

Bond University

Bond Law Review

Volume 34

Issue 1

2022

Hear no Evil, See no Evil, Speak no Evil: The Secretisation of Information
by Government in Australia

Kylie Weston-Scheuber
Victorian Bar

Follow this and additional works at: <https://blr.scholasticahq.com/>



This work is licensed under a [Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 Licence](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Hear no Evil, See no Evil, Speak no Evil: The Secretisation of Information by Government in Australia

KYLIE WESTON-SCHEUBER*

(H)istory ... shows that in countries where democratic institutions have been unconstitutionally superseded, it has been done not seldom by those holding the executive power ... the power to legislate for the protection of an existing form of government ought not to be based on a conception ... adequate only to assist those holding power to resist or suppress obstruction or opposition or attempts to displace them or the form of government they defend.¹

I Introduction

In October 2019, the front pages of both national newspapers and all major metropolitan papers featured the same thing: a heavily redacted memo saying, “When government keeps the truth from you, what are they covering up?”²

The catalyst for this unprecedented media synchronicity was media concern following police raids on the ABC and a News Corporation journalist, Annika Smethurst, for their reporting on, respectively, alleged war crimes in Afghanistan, and plans for government surveillance on citizens. The “Your Right to Know” campaign that the headlines heralded was a reaction to what was perceived as an impermissible attempt by government to suppress the free flow of information.

The concept of state secrecy is not new. Nor is the concept that the protection of information sensitive to the state, in particular information relating to national security, may warrant limitations on the rights of

* Dr Kylie Weston-Scheuber BMus, BA/LLB (Hons), PhD, AICD is a barrister at the Victorian Bar. This article is the written version of the inaugural Legal and Social Change Lecture for the Bond University Global and Comparative Law and Policy Network delivered on 26 May 2021. The author wishes to thank Jeremy Armour, Joud Ghassali and Alankrita Malhotra for research assistance and Professor Rachael Field, Dr Victoria Baumfield and Grace Georgilopoulos for editorial assistance, together with Professor Jonathan Crowe and the Global and Comparative Law and Policy Network for the opportunity to present the lecture on which the paper is based.

¹ *Australian Communist Party v Commonwealth* (1951) 83 CLR 1, 187-8 (Dixon J).

² Joshua McDonald, “Your Right to Know’ Campaign Launches Against Government Secrecy in Australia’, *The Diplomat* (online, 16 April 2021) <<https://thediplomat.com/2019/10/your-right-to-know-campaign-launches-against-government-secrecy-in-australia/>>.

individuals, for example the right to freedom of expression and the right to a fair trial.

State secrecy provisions have existed for a long time in common law countries. In the United Kingdom, the *Official Secrets Acts* of 1899 and 1911 were enacted in response to instances of the media publishing state secrets.³ In Australia, the first state secrets laws were the *Post and Telegraph Act 1901* (Cth) ss 9 and 127 and *Crimes Act 1914* (Cth) ('Crimes Act') s 79.⁴ The Australian Law Reform Commission ('ALRC') has observed that official secrecy was the norm for most of Australia's history, until the rise of the 'new administrative law' constituted by the *Administrative Appeals Tribunal Act 1975* (Cth), the *Freedom of Information Act 1982* (Cth) ('FOI Act') and other reformative laws of the 1970s and 1980s.⁵

ANU academic Hitoshi Nasu notes that globally, freedom of information laws developed much later in the 20th century as an essential component of freedoms of opinion and expression. In parallel to this growth, more specialised state secrets legislation was enacted, which focused on prohibition of the disclosure of state secrets.⁶

Over time, state secrets laws have broadened in scope due to the expansion and diversification of meanings of 'national security', intermingling of the security interests of different states, the rise of 'mosaic theory' and the speed of travel of individuals and communications.⁷ Mosaic theory has been used for decades by governments to classify documents at higher levels and to withhold documents from Freedom of Information ('FOI') requests.⁸

In the International Covenant on Civil and Political Rights ('ICCPR') and other human rights instruments, the right to freedom of expression is qualified by exceptions necessary for the protection of national security. However, there is a difficult balance to be achieved between the public interest in avoiding harm to national security, and the public interest in disclosing matters that should rightfully be in the public domain, including information that it is necessary to disclose in the interests of government accountability.

In Australia, the trend towards suppression of the free flow of information, particularly in recent years, suggests that this delicate balance has been overthrown. The UN Special Rapporteur on Human Rights Defenders, for example, has warned in relation to the ABC and

³ Hitoshi Nasu, 'State Secrets Law and National Security' (2015) 64(2) *International & Comparative Law Quarterly* 365.

⁴ Ibid.

⁵ Australian Law Reform Commission, *Secrecy Laws and Open Government* (Report No 112, December 2009) [2.5], [2.7], [2.13]-[2.18].

⁶ Nasu (n 3) 369-71.

⁷ Nasu (n 3). 'Mosaic theory' is the concept that separate items of information, while individually limited, can take on significance when combined with other pieces of information.

⁸ David E Pozen, 'The Mosaic Theory, National Security, and the Freedom of Information Act' (2005) 115(3) *Yale Law Journal* 628.

Smethurst raids that the charges may have a chilling effect on Australian journalism.⁹

The Parliamentary Joint Committee on Intelligence and Security ('PJCIS'), reporting in the context of an inquiry following these events, noted that the 'prevailing argument' from non-government stakeholders was 'that the balance in legislation and culture within the Australian Government has tipped away from transparency and engagement to excessive and unnecessary secrecy'.¹⁰ They also noted the chilling effect on journalists that the operation of national security laws has had.¹¹

In recent years, the Australian government has been criticised for secrecy in a number of areas, including border protection, foreign aid, freedom of information and more generally.¹²

⁹ Jennifer Robinson, 'Press Freedom Under Threat from National Security Law Spree', *The Sydney Morning Herald* (online, 21 October 2019) <<https://www.smh.com.au/national/press-freedom-under-threat-from-national-security-law-spree-20191020-p532f8.html>>.

¹⁰ Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Final Report, August 2020) [2.73] ('*Law Enforcement and Intelligence Powers on the Freedom of the Press*').

¹¹ Ibid [2.102]-[2.107].

¹² Heath Aston, 'Abbott Government Under Fire For Secret Bid To Hand Back Asylum Seekers To Vietnam', *The Sydney Morning Herald* (online, 17 April 2015) <<https://www.smh.com.au/politics/federal/abbott-government-under-fire-for-secret-bid-to-hand-back-asylum-seekers-to-vietnam-20150417-1mnlpb.html>>; Adam Gartrell, 'Savage Cuts and Secrecy: The Abbott Government's New Aid Paradigm', *The Sydney Morning Herald* (online, 12 June 2015) <<https://www.smh.com.au/politics/federal/savage-cuts-and-secrecy-the-abbott-governments-new-aid-paradigm-20150612-ghm9mu.html>>; Sophie Morris, 'Abbott Government Weakens FOI and Public Service Disclosure', *The Saturday Paper* (online, 20-26 June 2015) <<https://www.thesaturdaypaper.com.au/news/politics/2015/06/20/abbott-government-weakens-foi-and-public-service-disclosure/14347224002030#hrd>>; Rodney Tiffen, 'The Abbott Government's War On Transparency', *Inside Story* (online, 5 June 2014) <<https://insidestory.org.au/the-abbott-governments-war-on-transparency/>>; Amy Nethery and Rosa Holman, 'Secrecy and Human Rights Abuse in Australia's Offshore Immigration Detention Centres' (2016) 20(7) *The International Journal of Human Rights* 1018; Maureen Henninger, 'Reforms To Counter A Culture Of Secrecy: Open Government In Australia' (2018) 35(3) *Government Information Quarterly* 398; Kim McGrath, 'Drawing The Line: Witness K and The Ethics Of Spying' [2020] (9) *Australian Foreign Affairs* 53; Jude McCulloch and Joo-Cheong Tham, 'Secret State, Transparent Subject: The Australian Security Intelligence Organisation In The Age of Terror' (2005) 38(3) *Australian and New Zealand Journal of Criminology* 400; Mark Rix, 'Security without Secrecy? Counterterrorism, ASIO and Access To Information' in Daniel Baldino (ed), *Spooked: The Truth About Intelligence in Australia* (NewSouth Publishing, 2013) 240; Keiran Hardy and George Williams, 'National Security Reforms Stage One: Intelligence Gathering and Secrecy' (2014) 6 *LSJ: Law Society of NSW Journal* 68; Christopher Knaus, 'Bernard Collaery Case: Lawyers for Attorney General Call for Redactions of Judgement That Lifted Secrecy Orders', *The Guardian* (online, 2 November 2021) <<https://www.theguardian.com/world/2021/nov/02/bernard-collaery-case-lawyers-for-attorney-general-call-for-redactions-of-judgment-that-lifted-secrecy-orders>>; Richard Ackland, 'Suppression and Secrecy: How Australia's Government Put a Boot on Journalism's Throat', *The Guardian* (online, 1 September 2019) <<https://www.theguardian.com/commentisfree/2019/sep/01/suppression-and-secrecy-how-australias-government-put-a-boot-on-journalisms-throat>>; Georgie Moore, 'Alarm Over Australian 'Culture of Secrecy'', *The Canberra Times* (online, 6 September 2021) <<https://www.canberratimes.com.au/story/7417239/alarm-over-australian-culture-of->

This article draws together commentary and recent examples in relation to state secrecy provisions in a range of different areas, and considers the use of secrecy by the government in Australia, with some relevant comparisons to other common law countries. This extends beyond the secrecy offences that would ordinarily be referred to under the umbrella of ‘state secrecy’ to other laws that may be utilised to keep government information secret, for example closed court orders and FOI exemptions. Broadly, the article outlines a series of laws and patterns of decision-making that together combine to effect an approach to the free flow of information of “Hear no evil, speak no evil, see no evil”.

The article will examine:

Hear no evil:

- (a) the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) (‘NSI Act’) and its application;

See no evil:

- (b) restrictions on FOI and access to Commonwealth records, with a particular focus on the Palace Papers litigation;

Speak no evil:

- (c) the prosecution of whistleblowers in relation to those who reveal information in the public interest;
- (d) suppression and restrictions on media reporting of matters in the public interest; and
- (e) the implied freedom of political communication and its potential to protect the free flow of information.

Through these various, often overlapping, aspects of state secrecy law, it is argued here that there is an increasing and alarming tendency in Australia towards suppression of the free flow of information that the state postulates as needing to be kept secret in the national interest. These developments are concerning on a number of levels, and require deeper scrutiny and questioning.

secrecy/>; Ben Doherty, “Authoritarian-Style’ Law Would Allow Australia to Use Secret Evidence to Deport Migrants’, *The Guardian* (online, 11 October 2021) <<https://www.theguardian.com/australia-news/2021/oct/11/authoritarian-style-law-would-allow-australia-to-use-secret-evidence-to-deport-migrants>>.

II Hear no Evil – Secret Trials and Restriction of Access to Information Under the NSI Act

A. *The National Security Information Act*

‘Open justice is one of the most fundamental aspects of the system of justice in Australia.’¹³

‘The case is too trifling to need a lawyer, but I could do very well with an advisor.’ ‘Yes, but if I am to be an advisor I must know what it’s all about,’ said Fraulein Burstner. ‘That’s just the snag,’ said K. ‘I don’t know that myself.’¹⁴

The principle of open justice is fundamental to our legal system. It has three aspects: first, the conduct of proceedings in open court; secondly, that evidence presented in court is communicated to those present, and thirdly, the fair and accurate reporting of proceedings.¹⁵

The Universal Declaration of Human Rights article 10 provides that everyone is entitled in full equality to a fair and *public hearing* by an independent and impartial tribunal in the determination of rights and obligations and any criminal charge. The right is also enshrined in article 14 of the ICCPR and article 6 of the European Convention on Human Rights. Like all human rights, these rights are subject to limitation where that is proportionate and adapted to a legitimate public purpose.

The principle of open justice is crucial to the maintenance of transparency and accountability of government. Particularly where criminal proceedings are initiated by the state against individuals, the conduct of proceedings in open court ensures that those proceedings are available to the public, and to be reported on by the media, ensuring that individuals are held publicly to account for their crimes, and also that the process of the state’s enforcement of the law is open to scrutiny.

For that reason, a court can only depart from the open justice principle where the administration of justice would be frustrated, or some other public interest for whose protection Parliament has modified the rule, would be frustrated. A departure from the open justice rule must be really necessary to secure the proper administration of justice. An order must do no more than is necessary to achieve the due administration of justice.¹⁶

There are a number of recognised exceptions to the open justice principle. For example, courts are routinely closed where open proceedings would identify a police informer or the victim of blackmail,

¹³ *R v Lodhi* [2006] NSWSC 596, [6] (Whealy J).

¹⁴ Franz Kafka, *The Trial* (Vintage, 1925) 29.

¹⁵ Jason Bosland and Ashleigh Bagnall, ‘An Empirical Analysis of Suppression Orders in the Victorian Courts: 2008-12’ (2013) 35(4) *Sydney Law Review* 671, 674.

¹⁶ *John Fairfax & Sons v Police Tribunal of New South Wales* (1986) 5 NSWLR 465, 476-7.

as there is a clear public interest in protecting the identities of such persons.

There is a significant body of legislation that provides for the closing of courts and making of what may broadly be described as ‘suppression orders’, which prohibit the publication or reporting of proceedings, or of evidence produced in proceedings.¹⁷ In 2014, it was observed that there were more than 200 pieces of legislation in Australia providing for the making of suppression orders.¹⁸

To date, there has been no national review carried out of suppression orders. The Law Council of Australia has called for such a review, with then President Arthur Moses noting that media reporting is central to open justice, which must always be part of the balancing equation.¹⁹

A Victorian study carried out in 2013 found that in the five years between 2008 and 2012, 1,500 non-publication orders were made in Victorian courts, an apparent increase on previous years. The study found that 36% of orders made imposed blanket bans on publication of *any aspect* of the proceedings even though the legislation requires that the orders should be no more than is necessary to achieve its aim. Further, almost 70% of orders did not contain any temporal limitation.²⁰ A 2018 inquiry found that the introduction of the *Open Courts Act 2013* in Victoria had not brought about a significant decrease in the number of orders made, and that in 12% of suppression orders made there was no ground specified.²¹ These state-specific surveys indicate the need for vigilance to ensure that closed court and suppression orders are made appropriately and within applicable legislative limits.

The NSI Act was introduced as the *National Security Information (Criminal Proceedings) Act 2004* (Cth) in the wake of the events of 11 September 2001 and includes provisions enabling proceedings to be conducted in closed court, and for the making of suppression orders, that are in addition, and without prejudice, to the other powers that the court has to exclude members of the public from hearings or to prevent publication of evidence.²²

A further catalyst for the enactment of the NSI Act, in addition to the events of September 11, was the ACT Supreme Court’s decision in

¹⁷ For example, *Federal Court of Australia Act* (Cth) s 37AG, *Criminal Code Act 1995* (Cth) s 93.2, *Open Courts Act 2012* (Cth), *Open Courts Act 2010* (NSW), *Open Courts Act 2013* (Vic).

¹⁸ Larina Mullins, ‘Open Justice versus Suppression Orders: A Battle of Attrition’ (2014) 33(3) *Communications Law Bulletin* 7.

¹⁹ Reported in Kirrily Schwarz, ‘The Storm Around Suppression Orders’, *Law Society Journal Online* (Online, 30 April 2019) <<https://lsj.com.au/articles/the-storm-around-suppression-orders/>>.

²⁰ Bosland and Bagnall (n 15) 686.

²¹ Frank Vincent, *Open Courts Act Review* (Final Report, September 2017) 1 [8].

²² Originally enacted as the *National Security Information (Criminal Proceedings) Act 2004*. See *National Security Information (Civil and Criminal Proceedings) Act* notes to s 29 and s 381. Sections 20B and 38AB expressly require the court to consider making an order pursuant to s 93.2 of the Criminal Code.

