assesses the impact of s 35P on press freedom in Australia, and explores solutions that could help to strike an appropriate balance between secrecy and accountability in this context. Part II provides an overview of the changes introduced by the NSLAA, including those with respect to ASIO's intelligence-gathering powers. Part III considers the impact of s 35P on press freedom. In particular, this section considers whether there is anything unique about s 35P compared to other existing offences for disclosing sensitive information. Part IV explores potential solutions for limiting the impact of s 35P, such as including an exemption for information disclosed in the public interest. It suggests that a limited public interest exemption based on whistleblower protections in the *Public Interest Disclosure Act 2013* (Cth) would provide the most viable solution to the dangers posed by s 35P.

---

[9] Media, Entertainment and Arts Alliance, *MEAA Says National Security Law an Outrageous Attack on Press Freedom in Australia* (26 September 2014) <http://www.alliance.org.au/meaa-says-national-security-law-an-outrageous-attack-on-press-freedom-in-australia>; Christopher Warren and Mike Dobbie, *Surveillance State Seizes Its Chance*, The Walkley Foundation (24 October 2014) <http://walkleys.com/surveillance-state-seizes-its-chance/>.

[10] See George Brandis, *Press Conference Announcing the Introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (30 October 2014) <http://www.attorneygeneral.gov.au/transcripts/Pages/2014/FourthQuarter2014/30October2014-PressConferenceAnnouncingIntroductionOfTelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill.aspx>. The WikiLeaks saga began in 2010 when Bradley (now Chelsea) Manning downloaded the contents of a secure military database while working as an intelligence analyst for the US military in Iraq. Manning sent the documents to WikiLeaks, a not-for-profit media organisation founded by Julian Assange which specialises in protecting sources who leak classified information. The documents were published in stages on the WikiLeaks website and by major newspapers including *The Guardian*, *The New York Times* and *Der Spiegel*: see generally David Leigh and Luke Harding, 'WikiLeaks: Inside Julian Assange's War on Secrecy', *The Guardian* (online), 10 April 2011. Beginning in June 2013, Edward Snowden released a trove of classified documents from the United States' National Security Agency (NSA): see Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton, 2014).

II THE NSLAA: AN OVERVIEW

The NSLAA makes a large number of amendments to the legal framework surrounding Australia's intelligence agencies. Many of these are technical and uncontroversial, such as formally renaming the defence intelligence agencies and updating employment conditions for ASIO officers.[11] In other areas, however, the Act introduced new powers and offences that are of much greater concern. These changes significantly increase the ability of Australia's intelligence agencies to collect intelligence on Australian citizens, and to keep those activities secret.

One key area of concern relates to ASIO's power to collect intelligence from computers. Section 25A of the ASIO Act allows the Attorney-General, on request by the Director-General of Security (the head of ASIO), to issue a 'computer access warrant'. Previously, such warrants allowed ASIO officers to access data held in a single computer. By virtue of amendments in the NSLAA, a computer access warrant now allows ASIO officers to access data held in one or more computers, computer systems, or computer networks.[12] This includes entering private premises, using reasonable force against persons or things to execute the warrant, and doing anything necessary to conceal the officers' actions.[13] It gives ASIO the power, for example, to access all of the computers located at a university, hospital, or other workplace.

Most public debate has focused on the s 35P disclosure offence, which the NSLAA inserted into the ASIO Act.[14] Section 35P attaches to a new SIO regime, which grants ASIO officers civil and criminal immunity for acts done in the course of special undercover operations that are approved by the Attorney-General.[15] The SIO regime does not provide immunity for acts done by ASIO officers that cause death or serious

[11] *National Security Legislation Amendment (No 1) Act 2014* (Cth) schs 1, 7.
[12] See the definition of computer in *Australian Security Intelligence Organisation Act 1979* (Cth) s 22, as amended by the *National Security Legislation Amendment (No 1) Act 2014* (Cth) sch 2 cl 4.
[13] *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A(4).
[14] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35P.
[15] *Australian Security Intelligence Organisation Act 1979* (Cth) pt III div 4. An SIO may be approved if the Attorney-General is satisfied that the operation 'will assist the Organisation in the performance of one or more special intelligence functions'; *Australian Security Intelligence Organisation Act 1979* (Cth) s 35C(2)(a). A special intelligence function simply means ASIO's normal activities in producing intelligence that is relevant to security, and communicating that intelligence to government departments: *Australian Security Intelligence Organisation Act 1979* (Cth) s 4.

bodily injury, involve the commission of a sexual offence, cause serious property damage, or constitute torture.[16]

The SIO regime is based on the controlled operations regime in Part IAB of the *Crimes Act 1914* (Cth) ('*Crimes Act*'). The controlled operations regime was seen as necessary because law enforcement officers may need to commit criminal acts in order to collect evidence on suspects during undercover "sting" operations. For example, officers of the Australian Federal Police ('AFP') may need to handle large quantities of illegal drugs or access child pornography in order to surveil and ultimately arrest a suspect. The controlled operations regime grants immunity for such acts, so that the officers cannot be prosecuted for conduct that is technically criminal but forms a necessary part of police operations.

Section 35P created an offence, punishable by five years imprisonment, where a person (a) discloses information, and (b) the information relates to an SIO.[17] There are no other elements to this offence, such as an intention to prejudice security or defence by disclosing the information. The person need not even know that the information relates to an SIO, so long as they are reckless as to that fact.[18] This means that the offence will apply where a person is aware of a substantial risk that the information relates to an SIO,[19] and chooses to publish it anyway.

The offence would apply to any person, not just intelligence officers or government contractors. The final version of the Bill included exemptions for information disclosed to the Inspector-General Intelligence of Security or for the purpose of obtaining legal

[16] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35K(e). The prohibition on immunity for torture was added as an amendment after the original Bill was introduced, largely on the basis of criticism by Senator David Leyonhjelm, which was supported by Bret Walker SC, the former Independent National Security Legislation Monitor: see Latika Bourke, 'George Brandis Rules Out Torture Under New National Security Legislation', *Sydney Morning Herald* (online), 22 September 2014 <http://www.smh.com.au/federal-politics/political-news/george-brandis-rules-out-torture-under-new-national-security-legislation-20140922-10k8wg.html>.

[17] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35P(1).