R v Lappas.²³ Lappas was a public servant who was charged with offences relating to the disclosure of secret documents and sought to tender in the criminal proceedings against him two of the documents that he was alleged to have leaked. The government claimed public interest immunity in relation to the documents. Justice Gray upheld the public interest immunity claim. However, his Honour also stayed the prosecution against Lappas in respect of one of the offences arising from the disclosure, on the basis that a fair trial would not be possible without him having the ability to tender the documents.²⁴

The Commonwealth Attorney-General, in his second reading speech for the NSI Act, referred indirectly to the Lappas trial, saying, '[The Bill] will provide a court which has found that sensitive security related information should not be disclosed with an alternative to simply dismissing the charge'.²⁵

In 2004, the ALRC considered the effectiveness of public interest immunity and s 130 of the Uniform Evidence Acts (which provides for objections to evidence on the ground of public interest immunity) for the purposes of protecting sensitive state information. The ALRC found that public interest immunity procedures worked effectively for most types of information. However, in its *Keeping Secrets* report, it recommended the enactment of specific procedures within a 'National Security Information Procedures Act' to govern the use of all classified and security sensitive information in Australian courts and tribunals. These special procedures would only operate in exceptional cases outside the general law and procedures governing admission and use of evidence.²⁶

The Bill that became the NSI Act was introduced four days prior to the publication of the ALRC's *Keeping Secrets* report. The ALRC was not consulted during the Bill's development.²⁷

The powers contained in the Act include powers to conduct closed court hearings, but also extend to the use to be made of national security information in the proceeding. The Act provides for the restriction of access to information deemed to be relevant to national security. 'National security' is defined in s 8 as meaning 'Australia's defence, security, international relations or law enforcement interests'.

Under the NSI Act, if a person considers that proceedings will disclose national security information, s 24 of the Act requires the person to notify the Attorney-General. In a criminal proceeding, this applies to the accused as well as to the prosecutor. The Attorney-

²³ *R v Simon Lappas and Sherryll Ellen Dowling* [2001] ACTSC 115.

²⁴ Human Rights Law Centre, *Opaque Justice* (April 2021) [3.12] ('*Opaque Justice*').

²⁵ Commonwealth, *Parliamentary Debates*, House of Representatives, (27 May 2004) 29129.

²⁶ Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report No 98, May 2004) [13].

²⁷ *Opaque Justice* (n 24).

General then determines whether disclosure of the information is likely to prejudice national security.²⁸

The Attorney-General may issue a certificate certifying that disclosure of the information is likely to prejudice national security. If the information is contained within a document, the certificate may provide the document with the information deleted (with or without a summary of the information) and a certificate stating that the potential discloser must not, except in permitted circumstances, disclose the information. A certificate issued by the Attorney-General in a criminal proceeding is conclusive evidence that disclosure of the information in the proceeding is likely to prejudice national security.²⁹

The notification requirement also applies if the prosecutor or the defendant knows or believes that a person they intend to call as a witness will disclose national security information in giving evidence. The Attorney-General may issue a certificate stating that the prosecutor or defence must not call a particular person as a witness in a criminal proceeding if notification is given or if the Attorney-General expects that the witness, by their mere presence, will disclose information that is likely to prejudice national security. The judge is required to make a determination in closed court as to whether the witness may be called.³⁰

In relation to the first category of certificate, the judge must make a determination as to whether the information referred to in the certificate should be disclosed. A hearing of this nature is conducted in the absence of the public.³¹ If the court considers that the information would be disclosed to the defendant and any legal representative of the defendant who has not been given a security clearance to the relevant level, and that the disclosure would be likely to prejudice national security, the court may order that the defendant or their representative is to be excluded from the hearing.³² A record of the proceeding is not to be accessed by anyone other than those specified in the provision.³³

The Act also applies specifically to a proceeding under Division 104 of the *Criminal Code Act 1995* (Cth) ('Criminal Code') relating to a request to make, confirm or vary a control order in relation to a 'relevant person'. In those circumstances, if the Attorney-General has provided a certificate, the relevant person and their legal representative may be excluded from the proceeding in which the national security information is disclosed to the court, and the court may consider that

²⁸ *National Security Information (Civil and Criminal Proceedings) Act 2004* (Cth)s 26(2) (criminal) and for civil proceedings see s 38D (for the notification) and s 38F (for the decision) ('*NSI Act*').

²⁹ *NSI Act* ss 26, 27(1) (criminal) and in civil proceedings see s 38F.

³⁰ *NSI Act* s 28 (criminal) and in civil proceedings see s 38H. In civil proceedings the court holds a hearing and makes a determination under s 38H(6), s 38J and s 38L.

³¹ *NSI Act* s 27(5), s 28(7) and s 31 (criminal) and for civil proceedings see s 38H(7), s 38J (control order proceedings) and 38L.

³² *Ibid* s 29(3) (criminal) and for civil proceedings see s 38I(3).

³³ *Ibid* s 29(5)(e) (criminal) and for civil proceedings see s 38I(5)(d).

information in the proceeding although it has not been disclosed. The court must be satisfied that the relevant person has been given sufficient information about the allegations on which the control order request was based to enable them to give effective instructions.³⁴

There are also powers in the Act to make such orders as the court considers appropriate in relation to the disclosure of national security information if the court is satisfied that it is in the interests of national security.³⁵ The Court must determine whether any non-disclosure order would have a 'substantial adverse effect' on the defendant's right to receive a fair hearing including in particular on the conduct of her or his defence.³⁶

The accused and their legal representative must be given an opportunity to make submissions in relation to disclosure of information or the calling of witnesses.³⁷ While it is implicit in the right to make submissions that the accused must know the substance of the argument in relation to non-disclosure, the provisions of the NSI Act mean that an accused person must make a submission about non-disclosure without knowing what the non-disclosed information is, or what impact it might have upon the case.³⁸

In making a determination, the court is required to give the greatest weight to the consideration of whether permitting disclosure or calling the witness would compromise national security.³⁹ The judge may uphold the claim for non-disclosure or may order disclosure of information, including in a redacted form or a summary.⁴⁰ Pursuant to s 22, the Attorney-General, prosecutor and defendant may agree to an arrangement about disclosure, protection, storage, handling or destruction of national security information. Section 38B provides for agreement in a civil proceeding.

Courts have emphasised the significant and 'proper respect' that ought to be placed on the views of the Executive about what national security interests require.⁴¹ However, this deference to the views of government in terms of what harm may flow from disclosure⁴² is an important reason for maintaining other safeguards in terms of openness and transparency of public interest immunity proceedings. If the mere existence of proceedings is not made public, then the fact of the making

³⁴ Ibid s 38J.

³⁵ Ibid s 19(1A) (criminal) and for civil proceedings see s 19(3A).

³⁶ Ibid s 31(7).

³⁷ Ibid s 29(4) (criminal) and for civil proceedings see s 38I(4).

³⁸ Luke Beck, 'Fair Enough? The National Security Information (Criminal and Civil Proceedings) Act 2004' (2011) 16(2) *Deakin Law Review* 405, 415.

³⁹ *NSI Act* s 31(8) (criminal) and for civil proceedings see s 38L(8).

⁴⁰ *NSI Act* s 31 (criminal) and for civil proceedings see s 38L.

⁴¹ *R v Scerba* [2015] ACTSC 176 [18] (Refshauge J).

⁴² Willem de Lint and Wondwossen Kassa, 'Bent into Security: Barrister Contribution to a Skewed Order in Two Terrorism Prosecutions in Australia' (2017) 44(2) *Journal of Law and Society* 169, 191-3.

of such claims by the state is completely devoid of any scrutiny outside of that exercised by the judge.

In 2020, former head of the Australian Security and Intelligence Organisation ('ASIO'), Dennis Richardson, carried out a review of the legal framework of national intelligence. The report noted a tendency to over-classification of material.⁴³ Richardson's report found that there was no need for major reform of the NSI mechanisms, but noted that some agencies lacked appreciation of the careful balance required between the right to a fair trial, the principle of open justice and the protection of national security information.⁴⁴

Richardson has noted that public interest immunity and protective orders (outside of the NSI Act) are relied upon in the majority of counter-terrorism prosecutions.⁴⁵ Since 2005, the NSI Act has been invoked in 36 individual prosecutions, including 11 of 140 counter-terrorism prosecutions in that time.⁴⁶ It is apparent, therefore, that the legislation is being applied in cases outside of the terrorism context in which it was enacted.

The first case in which the NSI Act was relied upon was *R v Lodhi*, a terrorism prosecution, where a constitutional challenge to the legislation was dismissed in 2006 on the basis that the Act was not incompatible with the exercise of judicial power as the judge retained the power to order disclosure of the material.⁴⁷

In that case, it was also argued that s 31 of the NSI Act impermissibly burdened the implied freedom of political communication, on the basis that the hearing to determine whether an order should be made relating to disclosure of information is held in closed court. The argument was put on the basis that s 31 limited those who could be present at a hearing where matters falling within the definition of 'national security', including the activities of the executive and international relations, would be discussed.

Justice Whealy found that that the burden of closed court proceedings would mainly fall upon legal argument, although there may be some political communications burdened by the legislation. However, the object of the Act, to protect national security and thus the system of representative and responsible government, was plainly compatible with the maintenance of that same system. The method to

⁴³ Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (2018) para 3.159 referred to in Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (December 2019) vol 1 [45.97] ('*National Intelligence Community*').

⁴⁴ *National Intelligence Community* (n 43) [3.133].

⁴⁵ *National Intelligence Community* (n 43) [45.34].

⁴⁶ *National Intelligence Community* (n 43).

⁴⁷ *R v Lodhi* [2006] 163 A Crim R 448 ('*Lodhi*').

be adopted under s 31 was not that different from the hearing of a public interest immunity claim.⁴⁸

B. *Restriction of Access to Information in Civil Proceedings*

In 2005, the NSI Act was amended to extend its operation to civil proceedings. Part 3A of the NSI Act provides for disclosure of information that is likely to prejudice national security in civil proceedings. The provisions are substantially similar to those applicable to criminal proceedings (outlined above).

The provisions were invoked by the Attorney-General for the first time in defamation proceedings brought by former SAS operative Ben Roberts-Smith against Fairfax newspapers, which relate to a series of articles alleging Robert-Smith's involvement in war crimes. In a statement in relation to those proceedings, the Law Council of Australia argued for a requirement for reasons justifying a decision to hear matters in closed court, and for the appointment of special advocates to make submissions prior to any party being called to leave a courtroom.⁴⁹

The High Court has previously accepted the use of confidential criminal intelligence information in civil proceedings. In the *Gypsy Jokers* case,⁵⁰ the appellant was issued with a 'fortification warning notice', being a notice relating to structures designed to prevent uninvited entry to premises. The appellant sought review of the decision and also challenged the Constitutional validity of s 76(2) of the *Corruption and Crime Commission Act 2003* (WA), which provided for the confidentiality of information provided to the court (including keeping material from a party) on the review if disclosure might prejudice the operations of the Commissioner. The High Court found that the information was subject to limits upon use and disclosure only where the court determined that the disclosure might prejudice the operations of the Commissioner. Therefore, the independent performance by the Supreme Court of its review function was not constrained. Only Crennan J considered the issue of the interference with procedural fairness, finding that Parliament can legislate to exclude or modify the rules of procedural fairness, and the ability to withhold information from the respondent here was no different from the modification of procedural fairness arising from principles of public interest immunity.⁵¹

⁴⁸ Ibid [117], [123].

⁴⁹ Christopher Knaus, 'Law Council Wants Changes to Secrecy Laws Invoked in Ben Roberts-Smith Defamation Case', *The Guardian* (online, 8 May 2020) <<https://www.theguardian.com/australia-news/2020/may/08/law-council-wants-changes-to-secrecy-laws-invoked-in-ben-roberts-smith-defamation-case>>.

⁵⁰ *Gypsy Jokers Motorcycle Club Incorporated v Commissioner of Police* (2008) 234 CLR 532.

⁵¹ Ibid [182], [183].

In *Chief Commissioner of Police v Nikolic*,⁵² the Victorian Court of Appeal upheld an appeal against a decision of Ginnane J finding that Nikolic should have been provided with certain information upon which a decision had been made under s 33(1) of the *Racing Act 1958* (Vic) ('Racing Act') to prohibit him from entering specified racecourses during race meetings. The Court held that in certain circumstances, the importance of protecting highly sensitive information may have the consequence that procedural fairness does not require disclosure of even the substance or gist of the information in question. The statutory context of the Racing Act and the legislated methods that allowed procedural fairness to be reduced to nothing, were key to the findings.⁵³

As with criminal proceedings, in civil proceedings the court retains the ability to stay proceedings where a fair hearing cannot be guaranteed. However, as the Law Council has pointed out, in the context of civil proceedings, this mechanism has the potential to halt proceedings *against* the government, enabling it to evade a civil liability that it might otherwise bear.⁵⁴ In other words, the proceedings that are likely to be stayed as a result of such a ruling are those brought by a plaintiff against the state.

C. *Criticism of the NSI Act*

The NSI Act has been the subject of considerable criticism. In evidence given before the Senate Legal and Constitutional Legislation Committee in relation to the NSI 2004 Bills, the Law Council of Australia noted that the Bills could result in:

Decisions which are critical to the nature of the prosecution case, including possibly exculpatory elements, being determined in the absence of the accused or his or her representative by a judge who is processing in secret and ... without the accused even knowing of the occasion.⁵⁵

More recently, the Law Council of Australia has criticised the legislation as unduly fettering the court's discretion to maintain, modify or remove restrictions on disclosure of information to a party.⁵⁶ The Law Council was also of the view that the system of non-disclosure is unjustified having regard to pre-existing mechanisms to protect national security information.⁵⁷ The Law Council further commented on

⁵² *Chief Commissioner of Police v Nikolic* (2016) 338 ALR 683.

⁵³ Note that in the context of a Commonwealth court, some things allowed to state courts may not be permissible: *Assistant Commissioner Michael James Condon v Pompano Pty Ltd* (2013) 252 CLR 38 [126].

⁵⁴ Law Council of Australia, Submission to the Independent National Security Legislation Monitor, *Inquiry into The Operation of the National Security Information (Criminal and Civil Proceedings) Act* (July 2013) [79].

⁵⁵ *Ibid* [70].

⁵⁶ *Ibid* 3.

⁵⁷ *Ibid* 4.

offences within the Act, including penalisation of ‘disclosure that may affect national security’.⁵⁸

Justice Whealy, who presided over a number of early cases involving application of the NSI Act, has observed that the Act has the capacity to create a situation where the defendant’s right to a fair trial may be significantly impaired.⁵⁹

While enacted in response to terrorist attacks, a lack of ongoing vigilance and attention to the exceptional nature of the laws can contribute to their adaptation to new contexts.⁶⁰ This has, it seems, led to a failure to follow the ALRC’s recommendation that these types of laws are for exceptional cases only.

The Act specifically provides that a non-disclosure order does not prevent a court from staying a matter if non-disclosure would have a substantial adverse effect on the right to receive a fair hearing.⁶¹ However, despite this important protection, it is inherently problematic for such a determination to be made in the absence of the accused. Only the accused can know the defences that they will raise to the charges against them, and the basis upon which they will be raised. A judge making such a determination in the absence of an informed submission from the accused with access to the material in dispute can only speculate as to whether a particular document or piece of information might be relevant to a defence to be raised by the accused. Even where an accused is able to participate in the proceeding, to make an argument in relation to disclosure may effectively require an accused to outline the basis for their defence, in advance of the trial.

Flinders University academics Willem De Lint and Wondwossen Kassa, who examined the integration by Australian lawyers of national security interests into public law, note:⁶²

To operate with efficiency, the regime depends upon a fairly generous attribution of good faith by judges to police and security actors on their claim that the information that is secured from public scrutiny has been properly deemed and interpreted as privileged by those agents.

One barrister who had appeared in terrorism trials and was interviewed by De Lint and Kassa noted that national security was used to shield documents from the defence, while another noted that judges reviewing secret affidavits not shown to defence barristers will not know all the possible arguments that could have been raised had the material been accessible by those counsel. Another noted that in one matter, secret

⁵⁸ Ibid [79].

⁵⁹ AnthonyG Whealy, ‘Difficulty in Obtaining a Fair Trial in Terrorism Cases’ (2007) 81(9) *Australian Law Journal* 743, 748.

⁶⁰ George Williams, ‘A Decade of Australian Anti-Terror Laws’ (2011) 35(3) *Melbourne University Law Review* 1136, 1169.

⁶¹ *NSI Acts* s 19(2) and for civil proceedings it is s 19(4).

⁶² De Lint and Kassa (n 42) 187-8.

affidavits were provided in relation to ongoing threats of terrorism, and a full roster of targets from a network being intercepted, from which the prosecution developed information against the accused, was found to be privileged on the basis of that ongoing threat.⁶³

In 2013, the Independent National Security Legislation Monitor found that there was no indication as at that date that the NSI Act had detracted from fair trial values in terrorism criminal proceedings to date, however the paucity of occasions when the Act had been argued in a fully contested fashion, made that conclusion provisional only.⁶⁴ No substantive review of the operation of the NSI Act has yet been carried out.

In his 2020 review, Richardson noted that the United States has a greater willingness to make public disclosures about sensitive information and capabilities to achieve a successful prosecution in relation to its equivalent legislation, and suggested that Australian intelligence agencies should be prepared to move in the same direction.⁶⁵

The United Kingdom has similar provisions to the NSI Act in the form of ‘closed material procedures’, which allow for one party to present evidence that the other party is not entitled to see. Closed material procedures were initially restricted to national security related tribunals, however their use has expanded to other areas.⁶⁶ Special advocates review the confidential information and act on the accused’s behalf in the proceeding, although they do not take instructions from the accused.

The United Kingdom Supreme Court found unconstitutional measures allowing the government to rely on confidential material in civil proceedings that was only disclosed to a special advocate.⁶⁷ However, the United Kingdom Parliament subsequently introduced the Justice and Security Bill to allow secret evidence to be used in a civil proceeding in these circumstances.⁶⁸

Fifty special advocates submitted a memorandum to the Joint Committee on Human Rights in relation to the Bill, noting (inter alia) that the Bill required the judge to accede to the government’s

⁶³ Ibid 188-9.

⁶⁴ Australian Government, *Independent National Security Legislation Monitor* (Annual Report, 7 November 2013) 124.

⁶⁵ *National Intelligence Community* (n 43) [3.135], [45.63], [45.163].

⁶⁶ Fred Allen, ‘Judicial Review and The Creep of Closed Material Procedures - R (on the application of Haralambous) v Crown Court at St Albans and Another’, *Kingsley Napley When It Matters Most* (Blog Post, 1 February 2018) <<https://www.kingsleynapley.co.uk/insights/blogs/public-law-blog/judicial-review-and-the-creep-of-closed-material-procedures-r-on-the-application-of-haralambous-v-crown-court-at-st-albans-and-another>>.

⁶⁷ *Al Rawi v The Security Service* [2011] 3 WLR 388.

⁶⁸ Miiko Kumar, ‘Protecting State Secrets: Jurisdictional Differences and Current Developments’ (2013) 82(4) *Mississippi Law Journal* 853.

application for a closed material procedure if there was any material disclosure that would damage national security, notwithstanding that the judge considered the case could be tried fairly under existing public interest immunity rules.⁶⁹ The advocates also noted that the category of ‘international relations’ had, in their collective experience, been relied upon to invoke closed material procedures ‘where the harm caused by disclosure is in reality little more than diplomatic embarrassment’.⁷⁰

One advocate has described the way in which the United Kingdom Act operates unfairly, so that as a special advocate, he is required to test evidence that he is unable to ask his client about. As he says, ‘If the state alleges that my client met a terrorist at a particular time, I cannot ask him whether he was there and if so, why. So I will never know if he had an alibi or an innocent explanation for the meeting, and nor will the court.’⁷¹

In 2006, the use of special counsel in a criminal trial was considered in the Australian context, and found not to be prohibited by the NSI Act, although such an appointment was referred to as ‘exceptional’ and only where the interests of justice are shown to require it.⁷² Procedures for the appointment of special advocates were adopted in Australia in 2017, but only in relation to control order proceedings, and subsequently extended in 2021 to supervision and continuing detention orders.⁷³ Most recently in *R v Collaery (No 11)*, Mossop J held that the Court has power to appoint special counsel in a criminal proceeding pursuant to either s 19(1A) of the NSI Act, or alternatively the inherent power of the Court.⁷⁴

To the writer’s knowledge, the Collaery trial is the only instance of appointment of a special advocate in a criminal trial in Australia. Based on the United Kingdom experience, it appears that the use of special advocates would, in any case, be limited in its ability to redress the unfairness that may arise from withholding access to information from one party to proceedings.

The NSI Act has recently been applied in two high profile cases, including the Collaery case, which have been the subject of extensive media commentary.

⁶⁹ Martin Chamberlain et al, Special Advocates’ Memorandum on the Justice and Security Bill Submitted to the Joint Committee on Human Rights (June 2012).

⁷⁰ Ibid [5].

⁷¹ Martin Chamberlain, ‘A Barrister Who’s Worked in Secret Courts Since 2003 Describes a Twisted System of Justice Worthy of Kafka’, *Daily Mail UK* (online, 14 March 2012) <<https://www.dailymail.co.uk/debate/article-2114162/Closed-material-procedure-Barrister-describes-twisted-justice-worthy-Franz-Kafka.html>>.

⁷² *Lodhi* (n 47) [13]–[16]; *R v Khazaal* [2006] NSWSC 1061 [51]. This decision predated the introduction of ss 38PA to 38PI of the NSI Act in relation to civil proceedings.

⁷³ NSI Act s 38PA to 38PI; *National Security Information (Criminal and Civil Proceedings) Amendment Regulations 2017* (Cth).

⁷⁴ *R v Collaery (No 11)* [2022] ACTSC 40 [26].

D. *Bernard Collaery and Witness K Prosecutions*

In 2018, Bernard Collaery, a barrister and former Attorney-General of the Australian Capital Territory, was charged with four counts pursuant to s 39 of the *Intelligence Services Act* and one count of conspiracy to breach s 39. The conspiracy alleged is one to communicate information to the Timor-Leste government that was prepared by or on behalf of the Australian Secret Intelligence Service ('ASIS') in connection with its functions. The breaches of s 39 relate to the communication of that information to ABC journalists. Collaery's alleged co-conspirator, Witness K, pleaded guilty and was convicted and sentenced to a three-month suspended sentence in June 2021.⁷⁵

The information allegedly disclosed by Collaery relates to the bugging of the Timor-Leste Cabinet rooms in 2004 by Australian security services, enabling the Australian government to secretly obtain information that was then used to Australia's commercial advantage in negotiations with East Timor over oil and gas reserves in the Timor Sea.

As part of the case against Collaery, the prosecution is required to prove that part of the information disclosed by him was true. The Attorney-General seeks to keep that part of the information confidential on the basis that it would create a risk of prejudice to national security if it were disclosed.

In seeking to suppress the publication of information in Collaery's trial, the government seeks to publicly maintain a 'neither confirm nor deny' position in relation to the bugging of the East Timorese cabinet rooms,⁷⁶ while secretly adducing evidence of the truth of those events, in order to successfully prosecute Mr Collaery.

In *R v Collaery (No 7)*,⁷⁷ Mossop J considered an application by the Attorney-General for orders pursuant to s 31 of the NSI Act that significant parts of the trial not be conducted in public and jurors could not disclose information given during closed portions of the hearing. Justice Mossop said that for s 31(7), the issue is whether, having regard to the Attorney-General's certificate, there would be a risk of prejudice to national security if the information were disclosed. His Honour found that the risk of prejudice from disclosure arose in a number of ways, including reputational harm amongst intelligence partners from the inability of the government to prosecute alleged significant breaches of the law by intelligence officers, a significant advantage to foreign intelligence services that would be of benefit to other countries, that information could be used for purposes of mosaic analysis by foreign

⁷⁵ Elizabeth Byrne, 'Court Documents Shed New Light on Man Behind Moniker "Witness K" and How He Met Lawyer Bernard Collaery', *ABC News* (online, 4 July 2021) <<https://www.abc.net.au/news/2021-07-04/court-document-witness-k-bernard-collaery-cleared-public-release/100263168>>.

⁷⁶ *R v Collaery (No 7)* [2020] ACTSC 165 [10].

⁷⁷ *Ibid.*

intelligence services, and prejudice to the capacity of intelligence services because disclosure would provide an incentive to disclose in a very public manner in order to undermine the government's claim to be entitled to protect the information.⁷⁸

Justice Mossop found that where what is being prosecuted is an alleged unlawful disclosure of sensitive information, it would be contrary to the proper administration of justice to compel the prosecution to disclose it to the world. Because there was no restriction on the accused's access to information or its use in his trial, there was not a substantial adverse effect on his right to a fair hearing.⁷⁹

On appeal from Mossop J's decision, the ACT Court of Appeal accepted that public disclosure of information relating to the truth of the matters of which Collaery sought disclosure would involve a risk of prejudice to national security. However, the Court of Appeal expressed doubt that this was a significant risk, and it had to be balanced against the very real risk of damage to public confidence in the administration of justice if the evidence could not be publicly disclosed. The Court particularly referred to the importance of criminal trials being heard in public in order to deter political prosecutions, allow public scrutiny of the actions of prosecutors and allow the public to assess the conduct of the accused. On remittal, Mossop J determined that the Attorney-General can rely upon 'court only evidence' that will not be shown to the accused or his lawyers in relation to the question of whether parts of the trial should be conducted in public, and a special counsel will be appointed to make submissions in relation to the use of that material. The material in question is not evidence to be tendered in the substantive trial against Collaery. In a further recent decision, Mossop J set aside subpoenas issued by Collaery to various intelligence agencies, finding that, as the prosecution is not required to prove that the subject matter of the disclosure involved only activities 'within' the functions of ASIS, the subpoenas lacked a legitimate forensic purpose.⁸⁰

The Collaery prosecution is an important touchstone for the operation of a range of provisions, including those pertaining to closed courts, suppression orders, public interest immunity and secrecy of

⁷⁸ Ibid [106]-[109].

⁷⁹ Ibid [128], [148].

⁸⁰ *Collaery v The Queen (No 2)* [2021] ACTCA 28. Information in relation to the appeal is taken from a summary of the judgment available on the ACT Supreme Court website. The judgment itself is not publicly available pending the Attorney-General's application for special leave to the High Court to appeal the Court of Appeal's decision not to suppress its reasons for decision: Christopher Knaus, 'Open Justice v Secrecy: What is the Case Against Witness K Lawyer Bernard Collaery All About?' *The Guardian* (online, 31 January 2022), <<https://www.theguardian.com/australia-news/2022/jan/31/open-justice-v-secrecy-what-is-the-case-against-witness-k-lawyer-bernard-collaery-all-about>>. The decision on remittal is *R v Collaery (No 11)* [2022] ACTSC 40. The subpoena decision is *R v Collaery (No 12)* [2022] ACTSC 108.

national security information. As at the time of writing, it remains undetermined how much of the trial will be conducted in public.

A number of individuals and bodies, including the ACT Bar Association, the Human Rights Law Centre, and prominent members of the legal profession, have called for an end to the prosecution against Collaery, on the grounds that the prosecution of a whistleblower who has brought to public attention the government's unlawful conduct is contrary to the public interest.⁸¹

E. *Witness J Prosecution*

In 2019, a person known only as Witness J was convicted of mishandling classified information that had the potential to expose the identity of agents for Australian intelligence agencies. The details of the offences he was sentenced for have only recently been revealed in the context of a review by the Independent National Security Legislation Monitor into the matter.⁸²

Witness J is a former military intelligence officer who was undergoing a security clearance process while living overseas. Frustrated by challenges to answers he gave as part of that process, he emailed the head of security and a departmental psychologist in Australia by insecure electronic means in which he communicated classified information.

The proceeding was remarkable for being conducted entirely in secret. The orders in relation to suppression of information were made by agreement between the prosecution and the defendant, pursuant to s 22 of the Act.

The matter came to public attention when two journalists encountered a sign in the court precincts reading, "Before Justice Burns, in Court Room SC4, at 10am. Sentence: Matter Suppressed". The journalists made an enquiry with the court, which revealed that orders had been made under the NSI Act closing the court to the public during the taking of evidence and submissions.⁸³ The matter was also brought

⁸¹ Naomi Neilson, 'Changeover Of A-G Opportunity To Stop Collaery and Witness K Prosecutions', *Lawyers Weekly* (online, 12 April 2021) <<https://www.lawyersweekly.com.au/biglaw/31110-changeover-of-a-g-s-opportunity-to-stop-collaery-and-witness-k-prosecutions>>; Jerome Doraisamy, 'There Is No Public Interest In Prosecuting Bernard Collaery and Witness K', *Lawyers Weekly* (online, 17 May 2021) <<https://www.lawyersweekly.com.au/politics/31384-there-is-no-public-interest-in-prosecuting-bernard-collaery-and-witness-k>>.

⁸² Independent National Security Legislation Monitor, *New Review: The Operation of Section 22 of The National Security Information (Criminal and Civil Proceedings) ACT 2004 (Cth) As it Applies in the 'Alan Johns' Matter (A Pseudonym)* (online, March 2020) <<https://www.inslm.gov.au/sites/default/files/2020-03/New%20Inquiry%20Johns%20Matter.pdf>>.

⁸³ Andrew Probyn, 'The Quiet Person You Pass on The Street': Secret Prisoner Witness J Revealed', *ABC Online* (online, 5 December 2019) <<https://www.abc.net.au/news/2019-12-05/witness-j-revealed-secret-trial/11764676>>.

to light when Witness J subsequently challenged the prison's actions in raiding his cell and his brother's home and temporarily freezing his communications when it was discovered that he had written a memoir.⁸⁴

Former NSW Justice Anthony Whealy has stated that Witness J's trial appeared to be a 'complete abandonment of open justice', and has queried whether Australia is now a 'totalitarian state where people are prosecuted, convicted and shunted off to prison without they or the public having any notion as to what has happened'.⁸⁵

The former Independent National Security Legislation Monitor, James Renwick, initiated an inquiry into Witness J's case in March 2020, observing:

As far as we know there has never been another case, at least in peace time in Australia, where all that has been conducted in secret. That is something significant and different, and for my part, I would not like to see it repeated.⁸⁶

The Monitor's own motion review indicates that the Monitor will consider whether the NSI Act should require, or require the court to consider, whether a contradictor (e.g., a special advocate) should be heard on the question of suppression orders, whether some details of the charges and orders should always be publicly known, and whether reasons should always be given by the presiding judge for the decision to depart from the open justice principle.⁸⁷

In a submission to the Monitor's review, the Human Rights Law Centre submitted that the combination of closed court and suppression of the defendant's name can never be justifiable in view of the compelling public interest in open justice. It noted that the interests of the prosecution and the defendant in secrecy are often aligned, to the extent that agreements pursuant to s 22 of the NSI Act are commonplace.⁸⁸ This means that, by agreement, information can be kept secret, but also proceedings not published so that the public may be unaware even of their existence.

The Human Rights Law Centre recommended that the NSI Act be reformed to ensure minimum standards of openness in any s 22 order (the order that allows agreement between parties regarding disclosure

⁸⁴ Christopher Knaus, 'Are We Now A Totalitarian State?': Case of Canberra's Mystery Prisoner Alarms Judge', *The Guardian* (online, 21 November 2019) <<https://www.theguardian.com/law/2019/nov/21/are-we-now-a-totalitarian-state-case-of-canberras-mystery-prisoner-alarms-judge>>. See also *Johns v Director-General of The ACT Justice and Community Safety Directorate* [2011] ACTSC 311.

⁸⁵ Knaus (n 84).

⁸⁶ Senior Counsel James Renwick, 'What Are the Right Encryption Laws for Australia?' (Speech, Lowy institute, 5 March 2020) [1.71] <https://www.lowyinstitute.org/sites/default/files/Renwick%20-%20The%20Right%20Encryption%20Laws%20for%20Australia%20-%20205-3-2020_1.pdf>.