[18] This standard of recklessness was confirmed in the final version of the Bill after a report by the Parliamentary Joint Committee on Intelligence and Security: see Supplementary Explanatory Memorandum, National Security Legislation Amendment Bill (No 1) 2014 (Cth) 7; Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (September 2014) 59–61 ('*Advisory Report on the NSLAA*').

[19] *Criminal Code Act 1995* (Cth) s 5.4(1)(a).

advice in relation to the SIO regime.[20] There is no exemption for information disclosed in the public interest.

There is an aggravated version of this offence, punishable by 10 years imprisonment, where the disclosure endangers the health or safety of any person, or prejudices the undercover operation.[21] This aggravated offence also applies where the person intends such results,[22] although this is framed as an alternative so an intention to cause those results need not be proven for the higher penalty to apply.

In addition to s 35P, the NSLAA strengthened disclosure offences for intelligence officers in two respects. These offences would not apply to journalists, but they are also a core part of the government's attempt to prevent intelligence whistleblowing. First, the NSLAA significantly increased the penalties for existing disclosure offences in the ASIO Act and the *Intelligence Services Act 2001* (Cth), and it introduced new offences so that these are consistent across all of the intelligence agencies.[23] It is now an offence punishable by 10 years imprisonment for an employee of an intelligence agency to disclose information obtained in the course of their duties.

Secondly, the NSLAA introduced new offences for 'unauthorised dealing with records'.[24] These are punishable by three years imprisonment, and apply where an intelligence officer copies or records information in circumstances outside the terms of the person's employment.

These last two categories of disclosure offences are targeted primarily at intelligence officers, but they also apply to those contracted to work for intelligence agencies (thereby addressing the possibility of a Snowden-style scenario) and any other person who has entered into an 'agreement or arrangement' with an intelligence agency.[25] Like

[20] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35P(3)(e)-(g).
[21] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35P(2)(c)(ii).
[22] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35P(2)(c)(i).
[23] *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(2); *Intelligence Services Act 2001* (Cth) ss 39–40B.
[24] *Intelligence Services Act 2001* (Cth) ss 40C–40M.
[25] This last inclusion is problematic as it is not clear that those entering into an 'agreement or arrangement' with an intelligence agency would understand the special obligations surrounding classified information to the same degree: see Keiran Hardy and George Williams, 'Terrorist, Traitor or Whistleblower' (2014) 37(2) *University of New South Wales Law Journal* 784, 808.

s 35P, none of these offences require an intention to cause harm by disclosing the information. Indeed, the unauthorised dealing offences do not even require the information to be disclosed, and will trigger liability before a person has formed an intention to pass that information on to others.

III S 35P AND PRESS FREEDOM

A *Impact on Journalists*

By criminalising the disclosure of any information relating to SIOs, s 35P clearly restricts the ability of media outlets to report on ASIO's activities. Journalists will face five years in prison if they publish any information that relates to an SIO — provided they either know that the information relates to an SIO or are aware of a substantial risk that the information relates to an SIO. This penalty would apply even if disclosing that information would reveal, for example, that ASIO officers did some unlawful act outside the terms of the operation — such as physically harming a suspect, stealing money or property from a suspect's home, or using information gained during the operation to blackmail a person for financial advantage. If publishing the information endangered the safety of any ASIO officers involved in the operation (such as by revealing their identity) or impacted on the success of that operation, the journalist would face twice that penalty.

The rationale for the offence is to prevent intelligence officers from leaking information to journalists about SIOs. Little specific justification was given for s 35P at the time it was introduced,[26] although Attorney-General George Brandis QC later confirmed that the provision was intended to prevent intelligence whistleblowing.[27] This is consistent with the other offences updated and introduced by the NSLAA, which are clearly designed to criminalise whistleblowing by intelligence officers.[28]

When explaining those offences, Brandis referred to 'recent, high-profile international events' — likely the large-scale disclosures by Julian Assange and Edward Snowden — and emphasised that the disclosure of classified information 'can have devastating

[26] See Explanatory Memorandum, National Security Legislation Amendment Bill (No 1) 2014.
[27] Brandis, above n 10.
[28] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18–18B; *Intelligence Services Act 2001* (Cth) pt 6 div 1.

consequences for a country's international relationships and intelligence capabilities'.[29] These consequences were certainly evident when information disclosed by Snowden revealed that Australia's intelligence agencies had spied on senior members of the Indonesian government, and Australia's diplomatic relations with Indonesia were damaged as a result.[30]

At the same time, the need for maintaining secrecy about intelligence operations must be balanced against the need for accountability, and it is clear that s 35P will significantly constrain the media's ability to report on ASIO's activities. This includes, and indeed is specifically designed to prevent, the discussion of conduct by ASIO officers that is contrary to Australian law.

Opposition to s 35P on these grounds is not simply 'business as usual' at the 'biased' national broadcaster.[31] In the Sir Keith Murdoch Oration, Lachlan Murdoch made an impassioned (albeit belated) stand against the provision, arguing that '[w]e certainly do not need further laws to jail journalists who responsibly learn and accurately tell'.[32] He called on journalists and the public to 'be vigilant of the gradual erosion of our freedom to know, to be informed, and make reasoned decisions in our society and in our democracy.'[33]

In response to these concerns, George Brandis issued a directive to the Commonwealth Director of Public Prosecutions ('CDPP') that no prosecution under s 35P will proceed against a journalist unless the CDPP has consulted with and obtained the consent of the Attorney-General of the day.[34] He reassured the public that '[t]here is no possibility, no

---

[29] Commonwealth, *Parliamentary Debates*, House of Representatives, 16 July 2014, 5157.
[30] See George Roberts, 'Indonesia Recalls Ambassador After Leaked Documents Reveal Australia Spied on President Susilo Bambang Yudhoyono', *ABC News* (online), 19 November 2013 <http://www.abc.net.au/news/2013-11-18/indonesia-angered-by-revelations-australia-spied-on-sby/5100264>.
[31] Janet Albrechtsen, 'Business As Usual At Biased Broadcaster', *The Australian* (online), 2 February 2014 <http://www.theaustralian.com.au/opinion/columnists/business-as-usual-at-biased-broadcaster/story-e6frg7bo-1226817953813>.
[32] Lachlan Murdoch, 'A Free Media "Dependent on No One For Favours"', State Library of Victoria (23 October 2014) <http://www.slv.vic.gov.au/audio-video/lachlan-murdoch-free-media>. See Michael Bradley, 'Murdoch's Belated Stand for Press Freedom', *The Drum (ABC)* (online), 24 October 2014 <http://www.abc.net.au/news/2014-10-24/bradley-murdochs-belated-stand-for-press-freedom/5839584>.
[33] Murdoch, above n 32.
[34] Brandis, above n 10.