⁸⁷ Independent National Security Legislation Monitor, *New Review* (n 82).

⁸⁸ *Opaque Justice* (n 24) [3.3].

and protection of information), and that reasons for such orders should be published. It recommended the appointment of an Open Justice Advocate for proceedings where the NSI Act was invoked, and that the Attorney-General's Department include information on the use of the Act in its annual report, and for a 'secret judgments' library to be kept.⁸⁹

The current Monitor, Grant Donaldson, has indicated that a fuller review of the operation of the NSI Act would more appropriately await the conclusion of the Bernard Collaery and Witness K prosecutions and the Roberts-Smith litigation, to avoid interference with matters before the courts, and also to obtain the assistance post-event of persons involved in those matters.⁹⁰

However, Mr Donaldson noted at a hearing of the review in June 2021 that there was no reason why the orders that were made in the Witness J case could not have been published much earlier than they were.⁹¹ This is perhaps a preliminary indication that his report will indicate the need for more limitations to be exercised in relation to the suppression of information under the NSI Act.

F. Hear no Evil: Observations

The NSI Act has never been subject to a comprehensive review.⁹² The time is right for such a review, particularly in light of the recent secret trial of Witness J and the ongoing trial of Bernard Collaery. It is to be hoped that the recent observation of the Independent National Security Legislation Monitor that such a review should be conducted after the conclusion of current proceedings is followed through.

Such a review should examine the nature of the information suppressed in those trials and consider whether, objectively, it has been in the public interest to have the information restricted in the way that it has been. It is only in examining how the provisions of the Act operate in practice, including where that is by consent of the parties, that it is possible to discern whether the restrictions that have been put in place are an appropriate protection of national security that simultaneously respects the right of voters in a democratic society to know about wrongdoing by their government and its agencies.

It is also time that there be a national review of legislation allowing the closing of courts and suppression of reporting of court proceedings. Such a review should pay particular attention to closed court or suppression orders sought by the government, including the reasons for

⁸⁹ *Opaque Justice* (n 24) [2] Recommendations.

⁹⁰ Independent National Security Legislation Monitor, *Annual Report 2019-2020* (Annual Report, February 2021) 13-19.

⁹¹ Office of the Independent National Security Legislation Monitor, *Review into the Operation of Part 3, Division 1 of the National Security Information (Criminal and Civil Proceedings) Act 2004 (Cth)* (Transcript of Proceedings of Public Hearing, 9 June 2021).

⁹² *Opaque Justice* (n 24) [3.2].

seeking such orders, the outcome, and the particular limitations imposed.

III See no Evil – Freedom of Information

A. *Restrictions on Freedom of Information*

[The] overarching purpose of access to information legislation is to facilitate democracy ... rights to state held information are designed to improve the workings of government; to make it more effective, responsive and accountable.⁹³

Access to information in Australia is governed at a federal level by the FOI Act. Australia was the first Commonwealth country to enact a FOI Act, followed by New Zealand in 1982 and Canada in 1983.⁹⁴

The original FOI Act was criticised for having a large number of broadly-drafted exemptions, and also for its scheme of ‘conclusive certificates’ that a document is exempt from FOI, which effectively gave the Minister a right of veto in relation to the release of a document.⁹⁵

*McKinnon v Secretary, Department of Treasury*⁹⁶ concerned an application by the Freedom of Information (‘FOI’) Editor at *The Australian* newspaper for access to information held by Treasury relating to ‘bracket creep’ in the federal taxation system and material relating to the First Home Owners Scheme. Access was refused in reliance on former s 36 of the Act, which provided an exemption for a document if disclosure would reveal advice that has taken place in the course of the deliberative processes involved in the functions of an agency or Minister of the Government and would be contrary to the public interest.

Following *McKinnon*, the Government implemented a number of reforms to the FOI Act, including removal of the ‘conclusive certificate’ mechanism and establishment of the offices of the Australian Information Commissioner and the FOI Commissioner.⁹⁷

The *Freedom of Information Amendment (Reform) Act 2010* removed the regime of conclusive certificates and introduced a scheme of ‘conditionally exempt’ documents, which must be disclosed unless it would be contrary to the public interest.⁹⁸ ‘Conditionally exempt’ documents include (relevantly):

⁹³ *Dagg v Canada* (1997) 148 DLR (4th) 385, 403 (La Forest J).

⁹⁴ Moira Paterson and Maeve McDonagh, ‘Freedom of Information and The Public Interest: The Commonwealth Experience’ (2017) 17(2) *Oxford University Cth Law Journal* 189-210, 189.

⁹⁵ Gerard Craddock, ‘The Freedom of Information Act 1982 and Review on The Merits’ (1958) 8(2) *UNSW Law Journal* 313, 314.

⁹⁶ *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423.

⁹⁷ Moira Paterson, ‘The Freedom of Information Act Post-McKinnon v Treasury’ [2012] 108 *Precedent* 35.

⁹⁸ *Freedom of Information Act 1982* (Cth) s 11A.

1. documents that would, or could reasonably be expected to, cause damage to relations between the Commonwealth and a State, or divulge matters communicated in confidence between the same;
2. documents that would disclose matters in the nature of opinion, advice, or recommendation or deliberation involved in the functions of an agency, Minister or the Government;
3. documents disclosure of which would have a substantial adverse effect on the financial or property interests of the Commonwealth or an agency.

Section 11B sets out a number of factors favouring access to the document in the public interest, including whether access to the document would promote the objects of the Act, inform debate on a matter of public importance, and promote effective oversight of public expenditure. It also makes irrelevant factors including whether access could result in embarrassment to the Commonwealth government, or cause a loss of confidence in the government, or whether access to the document could result in any person misinterpreting or misunderstanding it.

The Act also contains an exemption in s 33 from FOI for material that would, or could ‘reasonably be expected to’ cause damage to the security, defence or international relations of the Commonwealth, or divulge any information or matter communicated in confidence by or on behalf of a foreign government to an authority of the Commonwealth.

Section 33 is one of a number of categories of ‘exempt documents’ pursuant to Division 2 of Part IV, which also includes s 38 (referred to below), cabinet documents (s 34) and documents affecting enforcement of law and protection of public safety (s 37).

To fall within the exemption in s 33, there must be a higher degree of certainty of damage to national security than a risk.⁹⁹ Neither mere embarrassment nor the risk of exposure to public criticism is sufficient to justify an exemption.¹⁰⁰ A simple assertion that damage to national security will ensue is not sufficient to justify withholding of information.

The question for the decision maker in determining whether the exemption in s 33(a)(i) applies is whether disclosure would, or could reasonably be expected to, cause damage to the security of the Commonwealth, such that while there is no scope to balance competing interests, there are matters of judgment that may involve difficult questions of fact and degree.¹⁰¹

⁹⁹ *McGrath and Director-General, National Archives of Australia*, [2020] AATA 1790, [140] (‘*McGrath and Director-General*’).

¹⁰⁰ *Ibid* [143] citing *Re Fernandes and National Archives of Australia* [2014] AATA 180 per Kerr J.

¹⁰¹ *Prinn and Dept of Defence* (2016) 152 ALD 162 [61]–[96].

The Act also contains a blanket exemption under the FOI Act for documents originating or received from the intelligence agencies (ASIS, ASIO, Australian Signals Directorate ('ASD'), Office of National Intelligence ('ONI'), Australian Geospatial Intelligence Organisation ('AGO') and Defence Intelligence Organisation ('DIO')).¹⁰²

Section 38 contains a 'secrecy exemption' which applies to situations where disclosure of the information is prohibited under a provision of an enactment that is specified in Schedule 3 or where s 38 is expressly applied by an enactment. Schedule 3 specifies a number of secrecy provisions from different Acts. This provision continues to exist notwithstanding recommendations by civil liberties and media groups in 2010 to repeal it.¹⁰³

The public interest is an irrelevant consideration in relation to the exemption in s 33 for information that would prejudice national security.¹⁰⁴ There is no 'public interest' test in relation to any of the categories of 'exempt documents' referred to above.

A challenge to a decision made not to disclose a document exempt pursuant to s 33 may entail the making of a confidentiality order, meaning that the applicant for review is not entitled to review the document that has been found exempt from disclosure.¹⁰⁵ In *Matson's case*, the Tribunal granted a confidentiality application sought by the Attorney-General's Department in relation to certain documents, finding that not to do so would obviate the purpose of the substantive application. The Tribunal stated: '(I)f a respondent claims that a document is exempt from disclosure, the document must remain undisclosed to the party seeking it unless and until the proceedings are finally resolved in the applicant's favour'. The applicant therefore has no way of judging for themselves whether there is merit to the national security exemption that has been raised.

Moir Paterson and Maeve McDonagh, who have carried out a review of public interest tests in Commonwealth law, argue that a 'harm test' is usually a key component of a good FOI law, as it prevents information being withheld from public view simply because it falls into a certain category of material.¹⁰⁶ There is no 'harm test' in relation to the s 7A exemption for security agencies, whereby documents are exempt if they originate or are received from one of those agencies, regardless of whether disclosure would have negative effects, nor is there a harm test in relation to a number of the other categories of exempt documents.

¹⁰² *Freedom of Information Act* (n 98) s 7(2A).

¹⁰³ Australian Law Reform Commission (n 5) [16.73].

¹⁰⁴ *Logo and Dept of Immigration and Citizenship* (2011) 124 ALD 238; *Aldred v Department of Foreign Affairs and Trade* [1990] AATA 833; *Prinn and Dept of Defence* (n 101).

¹⁰⁵ *Matson v Attorney-General's Dept* [2021] FCA 1027.

¹⁰⁶ Paterson and McDonagh (n 94) 194.

A public interest test is also key to ensuring that information can be disclosed where the public interest in disclosure outweighs the harm of disclosing.¹⁰⁷ As Paterson and McDonagh note, ‘the application of an exemption containing a harm test but no public interest test could result in refusal of access, even in circumstances where any harm that might be occasioned by release of the information is outweighed by countervailing interests in transparency’.¹⁰⁸ Section 33 is a good illustration of such a provision, which provides a ‘harm test’ in the form of damage to security, defence and international relations of the Commonwealth, but is not counterbalanced by any public interest test.

These limitations on the FOI Act indicate that there exists the capacity for documents to be exempt from disclosure without the need for any proof that their disclosure would cause harm, and also where there is no scope for consideration of whether disclosure would be in the public interest.

This is concerning when one considers that there have been a number of instances where information has been withheld by government agencies under FOI exemptions where, upon challenge, an order has been made that the information should be disclosed. These examples illustrate that decisions can be made by government agencies limiting access to documents that are subsequently found not to fall within the claimed exemptions, or where the public interest lies in disclosure. A ruling to that effect, however, requires persistence and willingness on the part of the applicant to institute an appeal.

For example, in *Dunn v Department of Defence*, estimated casualty figures for a Gulf operation known as ‘Operation Iraqi Freedom’ were withheld on the basis that they could reasonably be expected to cause damage to the security or defence of the Commonwealth. Upon appeal, it was held that the release of those figures could not reasonably be expected to cause damage to security or defence.¹⁰⁹

Re Besser; Secretary, Dept of Employment (Freedom of Information),¹¹⁰ concerned an application by a journalist for information from the Department of Employment relating to its administration of an employment services program and an investigation of various service providers. The request was denied on the basis that the documents were exempt pursuant to s 47G of the Act (information concerning the business or professional affairs of a person – a category of ‘conditionally exempt’ documents). The Information Commissioner set aside that decision and ordered production of the documents. On appeal to the AAT, it was held that there was public interest in the

¹⁰⁷ Ibid.

¹⁰⁸ Ibid.

¹⁰⁹ *Dunn v Dept of Defence* (2004) 84 ALD 419.

¹¹⁰ *Besser; Secretary, Dept of Employment (Freedom of Information)* (2017) AATA 835.

documents being provided, although the names of the relevant providers should be redacted.¹¹¹

In *Patrick v Secretary, Department of Prime Minister and Cabinet (Freedom of Information)*,¹¹² Senator Rex Patrick sought access to an audit report from the auditor general relating to the acquisition by the Department of Defence of a fleet of vehicles described as ‘protected mobility vehicles – light’. Exemptions were claimed pursuant to ss 33(a)(ii), 47C, 47D and 47G(1)(a). The secretary resisted disclosure on the basis that it would harm the prospects of exporting the vehicles, which would have a negative flow-on consequence for the sustainment of the capability of the vehicles for use by the Australian army. The tribunal found that the report had been drawn from publicly available information and was not satisfied the disclosure would cause damage to the export prospects for the vehicles.

The ‘French submarines’ series of FOI litigation is an interesting recent example of disputes between politicians seeking information in the public interest and the government attempting to protect the secrecy of the documents. In *Xenophon v Secretary, Department of Defence (Freedom of Information)*,¹¹³ the Administrative Appeals Tribunal upheld a decision of the Australian Information Commissioner affirming a decision by the Department of Defence to refuse access to certain documents relating to a competitive evaluation process for the selection of a partner to design and build the next generation of Australian submarines. The documents were found to be exempt from disclosure pursuant to s 33 of the FOI Act, on the basis that there was a mutual understanding of confidence in relation to the documents and release of the material could adversely impact upon the ability of the Australian government to maintain good working relationships with other governments. The tribunal found that the fact that damage caused to international relations may be capable of remediation does not disengage the international relations exemption in s 33(a)(iii).¹¹⁴

In August 2020, the Australian Information Commissioner ordered the Department of Defence to release to Senator Patrick details of the value of the contract to build the navy’s submarines.¹¹⁵ She rejected Defence’s argument that the documents were conditionally exempt under s 47C (deliberative processes) and s 47G (business affairs)

¹¹¹ For other cases involving departmental decisions to refuse disclosure that have been overturned on appeal see *McKinnon and Secretary, Dept of Families, Housing, Community Services and Indigenous Affairs* (2008) 103 ALD 348 and *McKinnon v Dept of Finance and Deregulation 2* [2011] AATA 604.

¹¹² *Patrick v Secretary, Department of Prime Minister and Cabinet (Freedom of Information)* [2020] AATA 4964.

¹¹³ *Xenophon v Secretary, Department of Defence (Freedom of Information)* [2019] AATA 3667.

¹¹⁴ *Ibid* [120].

¹¹⁵ Andrew Tillett, ‘Defence Ordered to Hand Over Submarine Contract Details’, *Financial Review* (online 27 August 2020) <<https://www.afr.com/politics/federal/defence-ordered-to-hand-over-submarine-contract-details-20200824-p550pw>>.

exemptions.¹¹⁶ The finding included a statement that ‘disclosure would further transparency and accountability with respect to the information provided by Naval Group to persuade the Commonwealth that it is best placed to deliver the Future Submarines Program’.¹¹⁷

In May 2021, it was revealed during Senate Estimates that the Department of Defence was covering the legal expenses of the French submarine manufacturer, in relation to the government’s appeal of the decision to the Administrative Appeals Tribunal, which subsequently succeeded.¹¹⁸ In September 2021, the Australian government announced the abandonment of the French contract, and the institution of a new plan to construct nuclear-powered submarines as part of a partnership with the United States and the United Kingdom.¹¹⁹

Senator Patrick also recently succeeded in a freedom of information application to gain access to documents of the ‘national cabinet’ which the government had sought to withhold under FOI exemptions relating to official records of a Cabinet committee, and damage to Commonwealth-State relations.¹²⁰ He is also involved in attempts to access information relating to the bugging of the Timor-Leste cabinet rooms (referred to above) and to publish the names of companies who received JobKeeper payments and the amounts they received, and how much (if any) has been paid back.¹²¹

In terms of FOI performance generally, lawyer Jennifer Robinson has noted that the OAIC, which oversees the FOI Act, is drastically underfunded, with reviews often taking more than a year. She observes that the federal government (in 2019) had been called out for

¹¹⁶ *Rex Patrick and Department of Defence (No 2)* (Freedom of Information) [2020] AICmr 40.

¹¹⁷ *Ibid* [75].