practical or foreseeable possibility, that in our liberal democracy a journalist would ever be prosecuted for doing their job'.[35]

These are welcome assurances, although they still leave the possibility of prosecuting journalists open to executive discretion. It is not clear that Brandis would stand by his promise if a journalist published information that was 'deeply embarrassing' to the government.[36] Even if he did deny consent to prosecute in such circumstances, it is not clear that future Attorneys-General, from either side of politics, would make the same commitment.[37] This is important given that s 35P is not, like several other controversial counter-terrorism measures,[38] subject to a sunset clause that sets a date for its expiry.

In particular, it is not clear that Brandis would stand by his commitment if a journalist disclosed classified information to the general public for the first time. When pushed on this question on the ABC's *Q&A* program, Brandis responded by saying 'if the event is already disclosed by someone else and a journalist merely reports that which has already been disclosed, as it was by Snowden, then the provision would not be attracted'.[39] It would certainly seem unreasonable for a journalist to be prosecuted in circumstances where an intelligence officer leaks the information to the public at large, and the journalist "re-reports" that information.

However, if an intelligence officer secretly contacts a media outlet, and the media outlet plays a key role in deciding which classified documents are published and in what form they are published (as happened with *The Guardian* newspaper in both the WikiLeaks and Snowden affairs),[40] it seems much more likely that the government would be inclined to prosecute the journalists involved. Brandis has claimed that s 35P was

[35] Ibid.
[36] George Williams, 'Anti-Terror Laws Undermine Democracy', *Sydney Morning Herald* (online), 3 November 2014 <http://www.smh.com.au/comment/antiterror-laws-undermine-democracy-20141102-11fmui.html>.
[37] Ibid.
[38] See *Criminal Code Act 1995* (Cth) s 104.32, 105.53, 119.2(6).
[39] ABC Television, 'National Security: Finding a Balance', *Q&A*, 3 November 2014 (George Brandis) <http://www.abc.net.au/tv/qanda/txt/s4096883.htm>.
[40] See Leigh and Harding, above n 10, 104–115; Greenwald, above n 10, 7–32.

designed primarily to address Snowden-style scenarios,[41] and so this would appear to be precisely the kind of scenario that the offence is designed to target.

In any case, it is clear that s 35P will have a significant chilling effect on the freedom of media outlets to report on ASIO's activities. Consider, for example, if a reporter were informed about dawn raids on the houses of terrorist suspects. They might decline to publish that information out of fear they will be disclosing information that relates to an SIO. Given that a journalist need only be aware of a "substantial risk" that the information relates to an SIO, journalists will likely think twice before publishing anything relating to counter-terrorism operations in which ASIO is involved.

Regardless of whether the government chooses to prosecute journalists under s 35P, the offence is likely to have a significant, indirect impact on press freedom by discouraging journalists from reporting on ASIO's activities and criticising any wrongdoing by the organisation. This impact can already be seen in the substantial opposition to s 35P, and the fear evident amongst media outlets that the government is targeting journalists who report on national security issues.

B *Is s 35P Unique?*

Before exploring potential solutions that might help to reduce the impact of s 35P on press freedom, it is important to clarify what is — and what is not — unique about the offence. Section 35P is *not* unique in prohibiting the disclosure of information relating to national security. Secrecy offences attach to several other counter-terrorism powers, including preventative detention orders ('PDOs'),[42] ASIO's questioning and detention warrant powers,[43] and, most recently, the delayed notification warrant scheme introduced by the Abbott government.[44] Suppression orders issued by courts can also prohibit the disclosure of information relating to the use of such powers in counter-

[41] Brandis, above n 10.
[42] *Criminal Code Act 1995* (Cth) s 105.41.
[43] *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS.
[44] *Crimes Act 1914* (Cth) s 3ZZHA.

terrorism operations.[45] These orders are typically issued to prohibit the disclosure of information that would prejudice a criminal trial.

For example, after large-scale counter-terrorism raids in Sydney in September 2014, the Acting Commissioner for the AFP, Andrew Colvin, was asked how many individuals were being detained and under what legislation. He responded by saying 'I'm not in a position where I can confirm under what legislation or provisions they are being detained'.[46] He later declined to answer again, saying 'it's not trying to be difficult. It's not a question that I can lawfully answer'.[47] It was subsequently revealed that three individuals were detained under the PDO legislation, which includes offences for disclosing information about a person's ongoing detention.[48] The Supreme Court of NSW also issued a broad and indefinite suppression order prohibiting the publication of any information about those orders.[49]

Of particular relevance are the secrecy offences that attach to the controlled operations regime in the *Crimes Act*. These provided the template for s 35P. Section 15HK of the *Crimes Act* makes it an offence where a person (a) discloses information and (b) the information relates to a controlled operation.[50] There is also an aggravated offence, which applies where the disclosure endangers life or safety or prejudices a controlled operation, or where the person intends such.[51] The elements of these offences are directly equivalent to those found in s 35P. There is therefore nothing remarkable about the particular terms in which s 35P has been drafted.

Other secrecy offences could also apply where journalists disclose classified information. For example, under the offence of disclosing "official secrets" in s 79 of the *Crimes Act*, a journalist could face seven years imprisonment for receiving information in

[45] *Court Suppression and Non-Publication Orders Act 2010* (Cth) s 7.
[46] Paul Farrell, 'Terrorism Suspects in Detention: Police Won't Say How Many Are Being Held', *The Guardian* (online), 19 September 2014 <http://www.theguardian.com/world/2014/sep/19/terrorism-suspects-in-detention-police-wont-say-how-many-are-being-held>.
[47] ABC Television, 'Police Used Extraordinary Powers to Detain Without Trial', *Lateline*, 19 September 2014 (Andrew Colvin) <http://www.abc.net.au/lateline/content/2014/s4091562.htm>.
[48] *Criminal Code Act 1995* (Cth) s 105.41.
[49] Paul Farrell, 'Indefinite Ban On Reporting of Counter-Terrorism Preventive Detention Order', *The Guardian* (online), 23 September 2014 <http://www.theguardian.com/world/2014/sep/23/indefinite-ban-reporting-counter-terrorism-preventative-detention-order>.
[50] *Crimes Act 1914* (Cth) s 15HK(1).
[51] *Crimes Act 1914* (Cth) s 15HL(1).

circumstances that would constitute an act of espionage.[52] In contrast to s 35P, the espionage offences in s 91.1 of the *Criminal Code Act 1995* (Cth) require intent to prejudice security or defence.[53] However, this requirement would not likely be difficult to make out in an intelligence whistleblower scenario. For example, a disgruntled intelligence officer might pass on classified information in order to expose and undermine the success of morally dubious intelligence operations.

These other secrecy measures also significantly restrict the ability of journalists to report on national security issues. The Attorney-General was therefore correct, in this respect at least, in referring to s 35P as a 'commonplace law'.[54] And yet, these other offences have not engendered anywhere near the same amount of fear, or attracted anywhere near the same amount of criticism, as s 35P. It is not entirely clear why this is the case.

The most likely reason is that the hype surrounding the WikiLeaks and Snowden affairs has focused public debate on intelligence whistleblowing, and particularly the role of journalists in such disclosures. Fears that journalists would be targeted for disclosing classified information were heightened in 2013 when David Miranda was detained for nearly nine hours at Heathrow airport and his computer equipment seized by UK police.[55] Miranda is the partner of former Guardian journalist Glenn Greenwald, who was involved in the publication of the Snowden material.

Closer to home, concerns expressed by senior members of the Labor Party about s 35P have also fuelled media debate. After the NSLAA was passed, Opposition leader Bill Shorten wrote to the Prime Minister calling on the government to refer the laws to the

---

[52] *Crimes Act 1914* (Cth) s 79(5); see Hardy and Williams, above n 25, 805–806.
[53] *Criminal Code Act 1995* (Cth) s 91.1(1)(b).
[54] ABC Television, 'National Security: Finding a Balance', *Q&A*, 3 November 2014 (George Brandis) <http://www.abc.net.au/tv/qanda/txt/s4096883.htm>.
[55] See Jonathan Watts, 'David Miranda: "They Said I Would Be Put in Jail if I Didn't Co-operate"', *The Guardian* (online), 20 August 2013 <http://www.theguardian.com/world/2013/aug/19/david-miranda-interview-detention-heathrow>; Alan Rusbridger, 'David Miranda, Schedule 7 and the Danger That All Reporters Now Face', *The Guardian* (online), 20 August 2013 <http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters>. The England and Wales High Court originally held that Miranda's detention was lawful and proportionate and did not breach the freedom of expression, although he has been granted leave to appeal that decision: *Miranda v Secretary of State for the Home Department* [2014] EWHC 255 (Admin); Owen Bowcott, 'David Miranda allowed to appeal against ruling on Heathrow detention', *The Guardian* (online), 15 May 2014 <http://www.theguardian.com/world/2014/may/15/david-miranda-appeal-high-court-ruling-detention-heathrow>.

Independent National Security Legislation Monitor.[56] In addition, the Attorney-General's own defence of free speech, to the point of famously claiming a 'right to be a bigot', has added more than a hint of hypocrisy to the offence.[57]

Perhaps above all there is something particularly disagreeable about the idea of granting an intelligence agency a greater capacity to maintain secrecy about its operations. This is where s 35P differs from secrecy offences attaching to police powers such as PDOs or controlled operations, as law enforcement agencies are not surrounded by the same degree of fear and mystery as secret intelligence organisations. In particular, s 35P attaches to a regime which has the core purpose of granting intelligence officers immunity for committing unlawful acts. The idea of allowing ASIO officers to commit crimes, and then cover them up, is something that rightly offends public sentiment. It harks back to the years following 9/11 when the United States Central Intelligence Agency ('CIA') was discredited for sanctioning torture, black sites, and other illegal counter-terrorism operations.

There is no reason to believe that ASIO will be involved in such activities, and the SIO regime does not in any case provide immunity for acts that constitute torture, cause death or cause serious bodily injury.[58] The purpose of the SIO regime will be to prevent the prosecution of ASIO officers for a range of offences that would ordinarily be triggered by an undercover operation, such as participating in training or associating with members of a terrorist organisation.[59] But this last issue really gets to the heart of what makes s 35P exceptional compared to other secrecy offences — and that is that the offence attaches to an exceptional regime.

The SIO regime is exceptional because no comparable nation has seen it necessary to grant a domestic intelligence organisation immunity for committing unlawful acts. Officers of MI5, the United Kingdom's domestic security service, do not receive

[56] 'Bill Shorten Asks Tony Abbott to Review Journalist Terror Laws', *The Australian* (online), 30 October 2014 <http://www.theaustralian.com.au/in-depth/terror/bill-shorten-asks-tony-abbott-to-review-journalist-terror-laws/story-fnpdbcmu-1227106696768>.
[57] Dan Harrison and Jonathan Swan, 'Attorney-General George Brandis: "People Do Have a Right to Be Bigots"', *Sydney Morning Herald* (online), 24 March 2014 <http://www.smh.com.au/federal-politics/political-news/attorneygeneral-george-brandis-people-do-have-a-right-to-be-bigots-20140324-35dj3.html>.
[58] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35K(e).
[59] *Criminal Code Act 1995* (Cth) ss 101.2, 102.8.

immunity for unlawful acts done in the course of their undercover operations.[60] Neither do officers of the New Zealand or Canadian security services.[61] It is therefore difficult to see why such a regime is necessary in Australia.

The government has justified SIOs by pointing to the controlled operations regime,[62] which grants AFP officers immunity for engaging in unlawful conduct to investigate serious criminal offences. However, ASIO is not a law enforcement organisation and, as such, it does not operate under the same rigorous accountability framework. For example, police officers are subject to rigorous procedural rules surrounding the collection of evidence for criminal trials.