¹¹⁸ Andrew Greene, ‘Taxpayers Footing French Legal Bills to Keep Original Price of \$90 Billion Future Submarine Project Secret’, *ABC Online* (online, 10 May 2021) <<https://www.abc.net.au/news/2021-05-10/taxpayers-paying-french-submarine-naval-group-legal-fees/100127510>>. The appeal judgment is *Patrick; Secretary, Department of Defence and* [2021] AATA 4627. The appeal succeeded on the basis that disclosure would found an action for breach of confidence.

¹¹⁹ Julian Borger and Dan Sabbagh, ‘US, UK and Australia Forge Military Alliance to Counter China’, *The Guardian* (online, 16 September 2021) <<https://www.theguardian.com/australia-news/2021/sep/15/australia-nuclear-powered-submarines-us-uk-security-partnership-aukus>>.

¹²⁰ *Patrick and Secretary, Department of Prime Minister and Cabinet (Freedom of Information)* [2021] AATA 2719.

¹²¹ Nassim Khadeem, ‘JobKeeper Disclosure Rejected by Tax Office but Senate May Force it to Hand Over Names’, *The Guardian* (online, 13 August 2021) <[https://www.theguardian.com/australia-news/2021/aug/16/rex-patrick-launches-bid-to-make-government-reveal-long-secret-cabinet-documents-on-timor-leste](https://www.abc.net.au/news/2021-08-13/jobkeeper-ato-chris-jordan-rex-patrick-overpayments-centrelink/100370626#:~:text=Tax%20commissioner%20Chris%20Jordan%20has%20defied%20a%20Senate%20order%20that,list%20C%20citing%20public%20interest%20immunity&text=Companies%20that%20received%20JobKeeper%20but,to%20pay%20back%20the%20money>; Christopher Knaus, ‘Rex Patrick Launches Bid to Make Government Reveal Long-Secret Cabinet Documents on Timor-Leste’, <i>The Guardian</i> (online, 16 August 2021) <.

withholding more than 10,000 pages of documents from the public, which included records relating to the Adani coal mine.¹²²

In a 2017 review of FOI applications, Maureen Henninger found that there had been an increase in secrecy between 2000 and 2017, with a decline in the granting of policy-related information requests and subsequent rise in refusals over that period.¹²³

In 2019, an investigation by Guardian Australia found that FOI refusals were at their highest levels since the commencement of records in 2010-11, with more than 2,000 requests taking three months longer than the statutory timeframe. The rate of refusals for 2017-8 was 17%, with only 50% of requests granted in full. The investigation also reported on the understaffing of government FOI teams and of the Australian Information Commissioner.¹²⁴ Nevertheless, a recommendation by the Hawke Review in 2013 for a comprehensive review of the FOI Act¹²⁵ has never been implemented.

The *Archives Act 1983* (Cth) ('Archives Act') allows members of the public to access Commonwealth records that are 20 years or older. Intelligence agencies are included within the remit of the Archives Act. However, there are exemptions for disclosure of information that could cause damage to the defence, security or international relations of the Commonwealth (amongst other exceptions).¹²⁶

The Archives Act s 33(1)(a) largely mirrors s 33(1)(a) of the FOI Act, except that it refers to information that 'could reasonably be expected to' [prejudice national security], unlike the FOI Act, which refers to 'would, or could reasonably be expected to'. In *Re McGrath and Director-General, National Archives of Australia*¹²⁷ it was observed that the choice of different words was deliberate and reflects that the outcome of disclosure is more difficult to predict when documents relate to historical matters.¹²⁸

FOI and Archives Act provisions were considered as part of Richardson's review into the national intelligence community. Richardson followed the findings of the ALRC report *Open Government: A Review of the Federal Freedom of Information Act 1982* and the 2013 Hawke review of the FOI Act that the intelligence

¹²² Robinson (n 9).

¹²³ Henninger (n 12).

¹²⁴ Christopher Knaus and Jessica Bassano, 'How a Flawed Freedom-of-Information Regime Keeps Australians in the Dark', *The Guardian* (online, 2 January 2019) <<https://www.theguardian.com/australia-news/2019/jan/02/how-a-flawed-freedom-of-information-regime-keeps-australians-in-the-dark>>.

¹²⁵ Allan Hawke, *Review of the Freedom of Information Act 1982 and Australian Information Commissioner Act 1982* (Final Report, July 2013) 16, 36.

¹²⁶ *Archives Act 1983* (Cth) s 33.

¹²⁷ *McGrath and Director-General* (n 99).

¹²⁸ *Ibid* [128].

agencies should remain exempt from the FOI Act provisions.¹²⁹ Richardson rejected the idea of a class exemption for intelligence documents in the *Archives Act*. However he recommended that all security matters arising under the Act should be heard in the Security Division of the AAT.¹³⁰

1 *Palace Papers Litigation*

Reporter: Do you think the Queen knew about this course of action?

Whitlam: I shouldn't think so, but I don't know.

Reporter: Do you think the Governor-General took any advice from Buckingham Palace?

Whitlam: I don't know. I don't know. I was not informed that he had.¹³¹

A case concerning the application of FOI law in a particular context is *Hocking v Director-General of the National Archives of Australia*.¹³² The case concerns public access to a series of correspondence between the Queen and the Governor-General Sir John Kerr regarding the dismissal of the Whitlam Government in 1975, an event of enormous Constitutional significance in Australia.

Following Kerr's retirement, copies of his correspondence with the Queen were deposited with the Australian Archives by his Official Secretary under cover of a letter expressing the Queen's wishes and Kerr's instructions that the contents should remain closed for 60 years from his retirement.

Upon the enactment of the Archives Act, the correspondence became records forming part of the archival resources of the Commonwealth. Under the legislation, a 'Commonwealth record' must be made available for public access once within the open access period, which commences 31 years after the document's creation.

In 2016, Professor Jenny Hocking, a historian, requested access to the documents, which was denied by the Director General of the Archives on the basis that the correspondence did not constitute 'Commonwealth records' but was rather 'private correspondence' between the Queen and the Governor-General. Hocking challenged the decision and ultimately pursued the matter in the High Court, where she succeeded.

Ultimately, the decision turned on the definition of 'Commonwealth record' with a majority of the High Court finding that the

¹²⁹ *National Intelligence Community* (n 44) [43.75]-[43.78], recommendation 184, citing Australian Law Reform Commission, *Open Government: A Review of the Federal Freedom of Information Act 1982* (Report No 77, January 1996); Hawke (n 125).

¹³⁰ *National Intelligence Community* (n 44) [3.131].

¹³¹ Whitlam, (Interview, 11 November 1975), cited in Jenny Hocking, *The Palace Letters* (Scribe Publications, 2020), prior to contents page.

¹³² *Hocking v Director-General of the National Archives of Australia* (2020) ALR 395.

correspondence constituted 'Commonwealth records'. A 'Commonwealth record' means a record that is the property of the Commonwealth or of a Commonwealth institution, the latter including the official establishment of the Governor-General. The official establishment of the Governor-General is not the Governor-General, but does refer to organised staff provided at public expense for the assistance of the Governor-General.¹³³

The court found that 'property' in this context means a legally endorsed concentration of power to control physical custody of the record. Therefore, the correspondence was properly characterised at time of deposit as property of the official establishment of the Governor-General, regardless of whether the Commonwealth or Kerr as an individual was the true owner.¹³⁴

In her book, *The Palace Letters*, Hocking goes into the history of the litigation in great depth, pointing to a number of extraordinary aspects of the litigation:

1. The Commonwealth eventually spent some \$2 million in attempting to keep the correspondence out of public view;
2. a copy of Kerr's letters was initially available in the Commonwealth archives, however upon her making a request for them their status was changed on the basis that they were royal and thus personal;¹³⁵
3. the Archives initially refused to confirm or deny that there were other documents governing access to the letters;¹³⁶
4. Kerr's step-daughter signed a new instrument of deposit after proceedings commenced revoking the original conditions of deposit;¹³⁷
5. both the Federal Court at first instance and subsequently the Full Federal Court found that the correspondence constituted personal letters (and hence could be destroyed, sold or disposed of at the will of the person who they belonged to);
6. the Commonwealth initially refused to cap Hocking's fees in respect of the litigation, eventually agreeing to cap them at \$30,000 for the first round of litigation and for the appeal at \$60,000.

As set out by Hocking, the letters contain some extraordinary revelations. They reveal the Governor-General engaging in reports of political matters and meetings to the Queen's private secretary despite

¹³³ Ibid [86].

¹³⁴ Ibid [95], [165], [199].

¹³⁵ Hocking (n 131) 32-33.

¹³⁶ Ibid 47.

¹³⁷ Ibid 70-73.

the office of Governor-General being a politically neutral one.¹³⁸ The letters reveal Kerr discussing with the Queen's private secretary his unhappiness with some of Whitlam's advice and requesting his assistance in dealing with it.¹³⁹

They also demonstrate the palace's engagement with the question of the use of reserve powers to dismiss the Prime Minister where the Prime Minister had no knowledge of these discussions. This is of great significance given that, conventionally, the Governor-General is required to act on the advice of the Prime Minister.¹⁴⁰

Hocking has also discussed aspects of British intervention in the public's access to information. In her book she notes that documents in the British archives reveal the use of the term 'personal and confidential' deliberately applied to governor despatches to protect them from official record keeping.¹⁴¹ She has elsewhere discussed the palace's extraordinary secret interference in the creation of legislation to protect the property interests of the Crown.¹⁴²

The Palace Papers litigation is an example of the extraordinary lengths that the government has been prepared to go to in order to keep documents that are clearly an important part of Australian constitutional history from public view, spending some \$2 million in order to do so. It was only through the tenacity of an academic, financially supported by a GoFundMe campaign to cover legal costs, that the documents were eventually brought to light. While the arguments involved in the litigation were of a more technical nature, focusing on definitions of 'Commonwealth records' rather than arguments about the public interest, the case demonstrates that the path to obtaining documents that are clearly in the public interest can be a long, complicated and expensive one, and may be met with significant resistance.

B. *See no Evil: Observations*

Almost a decade after it was made, it is time to implement the 2013 recommendation for a review of the FOI regime. Recent studies indicate that the legislation is not functioning as intended, with many applications being rejected in whole or in part, and responses not made in a timely fashion.

Freedom of access to public information is a key plank in ensuring the accountability and transparency of government. However, a regime to allow access to information will not be effective without proper

¹³⁸ Ibid 176-81.

¹³⁹ Ibid 186-7.

¹⁴⁰ Ibid 189-93.

¹⁴¹ Ibid 78-9.

¹⁴² Jenny Hocking, 'A Royal Abuse of Political Power' (12 February 2021) *Pearls and Irritations*, <<https://johnmenadue.com/a-royal-abuse-of-political-power/>>.

funding, implementation and a culture of transparency underlying it. These things appear to be lacking in Australia's FOI regime at present.

IV Speak no Evil – Penalisation of Whistleblowing and Absence of Protection for Journalists

Even with the most robust schemes of FOI and internal accountability in place, the opportunity will always exist for governments and employees of government agencies to engage in illegal, corrupt, immoral or questionable behaviour, or simply to make mistakes that have consequences for the people they serve, which those persons, and others within their organisations, will not want to be revealed. For this reason, it is important that any democracy have in place protections for individuals within those organisations who learn of that conduct and make the decision to reveal it in the public interest in circumstances where the information would otherwise be kept secret. It is also vital to the free flow of communication that must underlie a representative democracy that the media be free to report on such matters, with appropriate consideration given to the need to protect national security information, as without the ability to bring this kind of conduct into public view, there is little point in protecting whistleblowers.

Since 2013, and after a lengthy history of discussion and debate, Australia has had in place a legislative mechanism for the protection of whistleblowers, however, as discussed below, the legislation has significant limitations. Further, recent years have seen a number of high-profile prosecutions of whistleblowers who have disclosed information that might broadly be considered to be in the public interest.

In the past, there has been push-back against journalists who reveal secret information, usually in the form of injunctions sought to restrain publication of the information. However, recent years have seen unprecedented attempts to investigate and consider prosecution of journalists who reveal sensitive information falling within the general remit of defence and intelligence. Further, the current broad range of offences that penalise the disclosure of government information, and the limitations on the defences available to journalists, have a potentially chilling effect on attempts to shed light on the kind of conduct that might be considered in the public interest to disclose.

A. Penalisation of Whistleblowing

I understand that I will be made to suffer for my actions but I will be satisfied if the federation of secret law, unequal pardon and irresistible

executive powers that rule the world that I love are revealed even for an instant.¹⁴³

Disclosures in the public interest, also known as ‘whistleblowing’, are essential in ensuring an effective system of open government that is accountable to the public.¹⁴⁴ ‘Whistleblowers’ are those who ‘report waste, fraud, abuse, corruption, or dangers to public health and safety to someone who is in the position to rectify the wrongdoing’.¹⁴⁵ They are generally motivated by a concern that the information they disclose should be revealed in the public interest.

In a 2020 report, Transparency International stated, ‘As government secrecy legislation grows, Australia’s strong traditions of independent journalism have been compromised. Indeed, the rights of all citizens to receive and share information, in the public interest, have been steadily disappearing.’¹⁴⁶ In recent years, in Australia and overseas, there have been high profile instances of pursuit and prosecution of persons charged with whistleblowing in circumstances where there is a strong arguable public interest in the disclosures they have made becoming public. Some of these cases are considered below.

1 *Secrecy offences*

In Australia, the disclosure of information held by government agencies is criminalised via a long catalogue of secrecy provisions. In the past, public servants who blew the whistle could be charged with an offence pursuant to s 70 of the Crimes Act, which prohibited a Commonwealth officer publishing or communicating any fact or document coming into their knowledge by virtue of being a Commonwealth officer, and which it is their duty not to disclose.

Now repealed, s 79 of the Crimes Act prohibited any person communicating a prescribed document or permitting another to have access to it, punishable by two years’ imprisonment. If done with the intention of prejudicing the security or defence of the Commonwealth, it was punishable by seven years’ imprisonment.

Sections 70 and 79 operated as ‘catch-all’ secrecy provisions. In 1991, the Gibbs Committee noted that the provisions drew no distinction between the disclosure of information that may cause real

¹⁴³ Glenn Greenwald, Ewen MacAskill and Laura Poitras, ‘Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations’, *The Guardian* (online, 11 June 2013) <<https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>>.

¹⁴⁴ Australian Law Reform Commission (n 5) 22.

¹⁴⁵ National Whistleblower Centre, *What is a Whistleblower?* (Web Page) <<https://www.whistleblowers.org/what-is-a-whistleblower/>>.

¹⁴⁶ AJ Brown et al, ‘Australia’s National Integrity System: The Blueprint for Action’ (Report, Transparency International Australia, 30 November 2020) 16.

harm to the public interest and disclosure of information that would cause no harm.¹⁴⁷

In 2011, the ALRC *Secrecy Laws and Open Government in Australia* (Report 112) found that there were 506 secrecy provisions in 176 pieces of legislation, including 358 criminal offences. The ALRC recommended that the general secrecy offences in the Crimes Act should be repealed and replaced with a new general secrecy offence in the Criminal Code, which should criminalise behaviour that harms essential public interests.¹⁴⁸

The ALRC also recommended narrowing the administrative secrecy provision in reg 2.1 of the *Public Service Regulations 1999* (Cth) to only apply to disclosures of information ‘reasonably likely’ to result in prejudice to the national interest, rather than disclosures ‘reasonably foreseeable’ to result in such prejudice.¹⁴⁹ However, such an amendment has never been made.

Sections 70 and 79 were repealed by Schedule 2 of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* and replaced in December 2018 by secrecy offences in Division 122 of the Criminal Code.¹⁵⁰ A number of amendments were made to the Bill prior to its enactment based on review by the PJCIS, including reduction of the proposed penalties.¹⁵¹

Section 122.1 prohibits Commonwealth officers communicating or dealing with ‘inherently harmful information’ that is obtained by that person by reason of their being a Commonwealth officer. Inherently harmful information is security classified information, information that was obtained by or made by an intelligence agency in connection with its functions or information relating to the operations of a law enforcement agency. As the definition of ‘inherently harmful information’ makes clear, there is no ‘harm’ requirement for the provision; rather the offence is based on dealings with information that by nature of classification or connection with an agency is deemed ‘inherently harmful’.