In any event, the SIO regime fails to recreate the same safeguards as the controlled operations regime. A controlled operation can only be authorised for an initial period of three months,[63] and then must be renewed intermittently by the Administrative Appeals Tribunal ('AAT').[64] By contrast, an SIO could be authorised at the outset for 12 months.[65] An overview of the AFP's controlled operations is also provided in an annual report,[66] whereas the same detailed reporting requirements do not apply to SIOs.[67]

Another key difference between the SIO and controlled operations regimes is that the penalty for the base offence in s 35P (five years imprisonment)[68] is more than twice that

[60] Officers of MI6 (the UK's foreign intelligence service) may be authorised to perform unlawful acts while operating outside the British Isles, but this power does not extend to officers of MI5, the UK's domestic security service (and equivalent of ASIO): *Intelligence Services Act 1994* (UK) ch 13 s 7. A similar distinction is drawn in Australia: officers of the Australian Secret Intelligence Service (Australia's foreign intelligence agency) will not be liable for unlawful acts done outside Australia if those acts are done in the proper course of the agency's functions, but traditionally this power has not been extended to ASIO officers operating domestically: *Intelligence Services Act 2001* (Cth) s 14.
[61] See *New Zealand Security Intelligence Service Act 1969* (NZ); *Canadian Security Intelligence Service Act 1985* (Can). The United States does not have a direct equivalent of ASIO or MI5, as the Federal Bureau of Investigation (a law enforcement organisation) is the lead agency responsible for domestic counter-terrorism, and the Central Intelligence Agency (CIA) is significantly constrained in its ability to collect intelligence within the United States: *FBI – Domestic Terrorism Post-9/11*, Federal Bureau of Investigation (2009) <http://www.fbi.gov/news/stories/2009/september/domterror_090709>; *Executive Order 12333: United States Intelligence Activities*, 4 December 1981 <https://www.cia.gov/about-cia/eo12333.html>.
[62] *Crimes Act 1914* (Cth) pt IAB.
[63] *Crimes Act 1914* (Cth) s 15GH(4)(c)(i).
[64] *Crimes Act 1914* (Cth) s 15GT.
[65] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35Dd(1)(d).
[66] *Crimes Act 1914* (Cth) s 15HN. See Australian Federal Police, *Controlled Operations Annual Report 2013–14: Part IAB of the Crimes* (2014).
[67] Cf *Australian Security Intelligence Organisation Act 1979* (Cth) s 35Q; *Crimes Act 1914* (Cth) s 15HM.
[68] *Australian Security Intelligence Organisation Act 1979* (Cth) s 35P(1).

for its equivalent in s 15HK of the *Crimes Act* (two years imprisonment).[69] Presumably the rationale for this discrepancy is that the disclosure of information relating to national security creates a greater risk to the safety of the general public compared to disclosures about undercover operations for drug or sex offences. If this is the reason, the government has nonetheless failed to sufficiently explain and justify important differences between the two regimes.

These last points suggest that the most appropriate solutions might lie in improving the SIO regime to ensure parity with its AFP equivalent, rather than redrafting s 35P. Greater accountability could be ensured by requiring intermittent renewal of SIOs by the Security Appeals Division of the AAT.[70] The penalty for the base offence in s 35P should also be reduced from five to two years imprisonment to ensure parity with the disclosure offences in the controlled operations regime.

Above all, the government should make a much stronger case justifying why the SIO regime is necessary. The government has claimed that the regime is necessary because 'some significant investigations either do not commence or are ceased due to the risk that an ASIO employee … could be exposed to criminal or civil liability'.[71] It is impossible to know the accuracy of this statement, though it seems unlikely that ASIO would fail to mount a significant investigation because an operative may technically be guilty of training with a terrorist organisation,[72] or that the government would ever prosecute an ASIO officer for doing so. Why, then, is it necessary to create a general scheme that provides formal immunity for ASIO officers who commit unlawful acts? In the absence of a more convincing explanation as to why SIOs are necessary, suspicions are likely to continue that the regime is designed to sanction morally dubious conduct.

Recognising these other important issues surrounding the SIO regime would help to clarify public debate about s 35P and its impact on press freedom. In particular, s 35P

[69] *Crimes Act 1914* (Cth) s 15HK(1).
[70] Some improved accountability mechanisms were already included in the final version of the Bill, such as requiring authorisation by the Attorney-General rather than the Director-General of Security, and requiring the Inspector-General of Intelligence and Security ('IGIS') to be notified whenever an SIO is approved: *Australian Security Intelligence Organisation Act 1979* (Cth) ss 35B, 35PA. See PJCIS, *Advisory Report on the NSLAA*, above n 18, 59–61.
[71] Explanatory Memorandum, National Security Legislation Amendment (No 1) Bill 2014 (Cth) 14.
[72] *Criminal Code Act 1995* (Cth) s 101.2

should be viewed as one in a long list of secrecy offences that prohibit the disclosure of information relating to national security. This would help to redirect public debate towards a much larger problem as to the legislative balance currently struck between secrecy and accountability.

Clarifying public debate in this way will not, however, solve the key problem at hand — which is that s 35P in its current form will significantly constrain the ability of journalists to report on ASIO's activities. Even if the penalty were appropriately reduced, the chilling effect of the offence on free speech is still likely to be significant. The next section considers some more specific options for rewording the offence to avoid this danger.

IV REMEDYING S 35P

One possible amendment that would reduce the impact of s 35P on press freedom would be to include an exemption for journalists. This appears to be the simplest and most direct solution to the problem, although there are reasons why such an exemption could prove problematic.

In its inquiry into the NSLAA, the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') concluded that such an exemption would grant too many bloggers and other informal 'reporters' a licence to damage intelligence operations:

> [T]he Committee does not consider it appropriate to provide an explicit exemption for journalists from the proposed offence provisions. Part of the reason for this is that the term 'journalism' is increasingly difficult to define as digital technologies have made the publication of material easier. The Committee considers that it would be all too easy for an individual, calling themselves a 'journalist', to publish material on a social media page or website that had serious consequences for a sensitive intelligence operation.[73]

[73] PJCIS, *Advisory Report on the NSLAA*, above n 18, 62 [3.101].

These concerns are valid, although it would be possible to restrict such an exemption to those producing news reports 'in a professional capacity',[74] or some similar wording that would allow established media outlets to report responsibly on SIOs.

The more fundamental reason why an exemption for journalists would be problematic is that it does not make sense in a liberal democracy founded on the rule of law to say that a criminal offence applies to everyone except individuals working in a certain profession. The idea that laws should have a general application — that is, that they should apply equally to every person, including the highest members of government — is a central tenet of the rule of law. An exemption for journalists, however well intentioned, would sit uneasily with this fundamental principle.

A more appropriate possibility would be to include a defence for individuals who disclose information in the public interest.[75] This would avoid the issue of exempting a category of persons from the offence, as it would apply to any person who disclosed sensitive information where it was in the public interest to disclose that information. The idea is that a public interest exemption would allow journalists to reveal information about SIOs in circumstances where, for example, it could be shown that ASIO officers had engaged in substantial wrongdoing or unlawful conduct such as false imprisonment or torture.

The difficulty with such an exemption, however, lies in determining what constitutes the 'public interest'. In particular, journalists and courts appear to have different ideas as to what these words mean. To journalists (or at least this appears to be the implication behind calls for a public interest defence), disclosing sensitive information would be in the public interest if it exposed the morally dubious or unlawful actions of intelligence officers. In other words, there is some public benefit to be gained in terms of the transparency and accountability of government by disclosing that information, even if the information is operationally sensitive. This is the logic underlying support for the large-scale disclosures by Chelsea Manning, Julian Assange, and Edward Snowden. For example, the WikiLeaks material revealed that US soldiers had killed innocent civilians

[74] This wording was included in the offence of entering or remaining in a 'declared area', as introduced by the second tranche of national security legislation: *Criminal Code Act 1995* (Cth) s 119.2(3)(f).
[75] See, eg, McClymont, above n 1; Williams, above n 36.

in Iraq and Afghanistan.[76] While this information related to ongoing military operations, there was clearly significant public interest (in terms of transparency, accountability, and public knowledge) in exposing the actions of the soldiers involved.

A court, however, may approach considerations of the public interest from a different perspective. It is difficult to know how a court would apply a public interest exemption specifically in the context of s 35P, but it seems unlikely that a court would hold the disclosure of information to be in the public interest if it contained any information relating to ongoing or recent intelligence operations.

In *Commonwealth v Fairfax*,[77] the High Court considered an injunction to prevent two newspapers from publishing extracts from an upcoming book. The book contained classified documents on Australia's defence and foreign policy. The court denied the government's claim to protect the information on public interest grounds,[78] as it considered that the documents, which were largely historical, had ceased to be a significant security risk.[79] The court believed that it would be 'unacceptable in our democratic society' to restrain the publication of information merely because it would expose the government to public discussion, criticism, and embarrassment.[80]

At the same time, however, the court suggested that it would have restrained publication of the extracts if they included information relevant to current defence operations or policy.[81] It held that the disclosure of information would be contrary to the public interest where it appeared that the disclosure would prejudice 'national security, relations with foreign countries or the ordinary business of government'.[82]

Given the High Court's approach in *Fairfax*, it seems unlikely that any exemption referring generally to the 'public interest', or some such similar phrase,[83] would give

[76] Christ McGreal, 'Wikileaks Reveals Video Showing US Air Crew Shooting Down Iraqi Civilians', *The Guardian* (online), 5 April 2010 <http://www.theguardian.com/world/2010/apr/05/wikileaks-us-army-iraq-attack>.
[77] (1980) 147 CLR 39.
[78] Ibid [37], although the court upheld the government's claim on copyright grounds: see [55]–[56].
[79] Ibid [33]–[34].
[80] Ibid [27], [35], [37].
[81] Ibid [29].
[82] Ibid.
[83] For example, the offence of disclosing official secrets contains a defence where it is a person's duty to disclose the information 'in the interest of the Commonwealth': *Crimes Act 1914* (Cth) s 79(2)(a)(ii).

journalists much scope to disclose information about SIOs. Information about SIOs will relate to ongoing or at least recent intelligence operations, so it seems likely that a court would hold the disclosure of such information to be operationally sensitive and therefore contrary to the public interest.

If a journalist revealed some very significant wrongdoing by ASIO officers during an SIO (such as planting evidence, or subjecting suspects to physical abuse), while being very careful not to reveal any names, sources, or methods relevant to that operation, it is possible that a court would permit disclosure under a public interest exemption. It is also possible that journalists would be permitted to report on past SIOs that are no longer operationally relevant. However, these would likely be in rare circumstances, and it would take a brave journalist to risk 10 years in prison when it is not clear how a court would decide the issue. Moreover, the ability to report on past SIOs would not permit discussion of important current affairs. It therefore seems likely that s 35P — even if it included a public interest exemption — would still have a significant chilling effect on the ability of journalists to report on ASIO's activities.

This effect could be reduced if a public interest exemption referred explicitly to the kinds of serious misconduct that journalists would be seeking to expose. Some guidance can be taken here from the *Public Interest Disclosure Act 2013* (Cth) ('PID Act'), which establishes a formal whistleblowing scheme for public officials. The PID Act provides immunity from civil, criminal, and administrative liability for public officials who disclose wrongdoing by government departments according to a specified procedure.[84] These protections are not available to journalists, and they would only be available to intelligence officers in very limited circumstances due to broad exemptions for intelligence information.[85] However, the principles underlying the scheme could provide a basis for drafting a more targeted exemption to s 35P.