Section 122.2 applies to Commonwealth officers who communicate information obtained in their official capacity, where the communication causes harm to Australia’s interests or is likely to do so. It carries a maximum penalty of seven years’ imprisonment. Causing harm to Australia’s interests includes harming or prejudicing the

¹⁴⁷ Harry Gibbs, *Review of Commonwealth Criminal Law* (Final Report, December 1991) [25.12].

¹⁴⁸ Australian Law Reform Commission (n 5) 22 Recommendation 4-1.

¹⁴⁹ Australian Law Reform Commission (n 5) 15 Recommendation 12-1.

¹⁵⁰ The offence was repealed by Schedule 2 of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth).

¹⁵¹ Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Advisory Report, June 2018), discussed in *National Intelligence Community* (n 43) [35.44].

security or defence of Australia, or harming or prejudicing Australia's international relations in relation to certain information communicated in confidence. 'Security or defence of Australia' includes the operations, capabilities or technologies of, or methods or sources used by, domestic intelligence agencies or foreign intelligence agencies.¹⁵² While this provision does carry a harm element, the concept of harm to security, defence and international relations is one that leaves room for a great deal of interpretation and has the potential to encompass revelations of misconduct in intelligence agencies.

Section 122.4 applies where a person who obtains information in their capacity as a 'Commonwealth officer' or being engaged to work for a Commonwealth entity, and who is under a duty not to disclose it, communicates that information. The offence carries a two-year maximum penalty. There is no specification or limitation as to the type of information that cannot be communicated.

Section 122.4A applies to non-Commonwealth officers and prohibits communicating or dealing with information obtained by *another* person who is a Commonwealth officer or engaged to work for a Commonwealth entity. The offence applies, inter alia, if the information is classified, or the communication of the information damages the security or defence of Australia. The offence carries a maximum penalty of five years' imprisonment (communication) or two years (dealing).

It is a defence to any of these offences pursuant to s 122.5(4) if a person communicates or deals with information for the purposes of communicating the information in accordance with the *Public Interest Disclosure Act 2013* (Cth) ('PIDA') or the FOI Act. The scope of this defence is outlined below. It is also a defence if the person communicated or dealt with the information for the purpose of reporting to an appropriate government agency a criminal offence: s 122.5(4A).

Richardson notes that the introduction of the general secrecy provisions in Division 122 introduced the 'harm-based' approach that had been recommended by the Gibbs Committee and the ALRC.¹⁵³ However, as noted above, the definitions of 'inherently harmful information' and 'cause harm to Australia's interests' are so broad as to effectively negate the threshold requirement that a 'harm' component might otherwise have established.

Section 90.1 defines 'information' as 'information of any kind, whether true or false and whether in a material form or not', and includes an opinion and a report of a conversation.

Section 91 of the Criminal Code creates the offence of 'Espionage'. Section 91.1 prohibits dealing with information or an article that has a

¹⁵² *Criminal Code Act 1995* (Cth) s 121.1.

¹⁵³ *National Intelligence Community* (n 43) [35.27].

security classification or concerns Australia's national security, where the person intends to prejudice Australia's national security or advantage the national security of a foreign country, and the conduct results in the information being communicated to a foreign principal or person acting on their behalf. The offence carries a maximum penalty of life imprisonment, or 25 years where the conduct is reckless. 'National security' is broadly defined and includes defence of the country, protection of any part of the country or the people, protection of border integrity, and Australia's political, military or economic relations with another country.¹⁵⁴

Section 91.2 prohibits 'dealing with' information or an article with intention to prejudice national security and where the conduct results or will result in the information being communicated or made available to a foreign principal. That offence carries a penalty of 25 years' imprisonment, while an alternative offence of recklessness carries a penalty of 20 years' imprisonment. It should be kept in mind that 'intention' in the context of the Code with respect to a circumstance (such as prejudice to national security) means that the person 'believes that it exists or will exist': s 5.2. In other words, if the person communicating the information believes that it will prejudice national security, then the element is made out, regardless of whether that was their 'motivation'.

Section 91 does not provide for a 'public interest' defence. The person's motive in communicating the information is therefore irrelevant.

There is also a long list of more specific provisions dealing with the disclosure of particular categories of information. Only a few are referred to here.¹⁵⁵

Sections 39, 39A, 40 and 40B of the *Intelligence Services Act 2001* (Cth) ('Intelligence Services Act') set out offences for employees of ASIS, AGO, ASD and DIO. Section 39 creates an offence if a person communicates any information acquired or prepared by ASIS in connection with its functions and the information has come to their knowledge by their being a staff member of having a contract with ASIS, and the other provisions contain similar prohibitions for employees of the other agencies. There is no harm threshold for these offences.

Section 42 of the *Australian Border Force Act 2015* (Cth) ('Australian Border Force Act') prohibits an 'entrusted person' making a record of or disclosing Immigration and Border Protection information. Section 48 of the Act contains a limited exception where an entrusted person reasonably believes that disclosure is necessary to prevent or lessen a serious threat to the life or health of an individual

¹⁵⁴ See (n 152) s 90.4.

¹⁵⁵ A number of specific secrecy offences are discussed in *National Intelligence Community* (n 43) [35.32].

and the disclosure is for the purposes of preventing or lessening that threat.

The original definition of ‘protected information’ in the Act was very broad: information obtained by a person in their capacity as an entrusted person. However, following a challenge to the constitutionality of the legislation by a group of medical professionals, the government amended the Act to omit the definition of ‘protected information’ and substitute ‘Immigration and Border Protection information’, which is largely limited to information the disclosure of which would prejudice security or international relations, prejudice the prevention, detection or investigation of an offence, or could reasonably be expected to prejudice the protection of public health or endanger life or safety.¹⁵⁶ This includes information that has a security classification, or originated with or has been received from an intelligence agency.¹⁵⁷

The Refugee Advice and Casework Service has commented that the Australian Border Force Act has a chilling effect on disclosures that may be made in the public interest.¹⁵⁸ It has been noted that the *Public Interest Disclosure Act 2013* (Cth)(discussed below) does not allow disclosure of ‘sensitive law enforcement information’, which may well be interpreted to include much of what happens in detention centres.¹⁵⁹

As at the time of writing, there were no reported cases in existence for offences pursuant to Division 122 or s 91 of the Criminal Code, s 42 of the Australian Border Force Act, or ss 39, 39A, 40 and 40B of the Intelligence Services Act (other than the ongoing matters of Witness K and Bernard Collaery, referred to above).¹⁶⁰

2 *Public Interest Disclosure Act 2013* (Cth) (‘PIDA’)

The PIDA was introduced as a means of providing some protection for those who disclose confidential information in the public interest.¹⁶¹ Prior to the PIDA, the only federal protections were contained in the *Public Service Act 1999* (Cth), prohibiting victimisation for reporting misconduct.

¹⁵⁶ *Australian Border Force Act 2015* (Cth) s 4; amendments introduced by the Australian Border Force Amendment (Protected Information) Bill 2017.

¹⁵⁷ *Ibid* s 4(5).

¹⁵⁸ Senate Legal and Constitutional Affairs Legislation Committee, *Australian Border Force Amendment (Protected Information) Bill 2017*, (September 2017).

¹⁵⁹ Khanh Hoang, ‘Of Secrecy and Enforcement: Australian Border Force Act’ (2015) 14 *LSJ: Law Society of NSW Journal* 78-79.

¹⁶⁰ In *AS v Minister for Border Protection and Immigration (No 3)* (2015) 307 FLR 122, it was necessary for a class action litigant to obtain an order from the court allowing disclosure of ‘protected information’ within the Australian Border Force Act for the purposes of the litigation.

¹⁶¹ There are also Public Interest Disclosure Acts in force in every state and territory: see *Protected Disclosures Act 2012* (Vic), *Public Interest Disclosure Act 2012* (ACT), *Public Interest Disclosure Act 2003* (WA), *Public Interest Disclosures Act 1994* (NSW), *Public Interest Disclosure Act 2008* (NT), *Public Interest Disclosures Act 2002* (Tas) and *Whistleblowers Protection Act 1993* (SA).

There was a lengthy lead up to the enactment of the PIDA, commencing with a review by the Senate Select Committee on Public Interest Whistleblowing in 1994.¹⁶² In 2004, the ALRC *Keeping Secrets* report recommended introducing a comprehensive public interest disclosure regime to clarify protections for whistleblowers (including coverage of defence, security and intelligence agencies). It also recommended a review of all laws and regulations that create duties not to disclose information. It recommended that the duty of secrecy should be imposed only in relation to information genuinely requiring protection and where disclosure is likely to harm the public interest.¹⁶³

In 2009, the House of Representatives Standing Committee on Legal and Constitutional Affairs reported on its inquiry into whistleblower protections.¹⁶⁴ That report noted the importance of whistleblowing in contributing to the integrity and accountability of government. However, the protections afforded by the PIDA contain some serious limitations.

Section 10 of the PIDA provides that public officials who make public interest disclosures are protected from civil, criminal and administrative liability. The exceptions in s 10 of the Act only apply if the information disclosed tends to show or the discloser believes on reasonable grounds that the information tends to show, an instance of ‘disclosable conduct’ as defined in s 29. This includes conduct that contravenes a law, perverts the course of justice or involves corruption or maladministration, is an abuse of public trust, results in wastage of public money or property, or unreasonably results in a danger to health or safety, or results in increased risk of danger to the environment. A disclosure must fit within one of these categories in order to warrant protection. Further, the disclosure must not be, on balance, contrary to the public interest.¹⁶⁵

Notably, information that can be the subject of a ‘public interest disclosure’ does not include ‘intelligence information’, unless there is a substantial and imminent danger to health or safety and the person disclosed only information relating to intelligence agencies in general terms.¹⁶⁶ The definition of ‘Intelligence information’ is extremely broad and includes information that has originated with, or been received from, an intelligence agency. It also includes ‘sensitive law enforcement information’ meaning information disclosure of which is reasonably likely to prejudice Australia’s law enforcement interests including interests in avoiding disruption to national and international efforts

¹⁶² Senate Select Committee on Public Interest Whistleblowing, *In the Public Interest: Report of the Senate Select Committee on Public Interest Whistleblowing* (Report, 1994).

¹⁶³ Australian Law Reform Commission (n 26) Recommendations [3.1]–[3.3] and [5.78].

¹⁶⁴ *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (Report, February 2009) [1.3] (‘*Whistleblower Protection Report*’).

¹⁶⁵ *Public Interest Disclosure Act 2013* (Cth) s 26.

¹⁶⁶ *Ibid* ss 26(1)(c), 41.

relating to law enforcement, criminal intelligence, criminal investigation, etc.¹⁶⁷

Further, the information that is disclosed must not disclose more than is reasonably necessary to identify one or more instances of wrongdoing.¹⁶⁸ In the case of an emergency disclosure, the disclosure must be no greater than is necessary to alert the recipient to the substantial and imminent danger.¹⁶⁹

Before the defence can be relied upon, the information must have been first disclosed internally or to the Ombudsman or another investigative agency. Only if the person disclosing reasonably believes that this process has been inadequate can the defence apply.¹⁷⁰ This requirement can be bypassed if the person 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, however this still does not apply if the information is intelligence information.

While the reasoning behind it is obvious, the internal reporting prerequisite also poses issues for potential whistleblowers. If a whistleblower considers it unlikely that reporting authorities will take their report seriously, or act upon it, they have to make a difficult decision. If they fail to report internally, they will not have complied with the legislation. However, by doing so, they effectively 'out' themselves as the informer to the relevant agency, virtually ensuring that any subsequent leak can be traced back to them. By contrast, a stakeholder committee in the US has recommended that state whistleblower laws allow anonymous internal reports to be made, which protect against such a risk.¹⁷¹

3 *Recent Whistleblower Prosecutions*

High profile recent examples of whistleblowing in Australia and overseas, where whistleblowers have faced or are facing prosecution, include:

1. the prosecution of Chelsea Manning, who leaked 500,000 secret military documents and videos of US forces killing Iraqi and Afghani civilians to WikiLeaks and was sentenced to 35 years imprisonment;
2. the prosecution of Edward Snowden, who released details of a worldwide data mining program being carried out by the United States Government's National Security Agency;

¹⁶⁷ Ibid s 8, 41.

¹⁶⁸ Ibid s 26(1) item 2(f).

¹⁶⁹ Ibid s 26(1) item 3(b).

¹⁷⁰ Ibid s 26 item 2(b) and (c).

¹⁷¹ Cited in 'National Security, Leaks and Freedom of the Press', *The Lawfare Podcast* (Lawfare Institute, 20 April 2021).

3. the prosecution of a customs officer, Kessing, under s 70 of the Crimes Act for revealing the contents of two classified reports revealing lax airport security procedures to journalists, which led to a major review of airport security;¹⁷²
4. the prosecution of Australian Taxation Office ('ATO') employee Richard Boyle for 24 (originally 66) offences relating to his revelations of ATO officials seizing funds from taxpayer accounts;
5. the prosecution of military lawyer David McBride, who was charged with a range of offences including theft of Commonwealth property, unauthorised disclosure of a Commonwealth document, and unlawfully giving information about Australia's defence capabilities; and
6. the prosecutions of Bernard Collaery and Witness K, discussed above.

Each of these persons has arguably disclosed information that there is a strong public interest in having in the public domain. Conversely, there is a real question as to whether there is any harm to the public interest as a result of disclosing the information. However, notwithstanding attempts over the last two decades to take measures to protect whistleblowers, there is a continuing legislative gap in relation to the effective protection of those who blow the whistle in the public interest, often at great personal cost.

Richard Boyle's case is a good example of the potential limitations of the public interest defence. Boyle, an ATO employee, revealed to the media what he considered to be aggressive debt collection practices allowing the ATO to seize funds from taxpayer bank accounts without notice. He initially reported internally within the ATO, which dismissed his concerns in an investigation that the Senate Economics Legislation Committee later commented 'could appear to the public to be superficial in addressing the concerns raised by ATO whistleblowers'.¹⁷³

It was only after his complaint was dismissed that Boyle approached the media. Subsequently, the Tax Ombudsman conducted a review, finding in part that the ATO did not always use its garnishee power proportionately and appropriately.¹⁷⁴

¹⁷² *R v Kessing* (2008) 73 NSWLR 22.

¹⁷³ Nassim Khadem, 'ATO Did a "Superficial" Investigation into Whistleblower Richard Boyle's Public Interest Disclosure', *Parliament Told*, *ABC News* (online, 18 June 2020), <<https://www.abc.net.au/news/2020-06-18/ato-whistleblower-richard-boyle-senator-rex-patrick-parliament/12365136>>.

¹⁷⁴ Inspector-General of Taxation, 'Review into the ATO's Use of Garnishee Notices – IGT Report Publicly Released', *Australian Government Inspector-General of Taxation* (Web Page, 13 March 2019) <<https://www.igt.gov.au/media-releases/ato-garnishee-notices-igt-report-released/>>.

Notwithstanding the fact that Boyle's initial internal reports were dismissed and subsequently found to be justified at least in part, prosecutors recently announced that the prosecution of charges against Boyle would continue in respect of 24 of the original 66 charges against him.¹⁷⁵

Former military lawyer David McBride released to the media material that formed the basis of Oakes and Clark's reporting into war crimes in Afghanistan (discussed below). McBride's reporting to the media only came after unsuccessful attempts to raise the issues internally and with the AFP.