For public officials to receive immunity under the PID Act, the information they disclose must fall within the definition of 'disclosable conduct'.[86] This encourages responsible disclosures, as whistleblowers will only receive protection if they disclose information

[84] *Public Interest Disclosure Act 2013* (Cth) s 10(1).
[85] *Public Interest Disclosure Act 2013* (Cth) ss 33, 41.
[86] *Public Interest Disclosure Act 2013* (Cth) s 29.

that reveals serious wrongdoing. The definition of disclosable conduct specifies a range of categories, including information about conduct which:

- contravenes a law of the Commonwealth, a state or a territory;
- perverts the course of justice or involves corruption of any kind;
- constitutes maladministration (including conduct that is based on improper motives; is unreasonable, unjust, or oppressive; or is negligent);
- is an abuse of public trust;
- results in the wastage of public money or property;
- unreasonably results in a danger to the health or safety of one or more persons; or
- results in an increased risk of danger to the environment.[87]

An exemption to s 35P could permit disclosure of information in the public interest, and then define the public interest by reference to more specific categories such as these. In other words, the disclosure of information about SIOs would be in the public interest if it revealed unlawful conduct, corruption, unreasonable danger to health or safety, or other similar wrongdoing. This definition of the public interest should be non-exhaustive so that courts could permit disclosures along similar lines as new circumstances arise. These considerations could then be balanced against the risk that the information will prejudice security, defence, or foreign relations.[88]

The advantage of this more targeted approach is that a court would be directed to consider whether the disclosure of information relating to SIOs would reveal serious wrongdoing or unlawful conduct by ASIO or its officers. This could give more significant weight to these considerations, whereas under a broad exemption that referred only to the 'public interest' and left the meaning open to interpretation by the courts, there is a greater risk that considerations of misconduct will be overlooked in favour of protecting operationally-sensitive information.

[87] *Public Interest Disclosure Act 2013* (Cth) s 29.
[88] As in *Public Interest Disclosure Act 2013* (Cth) s 26(3)(a).

An exemption along these lines may have a more limited scope, as it would direct courts to define the public interest according to a narrower range of misconduct, as opposed to anything that might promote discussion about public affairs. The trade-off, however, is that it could provide greater peace of mind to journalists, as the kinds of serious misconduct they are seeking to expose would be explicitly provided for in the legislation. The government may also be more willing to accept a public interest exemption that is drafted carefully along these lines, compared to one of broad and uncertain scope.

If this were still too broad an exemption for the government to accept, the legislation could include a requirement, along the lines of that included in the PID Act, that the person reveal no more information than is necessary to demonstrate one or more instances of wrongdoing.[89] This would further encourage responsible reporting on SIOs, as it would protect against WikiLeaks-style scenarios in which entire intelligence databases are leaked to the public. A person who disclosed large amounts of classified information would not be able to rely on the defence simply because some small portion of the information they disclosed was in the public interest.

An exemption to s 35P that drew on the approach of the PID Act in this way could perhaps be better described as a 'whistleblower defence' rather than a 'public interest' defence. It would play an important role in protecting freedom of the press by allowing journalists to report on instances of serious wrongdoing by ASIO officers involved in SIOs. However, it would do so in a more limited way, by directing considerations of the public interest towards a narrower range of serious misconduct and unlawful activity. As such, it would be a relatively small concession to the government, which should not in any case need to be covering up instances of serious misconduct by its intelligence agencies. Indeed, the government could significantly benefit its public image by introducing such an amendment. The government could uphold its outward commitment to free speech, while maintaining sufficiently strong protections for information relating to ASIO's secret activities.

[89] *Public Interest Disclosure Act 2013* (Cth) s 26(1) (Item 2 Column 3(f)).

V CONCLUSION

The s 35P disclosure offence introduced by the NSLAA has attracted significant criticism for restricting freedom of the press in Australia. In criminalising the disclosure of any information relating to SIOs, s 35P impacts directly on the ability of journalists to report on ASIO's activities. The offence is also likely to have a significant indirect impact on press freedom by deterring journalists from reporting on any counter-terrorism operations in which ASIO is involved.

Section 35P has received a surprising amount of public attention given that several other secrecy offences also prevent journalists from reporting on national security issues. Nonetheless, criticisms of s 35P are warranted in that the offence prohibits disclosure of information relating to an exceptional undercover operations regime. No comparable nation has deemed it necessary to grant formal immunity to officers of a domestic security service for committing unlawful acts. If ASIO officers are to commit unlawful acts during the course of their undercover operations, this should be the subject of rigorous and ongoing public critique, provided that revealing such information does not endanger any lives or prejudice intelligence operations. It is possible that a responsible discussion could be had about such matters but the blanket disclosure offences in s 35P will prevent *any* discussion about SIOs regardless of the impact that discussion might have on safety or security.

The most direct solution to these problems would be to exempt journalists from the offence, but this would not sit well with the fundamental principle of the rule of law that criminal offences should apply equally to every person in society. A more appropriate alternative would be to include an exemption for information disclosed in the public interest. A public interest exemption should be included in s 35P in order to protect the freedom of journalists to report on issues of public importance. While the government understandably needs to protect intelligence sources and methods, the public needs to be informed when intelligence agencies engage in corrupt, unlawful or unnecessarily dangerous conduct in the name of protecting our security.

For this exemption to have the desired effect, it should define the public interest by reference to categories of serious wrongdoing, such as those included in the PID Act. This

'whistleblower defence' would reduce the chilling effect on journalists because it would refer explicitly to the kinds of serious misconduct they would be seeking to expose. The government would also be more likely to accept such an amendment, as it would encourage responsible disclosures about SIOs in a narrower range of circumstances.

If the government were to explore this possibility, it could open up a much larger discussion as to the balance that is currently struck between secrecy and accountability in other legislation. If such a defence proved viable, it could provide a model for drafting exemptions to other criminal offences which unduly restrict freedom of the press. Indeed, a case might eventually be made for consolidating such defences into a 'whistleblowers charter' for journalists, in which media outlets would be protected for reporting responsibly on issues of public importance.

REFERENCE LIST

A *Articles/Books/Reports*

Australian Federal Police, *Controlled Operations Annual Report 2013-14: Part IAB of the Crimes* (2014)

Greenwald, Glenn, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton, 2014)

Hardy, Keiran, and George Williams, 'National Security Reforms Stage Two: Foreign Fighters' [2014] 1(7) *Law Society Journal* 68

Hardy, Keiran, and George Williams, 'Terrorist, Traitor or Whistleblower' (2014) 37(2) *University of New South Wales Law Journal* 784

Leigh, David, and Luke Harding, 'WikiLeaks: Inside Julian Assange's War on Secrecy', *The Guardian* (online), 10 April 2011

Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (October 2014)

Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (September 2014)

Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (May 2013)

B *Cases*

Commonwealth v Fairfax (1980) 147 CLR 39

Miranda v Secretary of State for the Home Department [2014] EWHC 255 (Admin)

C *Legislation*

Australian Security Intelligence Organisation Act 1979 (Cth)

Canadian Security Intelligence Service Act 1985 (Can)

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 (Cth)