Justice Brereton, who conducted an inquiry into war crimes in Afghanistan, recommended that no action be taken against those who helped to shed light on the war crimes (whose names are redacted). The report also recommends that serving members who have assisted in the exposure of misconduct, or are known to have acted with propriety and probity, be promoted at the earliest opportunity.¹⁷⁶ Notwithstanding that recommendation, as at the time of writing, McBride stands charged with five offences including theft of Commonwealth property and unauthorised disclosure of material to journalists. The Senate Standing Committee on Environment and Communications has recommended that the Commonwealth Director of Public Prosecutions ('CDPP') reconsider the prosecution on the grounds of public interest.¹⁷⁷

There is almost no protection under the PIDA for reporting on information relating to intelligence agencies. Williams and Hardy opine that under the current public interest disclosure regime, an Australian intelligence officer who became involved in conduct that they believed to be highly immoral and disclosed it, would not be protected by the PIDA, even if they took care not to divulge any operations, sources, methods or identities.¹⁷⁸ Even in circumstances where there was a substantial and imminent danger to health, safety or the environment, an intelligence officer could not legally divulge 'intelligence information' pursuant to these provisions, including to a journalist or a Member of Parliament.¹⁷⁹

¹⁷⁵ Nassim Khadem, 'Prosecutors Proceed with Case Against ATO Whistleblower Richard Boyle', ABC News (online, 30 April 2021) <<https://www.abc.net.au/news/2021-04-29/prosecutors-proceed-case-against-ato-whistleblower-richard-boyle/100105710>>.

¹⁷⁶ Inspector General of the Defence Force, *Report of Inquiry under Division 4A of Part 4 of the Inspector-General of the Australian Defence Force Regulation 2016 into Questions of Unlawful Conduct Concerning the Special Operations Task Group in Afghanistan* (Report, November 2020) 111.

¹⁷⁷ Senate Standing Committee on Environment and Communications, *Inquiry into Press Freedom* (Report, 19 May 2021) Recommendation 17.

¹⁷⁸ Keiran Hardy and George Williams, 'Terrorist, Traitor or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information' (2014) 37(2) *UNSW Law Journal* 748, 815.

¹⁷⁹ *Ibid.*

Brown notes that the definition of ‘intelligence information’ is so broad that in an emergency situation, the exemption for disclosing information involving intelligence agencies (which may be disclosed in an emergency) may well not apply, as that information would arguably fall within the intelligence information definition in any case (which may not be disclosed in an emergency). The practical effect of the laws, it is noted, is such that corruption in an intelligence agency could never be protected under the PIDA.¹⁸⁰

The Senate Standing Committee on Environment and Communications recently noted that these provisions preclude disclosure of matters intended to be covered by the PIDA that would not necessarily harm national security interests.¹⁸¹ Transparency International has recommended the removal of these blanket carve-out provisions for ‘intelligence information’ and ‘inherently harmful information’ from whistleblowing laws.¹⁸² It has also recommended the introduction of a test as to whether it is ‘reasonable in all the circumstances’ for disclosure to be made to an external party ‘to ensure that it is effectively investigated’, similar to the principle underpinning provisions in New South Wales, Queensland, Western Australia, the ACT, United Kingdom and Ireland.¹⁸³

The limitations to the PIDA are significant, keeping in mind the fact that simply because information is sourced from or associated with an intelligence agency does not mean that its disclosure is inherently risky for national security or national interest. Brian Toohey cites politicians including Gareth Evans who commented that in his thirteen years in Cabinet, ‘very little of any of the stuff that was ... gleaned [by ASIO or ASIS] added much value to our understanding of what was going on let alone vital to our security interests’.¹⁸⁴

In the 1970s, when Defence Head Arthur Tange demanded evaluations of damage that could be done via leaks of classified documents, following a string of such leaks, senior official Bob Hamilton said, ‘I do not consider the full or partial revelation as seriously or irretrievably damaging to our diplomatic or defence interests or those of our friends and allies, and I consider that further revelations would generally add only marginally to the damage’.¹⁸⁵

The lack of protection for intelligence agency whistleblowers does not appear likely to change any time soon, with the PJCIS and the

¹⁸⁰ AJ Brown, ‘Towards “Ideal” Whistleblowing Legislation? Some Lessons from Recent Australian Experience’ (2013) 2(3) *Labour Studies* 4, 29-30.

¹⁸¹ Senate Standing Committee on Environment and Communications (n 177) [4.41].

¹⁸² Brown et al (n 146) E-12.

¹⁸³ Ibid.

¹⁸⁴ Brian Toohey, ‘The Uses and Abuses of Intelligence’ cited in Brian Toohey, *Secret: The Making of Australia’s Security State* (Melbourne University Press, 2019).

¹⁸⁵ Brian Toohey, ‘Inspector Tange Investigate’ cited in Brian Toohey, *Secret: The Making of Australia’s Security State* (Melbourne University Press, 2019).

Richardson review recommending that neither specific secrecy offences relating to intelligence agencies nor general secrecy provisions in the Code should be amended to include an exception or defence for disclosures made in the public interest.¹⁸⁶

The Richardson report referred to an Australian Intelligence Community ('AIC') submission to the ALRC's secrecy inquiry that individuals should not be arbiters of which disclosures constitute damage to the public interest as such individuals are 'not in a position to have an appropriate understanding or appreciation of the possible national security impact of releasing that information'.¹⁸⁷ Richardson agreed that individual officers or disclosers are unlikely to have appropriate context or understanding of the potential impact of the relevant disclosure or be able to assess how it may harm the public interest.¹⁸⁸

Such an argument effectively precludes the ability of any intelligence agency to be held to account outside of the regulatory oversight arrangements that exist for that agency. This is a significant limitation on the ability of whistleblowers to draw to public attention wrongdoing within intelligence agencies, no matter how egregious.

In 2016, a review carried out by Philip Moss found that the PIDA had been difficult to apply in practice. The review recommended that the Commonwealth public sector's pro-disclosure culture be strengthened by encouraging reporting of wrongdoing to be seen as part of the ordinary work of agencies. He also recommended increasing the capacity of the Ombudsman and the Inspector General of Intelligence and Security to oversee the PIDA.¹⁸⁹

In December 2020, the Australian Government published its response to the Moss report. The response included:¹⁹⁰

1. agreement with the recommendation to strengthen the oversight of the Ombudsman and Inspector-General of Intelligence and Security (Recommendation 3);
2. encouraging disclosures and strengthening support for internal whistleblowing (Recommendation 24);
3. that consideration be given to restructuring the Act to make it easier to navigate; and
4. consider mandatory reporting of aggregated statistics relating to public interest disclosures, in tandem with the Ombudsman's office.

¹⁸⁶ Parliamentary Joint Committee on Intelligence and Security (n 151) [5.97].

¹⁸⁷ *National Intelligence Community* (n 44) [35.172].

¹⁸⁸ *National Intelligence Community* (n 44) [35.178].

¹⁸⁹ Philip Moss, *Review of the Public Interest Disclosure Act 2013* (Report, July 2016) 7.

¹⁹⁰ Australian Government, *Australian Government Response to the Review of the Public Interest Disclosure Act 2013* (Report, May 2021).

In 2017, the Parliamentary Joint Committee on Corporations and Financial Services ('PJCCFS') found that whistleblower protections have little practical effect in the public or private sectors.¹⁹¹ It recommended that a single Whistleblower Protection Authority be established covering both sectors. A number of recommendations, including the establishment of a single regime covering corporate, financial and credit sectors, were implemented with the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019* (Cth), however further recommendations in relation to the need for support for whistleblowers have not been implemented.¹⁹²

In a statement to the Senate Standing Committee on Economics, the Inspector-General of Taxation noted that her statutory framework was not designed to allow whistleblowing, and that her office was unable to offer whistleblowers protection. The Committee endorsed the recommendation of the PJCCFS for a single Whistleblower Protection Authority and suggested that this be considered as part of a review of the PIDA recommended to be carried out in 2021 (the recommended review has not yet taken place). It also recommended that whistleblowing tax officials should be automatically protected once an Inspector General Taxation Office review was being contemplated, without the need for the Tax Commissioner to authorise disclosures.¹⁹³

In tandem with reforms to the PIDA, consideration also needs to be given to the range and scope of secrecy offences. The Human Rights Law Commission and the Law Council of Australia have both noted that a recurring element of secrecy offences is the lack of an express element of harm to an essential public interest.¹⁹⁴ The ALRC's recommendations for an express harm element to be added to secrecy offences is being considered as part of a review of secrecy provisions by the Attorney General's Department.¹⁹⁵ No record is available of this review having been finalised at time of writing.

While there is a legitimate interest in keeping secret information that truly has the potential to prejudice Australia's national interests, careful scrutiny must be given to how that threshold is applied. Blanket prohibitions on the disclosure of information by public servants, regardless of whether that has the potential to cause harm, or without a clear definition of 'harm', cast the net too broadly in favour of secretisation, and place significant limitations on the ability of whistleblowers to draw to public attention wrongful conduct.

¹⁹¹ Parliamentary Joint Committee on Corporations and Financial Services, *Whistleblower Protections* (Report, 13 September 2017) ix.

¹⁹² Brown et al (n 146) E-6-E-10.

¹⁹³ Senate Standing Committee on Economics, *Performance of the Inspector-General of Taxation* (Report, June 2020) Ch 4.

¹⁹⁴ *Law Enforcement and Intelligence Powers on the Freedom of the Press* (n 10) [3.213]-[3.215].

¹⁹⁵ *Ibid* [3.223].

Moreover, the broad scope of these offences allows for selective enforcement, in circumstances where it is reported that politicians and staffers routinely leak classified information for political purposes.¹⁹⁶

There are a number of key improvements that can be made to ensure that there is adequate protection for those who reveal information that is in the public domain:

1. that prohibition on release of information contains a ‘harm’ test so that the disclosure of information that does no harm is not penalised;
2. inclusion of a public interest test so that even where there is or may be harm as a result of disclosure, a defence may apply where, on balance, disclosure of the information is in the public interest; and
3. revising the notion of ‘public interest disclosure’ under the PIDA so that it does not exclude such a broad range of conduct or activity involving intelligence agencies, and provides a defence for disclosure where it is not reasonably likely that will harm national security.

Assuming that they are conducted, the Attorney-General’s Department review of secrecy provisions and the recommended review of the PIDA are opportunities to consider these issues.

B. Reporting of Information by the Media in the Public Interest

It is unacceptable, in our democratic society, that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticise government action.¹⁹⁷

1 *Prosecution of Journalists*

It is vital to the preservation of our democracy that journalists who report on information in the public interest are protected from prosecution, and from the requirement to identify their sources. This extends to the reporting of information about matters that may be related to national security, particularly the conduct of intelligence agencies and the armed forces. Some of the most compelling and shocking disclosures of information through journalists have been of this type.

¹⁹⁶ Paul Barratt, ‘The Right to Know and the Role of the Whistleblower’ in Felicity Ruby and Peter Cronau (eds), *A Secret Australia: Revealed by the WikiLeaks Exposés* (Monash University Publishing, 2020).

¹⁹⁷ *Commonwealth v John Fairfax & Sons* (1980) 147 CLR 39 at 494.

As Brian Toohey notes, ‘At [intelligence’s] worst, governments can falsely claim they have intelligence that justifies aggression and wasteful national security spending, and helps demonise foreign political leaders’.¹⁹⁸ It is important that when it does, the public is made aware of it.

For example, Daniel Ellsberg’s leaking of the *Pentagon Papers* exposed lies that had been told by the United States government about the Vietnam War. Toohey writes that in 1976, the Australian Joint Intelligence Organisation listed more than 40 journalists who had published significant intelligence leaks between 1972 and 1975. This volume of leaks reflected a greater willingness in countries like Australia to subject secret institutions to scrutiny after the exposure of the lies told by the US government regarding the Vietnam War.¹⁹⁹

Partly motivated by Ellsberg’s actions, in 1971 Perry Fellwock, a former employee of the National Security Agency gave an interview to *Ramparts* magazine. Using the name ‘Winslow Peck’ he revealed the extent of the activities of the National Security Agency, including the monitoring of calls of some US citizens and communications from ‘allied’ countries.²⁰⁰ There is a striking similarity between these revelations and the reporting of Annika Smethurst, discussed below.

As far as it is possible to tell, there have been no reported instances of prosecutions of journalists in Australia or the United Kingdom for disclosing national security information, and until the prosecution of Julian Assange, none in the United States.

In the United States, in 2009, journalist James Rosen reported on information leaked by Department of State official Jin-Woo Kim that North Korea may undertake nuclear testing in response to UN sanctions. Kim was subsequently prosecuted, despite his revelations being described by a State Department official as a ‘nothing burger’. Rosen was the subject of a warrant obtained from a federal judge to seize the contents of his emails on the basis that there was ‘probable cause’ he was a co-conspirator. However, it was subsequently announced by the government that Rosen would not be prosecuted.²⁰¹ In the context of this and a spate of other warrants on journalists, US journalists commented that the practice of ‘spying’ on journalists was having a chilling effect preventing sources and whistleblowers from coming forward.²⁰²

¹⁹⁸ Toohey (n 184).

¹⁹⁹ Toohey (n 185).

²⁰⁰ Wikileaks, Perry Fellwock (Webpage) <https://wikileaks.org/wiki/Perry_Fellwock>.

²⁰¹ Peter Maass, ‘Destroyed by the Espionage Act’, *The Intercept* (online, 18 February 2015) <<https://theintercept.com/2015/02/18/destroyed-by-the-espionage-act/>>.

²⁰² Ryan Gallagher, ‘Government Spying on Fox News Reporter Even Worse than AP Case’, *Slate* (online, 20 May 2013) <<https://slate.com/technology/2013/05/james-rosen-spied-on-his-case-is-even-worse-than-the-ap-reporters.html>>.

The ongoing high-profile case of Julian Assange reflects the ongoing debate about the public's 'right to know' and the need to preserve security. As at the time of writing, Assange was in custody in the United Kingdom awaiting extradition to the United States, where he is charged with offences relating to the release of thousands of pages of classified documents.

From an Australian perspective, some of the things revealed by the WikiLeaks documents in the Australian context include the revelation of the bleak prospects of the war in Afghanistan, which contrasted with the optimistic projections of then Prime Minister Kevin Rudd. The implications of this lack of transparency have become startlingly clear with recent events in Afghanistan. In the United Kingdom context, the documents revealed a deference to US interests.²⁰³

In the United States, the leaked documents have revealed a vast array of wrongdoing by government forces, including the deliberate killing of civilians in Iraq, condoning of torture by Iraqi civilians, and the direct and cold-blooded killing of civilians and two journalists. The 'Guantanamo files' record the details of detainees at Guantanamo Bay, including that many people who were detained had no links to terrorism. The files known as 'Vault 7' speak to the widespread surveillance of United States citizens by their government.²⁰⁴

It is hard to see how it is not in the public interest for these things to be in the public domain. While there may be instances where prejudice has been caused to national security, it is undeniable that it is in the public interest to know the extent and scale of wrongdoing by armed forces.

The characterisation of Assange as a journalist is controversial. Some argue that as a releaser of documents he is not a journalist,²⁰⁵ and that he has in fact partnered with news agencies in relation to the leaking of many of the documents. Others point to WikiLeaks as a form of 'new journalism' whereby the public is given access to the 'raw data' rather than it being filtered through a journalism lens, so that the public is armed with the information to form their own conclusions and mount their own arguments.²⁰⁶

²⁰³ Barratt (n 196).

²⁰⁴ Ibid; Julian Burnside, 'The Wikileaks Decade' in Felicity Ruby and Peter Cronau (eds), *A Secret Australia: Revealed by the WikiLeaks Exposes* (Monash University Publishing, 2020); David Leigh, James Ball, Ian Cobain and Jason Burke, 'Guantanamo Leaks Lift Lid on World's Most Controversial Prison', *The Guardian* (online, 25 April 2011) <<https://www.theguardian.com/world/2011/apr/25/guantanamo-files-lift-lid-prison>>; 'Wikileaks releases thousands of "Vault 7" documents, reveals CIA's "entire hacking capacity"', *ABC News* (online, 8 March 2017) <<https://www.abc.net.au/news/2017-03-08/wikileaks-releases-thousands-of-documents-cia-revelation/8334366>>.

²⁰⁵ Robert Mahoney, 'For the Sake of Press Freedom, Julian Assange Must Be Defended', *Committee to Protect Journalists* (online, 11 December 2019) <<https://cpj.org/2019/12/press-freedom-julian-assange-wikileaks-defend/>>.