Court Suppression and Non-Publication Orders Act 2010 (Cth)

Crimes Act 1914 (Cth)

Criminal Code Act 1995 (Cth)

Intelligence Services Act 1994 (UK)

Intelligence Services Act 2001 (Cth)

National Security Legislation Amendment (No 1) Act 2014 (Cth)

New Zealand Security Intelligence Service Act 1969 (NZ)

Public Interest Disclosure Act 2013 (Cth)

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth)

E *Other*

ABC Television, 'National Security: Finding a Balance', *Q&A*, 3 November 2014 (George Brandis) <http://www.abc.net.au/tv/qanda/txt/s4096883.htm>

ABC Television, 'Police Used Extraordinary Powers to Detain Without Trial', *Lateline*, 19 September 2014 (Andrew Colvin) <http://www.abc.net.au/lateline/content/2014/s4091562.htm>

Albrechtsen, Janet, 'Business As Usual At Biased Broadcaster', *The Australian* (online), 2 February 2014 <http://www.theaustralian.com.au/opinion/columnists/business-as-usual-at-biased-broadcaster/story-e6frg7bo-1226817953813>

'Bill Shorten Asks Tony Abbott to Review Journalist Terror Laws', *The Australian* (online), 30 October 2014 <http://www.theaustralian.com.au/in-depth/terror/bill-

shorten-asks-tony-abbott-to-review-journalist-terror-laws/story-fnpdbcmu-1227106696768>

Bourke, Latika, 'George Brandis Rules Out Torture Under New National Security Legislation', *Sydney Morning Herald* (online), 22 September 2014 <http://www.smh.com.au/federal-politics/political-news/george-brandis-rules-out-torture-under-new-national-security-legislation-20140922-10k8wg.html>

Bowcott, Owen, 'David Miranda allowed to appeal against ruling on Heathrow detention', *The Guardian* (online), 15 May 2014 <http://www.theguardian.com/world/2014/may/15/david-miranda-appeal-high-court-ruling-detention-heathrow>

Bradley, Michael, 'Murdoch's Belated Stand for Press Freedom', *The Drum (ABC)* (online), 24 October 2014 <http://www.abc.net.au/news/2014-10-24/bradley-murdochs-belated-stand-for-press-freedom/5839584>

Brandis, George, *Press Conference Announcing the Introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (30 October 2014) <http://www.attorneygeneral.gov.au/transcripts/Pages/2014/FourthQuarter2014/30October2014-PressConferenceAnnouncingIntroductionOfTelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill.aspx>

Commonwealth, *Parliamentary Debates*, House of Representatives, 16 July 2014, 5157

Executive Order 12333: United States Intelligence Activities, 4 December 1981 <https://www.cia.gov/about-cia/eo12333.html>

Explanatory Memorandum, National Security Legislation Amendment (No 1) Bill 2014 (Cth)

Farrell, Paul, 'Indefinite Ban On Reporting of Counter-Terrorism Preventive Detention Order', *The Guardian* (online), 23 September 2014 <http://www.theguardian.com/world/2014/sep/23/indefinite-ban-reporting-counter-terrorism-preventative-detention-order>

Farrell, Paul, 'Terrorism Suspects in Detention: Police Won't Say How Many Are Being Held', *The Guardian* (online), 19 September 2014 <http://www.theguardian.com/world/2014/sep/19/terrorism-suspects-in-detention-police-wont-say-how-many-are-being-held>

FBI – Domestic Terrorism Post-9/11, Federal Bureau of Investigation (2009) <http://www.fbi.gov/news/stories/2009/september/domterror_090709>

Gilbert + Tobin Centre of Public Law, Submission No 3 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*, 1 October 2014

Harrison, Dan, and Jonathan Swan, 'Attorney-General George Brandis: "People Do Have a Right to Be Bigots"', *Sydney Morning Herald* (online), 24 March 2014 <http://www.smh.com.au/federal-politics/political-news/attorneygeneral-george-brandis-people-do-have-a-right-to-be-bigots-20140324-35dj3.html>

Human Rights Committee, *General Comment No 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011)

Lachlan Murdoch, 'A Free Media "Dependent on No One For Favours"', State Library of Victoria (23 October 2014) <http://www.slv.vic.gov.au/audio-video/lachlan-murdoch-free-media>

McClymont, Kate, 'Andrew Olle Media Lecture', *ABC Sydney* (online), 31 October 2014 <http://www.abc.net.au/local/stories/2014/10/31/4118651.htm>

McGreal, Christ, 'Wikileaks Reveals Video Showing US Air Crew Shooting Down Iraqi Civilians', *The Guardian* (online), 5 April 2010 <http://www.theguardian.com/world/2010/apr/05/wikileaks-us-army-iraq-attack>

Media, Entertainment and Arts Alliance, *MEAA Says National Security Law an Outrageous Attack on Press Freedom in Australia* (26 September 2014) <http://www.alliance.org.au/meaa-says-national-security-law-an-outrageous-attack-on-press-freedom-in-australia>

Roberts, George, 'Indonesia Recalls Ambassador After Leaked Documents Reveal Australia Spied on President Susilo Bambang Yudhoyono', *ABC News* (online), 19

November 2013 <http://www.abc.net.au/news/2013-11-18/indonesia-angered-by-revelations-australia-spied-on-sby/5100264>

Rusbridger, Alan, 'David Miranda, Schedule 7 and the Danger That All Reporters Now Face', *The Guardian* (online), 20 August 2013 <http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters>

Supplementary Explanatory Memorandum, National Security Legislation Amendment Bill (No 1) 2014 (Cth)

Warren, Christopher, and Mike Dobbie, *Surveillance State Seizes Its Chance*, The Walkley Foundation (24 October 2014) <http://walkleys.com/surveillance-state-seizes-its-chance/>

Watts, Jonathan, 'David Miranda: "They Said I Would Be Put in Jail if I Didn't Co-operate"', *The Guardian* (online), 20 August 2013 <http://www.theguardian.com/world/2013/aug/19/david-miranda-interview-detention-heathrow>

George Williams, 'Anti-Terror Laws Undermine Democracy', *Sydney Morning Herald* (online), 3 November 2014 http://www.smh.com.au/comment/antiterror-laws-undermine-democracy-20141102-11fmui.html