²⁰⁶ For example, 'In the Context of Empire: Episode 40', *The Pathology of Government* (Kevin Gosztola, 28 February 2021); Sulette Dreyfus, 'The Origins and Outcomes of a Digital

While Assange has been criticised for irresponsibility in releasing the documents in a wholesale fashion, the Editor-in-Chief of Wikileaks has noted that a third of the Afghan War Diary documents that WikiLeaks had obtained were withheld and not disclosed, and all Iraq War Logs were redacted before being given to journalists.²⁰⁷ Material leaked in partnership with *The Guardian* went through a process to redact vulnerable sources and anything that would compromise active special operations.²⁰⁸

Assange's lawyer, Jennifer Robinson, has noted that during the Chelsea Manning trial, a counter-intelligence witness was unable to identify a single instance of anyone who had been put at risk by the publication.²⁰⁹ The editor of *The Guardian* noted the same.²¹⁰ Yet the charges against Assange remain current and if extradited to the United States (which at time of writing seems likely to occur, subject to judicial review or an appeal to the European Court of Human Rights), he will face prosecution and potentially a lengthy prison sentence.

As detailed at the beginning of this paper, in June 2019, the AFP executed warrants issued by a magistrate on journalist Annika Smethurst and the ABC. Smethurst had authored a series of articles based on a Top Secret Departmental memo containing a proposal to expand the powers of the Australian Signals Directorate ('ASD'), including to allow the ASD to covertly access people's digital information without a warrant.²¹¹

A Federal Court judge issued a search warrant authorising a search of Smethurst's home. The warrant described the offence it related to as communication of a document or article to a person, that was not in the interests of the Commonwealth, and permitted that person to have access to the document, contrary to s 79(3) of the Crimes Act.²¹²

The High Court subsequently found the warrant to be invalid on the basis that it did not properly identify and describe the relevant offence. It was therefore unnecessary for the Court to consider an argument that

Pioneer' in Felicity Ruby and Peter Cronau (eds), *A Secret Australia: Revealed by the WikiLeaks Exposes* (Monash University Publishing, 2020).

²⁰⁷ Felicity Ruby and Peter Cronau, 'Secret no More' in Felicity Ruby and Peter Cronau (eds), *A Secret Australia: Revealed by the WikiLeaks Exposes* (Monash University Publishing, 2020).

²⁰⁸ Alan Rusbridger, 'WikiLeaks: The Guardian's Role in the Biggest Leak in the History of the World', *The Guardian* (online, 29 January 2011) <<https://www.theguardian.com/media/2011/jan/28/wikileaks-julian-assange-alan-rusbridger>>.

²⁰⁹ Robinson (n 9).

²¹⁰ Rusbridger (n 208).

²¹¹ Annika Smethurst, 'Spying Shock: Shades of Big Brother as Cyber-Security Vision Comes to Light', *Daily Telegraph* (online, 29 April 2018) <<https://www.dailytelegraph.com.au/news/nsw/spying-shock-shades-of-big-brother-as-cybersecurity-vision-comes-to-light/news-story/bc02f35f23fa104b139160906f2ae709>>.

²¹² *Crimes Act 1914* (Cth) s 79(3) actually makes it an offence to communicate a 'prescribed document or article' or 'prescribed information' to a person other than a person to whom she is authorised to communicate it, or a person to whom it is, in the interest of the Commonwealth, her duty to communicate it.

the warrant infringed the implied freedom of communication in relation to political matters.²¹³ However, by majority the High Court found that the AFP should not be compelled to destroy or return the information seized under the warrant.

The raid on the ABC concerned reports made by Dan Oakes and Sam Clark entitled 'The Afghan Files' which were based on secret defence force documents and revealed possible war crimes committed by Australian Special Forces in Afghanistan including the killing of unarmed detainees. The information had been disclosed by David McBride, a military lawyer who at time of writing was charged with offences relating to disclosure (discussed in this article). Their reports revealed investigations into the killing of unarmed civilians and children by Australian forces, and cultural issues within the special forces leading to desensitisation to these kinds of killing.²¹⁴

Justice Abraham of the Federal Court rejected a constitutional challenge to the validity of the warrant executed on the ABC, finding that s 3E of the Crimes Act imposed a justified and proportionate burden on political communication.²¹⁵ University of Queensland academic Dr Rebecca Ananian-Walsh has commented that this decision confirms that 'the implied freedom of political communication is an inadequate tool for protecting press freedom in Australia'.²¹⁶ The potential for the implied freedom to protect whistleblowers and journalists is discussed below.

Oakes and Smethurst were referred to the CDPP for possible prosecution, however a decision was subsequently made that no prosecution would be brought against them. In Oakes' case, the decision not to proceed was made based on the public interest.²¹⁷

The secrecy offence that relates to non-Commonwealth Officers includes a journalism-based defence: s 122.5(6). It is a defence to the offences in that division if a person who communicates information is a person engaging in a business reporting news who reasonably believed that communicating the information was in the public interest. As discussed above, the defence does not apply to the disclosure of 'intelligence information'.

²¹³ *Smethurst v Commissioner of Police* (2020) 376 ALR 575.

²¹⁴ Dan Oakes and Sam Clark, 'The Afghan Files: Defence Leak Exposes Deadly Secrets of Australia's Special Forces', *ABC News* (online, 11 July 2017) <<https://www.abc.net.au/news/2017-07-11/killings-of-unarmed-afghans-by-australian-special-forces/8466642?nw=0&r=HtmlFragment>>.

²¹⁵ *ABC v Kane (No 2)* [2020] FCA 133.

²¹⁶ Rebecca Ananian-Walsh, 'The 2019 AFP Raids on Australian Journalists Background Briefing 1/2020' (Policy Paper, 2020).

²¹⁷ Jordan Hayne, 'AFP Will Not Lay Charges Against Annika Smethurst Over Publishing of Classified Intelligence Documents', *ABC News* (online, 27 May 2020) <<https://www.abc.net.au/news/2020-05-27/afp-will-not-lay-charges-annika-smethurst-raid/12291238>>; 'ABC journalist Dan Oakes will not be prosecuted over Afghan Files leak', *ABC News* (online, 15 Oct 2020) <<https://www.abc.net.au/news/2020-10-15/dan-oakes-afghan-files-prosecution-decision/12771304>>.

In December 2019, two months after the raids on Smethurst and the ABC, the ALRC identified press freedom and whistleblowing as one of the most pressing areas in which law reform is required.²¹⁸ Transparency International has called for the introduction of ‘shield laws’ to protect journalists from prosecution for reporting on whistleblower disclosures.²¹⁹

Inquiries were referred to the PJCIS and to the Senate Committees on Environment and Communications.

The PJCIS inquiry noted that the raids on journalists were reported to have a flow-on effect on whistleblowers, creating a reluctance to come forward.²²⁰ The Inquiry made a number of recommendations including:

1. expanding the use of Public Interest Advocates to review warrants to be executed on journalists in relation to investigation of unauthorised disclosure of government information, including to make submissions on the public interest in facilitating exchange of information between journalists and members of the public (Rec 2);
2. annual reporting by the Attorney-General or the Minister of Home Affairs about the number of covert and overt warrants obtained in relation to journalists and media organisations, and the offences they relate to (Rec 5);
3. that the Attorney-General’s Department report in the context of its review on secrecy laws whether the relevant legislation adequately protects public interest journalism (Rec 6);
4. that the Government give consideration to whether defences for public interest journalism should be applied to other secrecy offences, referring to s 122.5(6) of the Criminal Code (Rec 7);
5. that the Government consider a mechanism to allow journalists to consult with the originating agency of national security information without threat of investigation or prosecution (Rec 8);
6. that the Government formally respond to the recommendations of the Review of the Public Interest Disclosure Act 2013: An independent statutory review conducted by Mr Philip Moss AM before completion of the Senate Environment and Communications References Committee’s inquiry into press freedom (Rec 9) (noting that this has now been done, as discussed above);

²¹⁸ Australian Law Reform Commission, *The Future of Law Reform: A Suggested Program of Work 2020-25* (Report, December 2019).

²¹⁹ AJ Brown et al (n 146)E-11.

²²⁰ *Law Enforcement and Intelligence Powers on the Freedom of the Press* (n 10) [2.80]-[2.81], [2.104].

7. that the Government provide for mandatory reporting of statistics on Public Interest Disclosures (Rec 11);
8. that the Inspector General of Intelligence and Security conduct a preliminary inquiry into the application of national security classifications in intelligence agencies and provide information to the public on the outcome of its inquiry (Rec 14); and
9. that the Government should review and prioritise promotion and training of a uniform FOI culture across departments (Rec 16).²²¹

In December 2020, the government responded to the PJCIS report. The government agreed to all of these recommendations.²²²

The Senate Committee on Environment and Communications handed down its report from the inquiry into press freedom on 19 May 2021. The Committee's recommendations included:²²³

1. the Attorney-General's department should examine how the public interest in a free press and open and accountable government can be better balanced with protecting classified and sensitive government information;
2. the Attorney-General's department, in its review of the secrecy provisions in Commonwealth law, should examine whether general secrecy offences should be amended to include an express harm requirement;
3. the government should develop guidance material to assist journalists to comply with secrecy provisions including the identification of classified information and special intelligence operations information;
4. the Attorney-General's department should examine the best way to amend s 35P of the *ASIO Act 1979* (Cth) to protect journalists who make public interest disclosures about special intelligence operations in good faith;
5. the government should consider amending the Code and other Commonwealth legislation to remove the evidential onus on journalists to establish that an unauthorised disclosure is in the public interest;
6. the Attorney-General's department should examine whether the national security legislation should require the prosecution to establish that a secrecy or unauthorised disclosure offence is not in the public interest;

²²¹ Ibid.

²²² Australian Government, *Australian Government Response to the Parliamentary Joint Committee on Intelligence and Security report: Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Report, December 2020).

²²³ Senate Standing Committee on Environment and Communications (n 177).

7. the government should expedite reforms to the PIDA to address deficiencies in protections for whistleblowers; and
8. the government should initiate an independent review of law-enforcement and national security laws to reduce duplication and inconsistency and align them with Australia's international human rights obligations including the right to freedom of expression.

2 Section 35P of the ASIO Act

Section 35P of the ASIO Act was introduced in 2014 and made it an offence to disclose information relating to a special intelligence operation.

In 2015, the former Independent National Security Legislation Monitor, Roger Gyles, carrying out a review of the operation of s 35P on journalists, concluded that a secrecy provision was not inappropriate.²²⁴ However, Gyles recommended that the provision be split into offences for 'insiders' and 'outsiders' (including journalists). Gyles also noted that the provision was arguably inconsistent with article 19 of the ICCPR and an express harm requirement should be inserted. These recommendations were followed.

The provision makes it an offence for an entrusted person to disclose information that comes into their knowledge or possession in that capacity, where the information relates to a special intelligence operation.

For 'outsiders' (including journalists), it is an offence to disclose information 'relating to' a special intelligence operation where the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation, and the person is reckless in relation to that effect. A higher penalty applies if the person intends to, or knows that, disclosure will endanger health or safety or prejudice the effective conduct of a special intelligence operation.

There are a number of problems with the provision from the perspective of media freedom and public interest. First, it is difficult for journalists to know what they may and may not report. Since 'special intelligence operations' are covert, it is not apparent when a person is reporting on a 'special intelligence operation' or what activities fall within that definition.

Secondly, and importantly, there is no public interest exemption to the offence provision. The defence for journalists in s 122.5(6) of the Code only applies to offences pursuant to that division. Therefore, a journalist could be prosecuted for reporting on misconduct by an ASIO

²²⁴ Roger Gyles, *Report on the Impact on Journalists of Section 35P of the ASIO Act* (Report, Oct 2015).

officer engaged in a special intelligence operation (for example that they have engaged in abuse of power or torture) on the basis that the reporting may prejudice the effective conduct of a special intelligence operation, even though there might well be strong public interest in that information being made public.²²⁵

In 2014, the Commonwealth Director of Public Prosecutions issued a national direction requiring prosecutors to seek the Director's approval to any prosecution under s 35P. The Attorney-General has also issued a direction requiring that their consent be obtained to the prosecution of a journalist for certain disclosure offences.²²⁶ However, these 'safeguards' are inherently discretionary and provide no comfort that those who disclose information in the public interest will not be prosecuted.²²⁷

3 *Speak no Evil: Observations*

The current regime of secrecy offences, together with the limitations of the PIDA, has a potentially chilling effect on whistleblowers and public interest journalism. It is not unreasonable that those who disclose or report matters of public interest give proper consideration to whether harm might result from their actions. However, free flow of information is at the heart of representative democracy. The more impediments there are to that free flow of information, the more likely that official misconduct and negligence will go unreported.

It is therefore important that those who report and disclose in the public interest have a reasonable measure of certainty as to whether or not their actions are illegal prior to publishing. It is also important that laws that exist to prohibit disclosures that are harmful to the public interest are properly tailored and only go so far as necessary in order to achieve that legitimate purpose.

A public interest test for the disclosure of all information is key to protecting that free flow of information. There should be no category of information that is 'off limits' simply by nature of its categorisation or classification. That leaves too much in the hands of bureaucrats and those who have a personal interest in limiting the flow of information.

Further, a mandated internal reporting scheme does not offer sufficient protection to a whistleblower who, if the results of that report are not adequate, must make the decision to identify themselves at the risk of punishment. For that reason, anonymous reporting avenues should be available to potential whistleblowers.

²²⁵ Kieran Hardy and George Williams, 'Special Intelligence Operations and Freedom of the Press' (2016) 41(3) *Alternative Law Journal* 160.

²²⁶ Parliamentary Joint Committee on Intelligence and Security (n 10) [2.36].

²²⁷ Danielle Ireland-Piper and Jonathan Crowe, 'Whistleblowing, National Security and the Constitutional Freedom of Political Communication' (2018) 46(3) *Federal Law Review* 321, 375.

In the context of journalism, there should be no category of information that, in and of itself, is exempt from being reported in the public interest. A public interest test should also apply to the reporting and publication of information to ensure that all information, regardless of its nature, is able to be reported in the public interest.

V A Right to Free Speech?

The problem is that there is a dynamic equilibrium of different forces within a nation, we can talk about globally as well, but within a nation there is a dynamic equilibrium of powers, so intelligence agencies, courts, media, banking, political forces, and so on. That dynamic equilibrium is what keeps bargaining power for individuals within society. Essentially it is what keeps society going completely to shit, because when one actor or allied power groups within a society start making life difficult for everyone, you can change your allegiance and change your support in another direction. What lubricates that whole system is information flow between people about what is happening within a society. We might call that investigative journalism or gossip or pricing information flowing throughout the economy, that is what keeps us aware of what is happening and whether our interests are being compromised and whether society is going to shit.²²⁸

Article 19(2) of the ICCPR provides that everyone shall have the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds. Article 19(3) of the ICCPR provides for such restrictions to be imposed on the freedom of expression as are necessary for the protection of national security or public order. This limitation was referred to in the Explanatory Memorandum to the Public Interest Disclosure Bill 2013.²²⁹

The US First Amendment protects free speech and freedom of the press from government encroachment. The US Supreme Court has never ruled on the application of the First Amendment to the *Espionage Act of 1917* ('Espionage Act'), although State courts have. Daniel Ellsberg, the first person to be charged with infringing the Espionage Act as a whistleblower, had the case against him dropped due to government misconduct. The issue was therefore not determined and has not been considered by the Supreme Court since.²³⁰ However, the Supreme Court did rule that the government carried a heavy burden in terms of justifying restraint of publication by the media, which had not been met in that case.²³¹

²²⁸ Scott Ludlum and Julian Assange, 'An Audience with Julian Assange' in Felicity Ruby and Peter Cronau (eds), *A Secret Australia: Revealed by the WikiLeaks Exposes* (Monash University Publishing, 2020).

²²⁹ Explanatory Memorandum, Public Interest Disclosure Bill 2013 6.

²³⁰ 'S7: Episode 35 – Daniel Ellsberg', *Unauthorized Disclosure* (Kevin Gosztoła, 27 September 2020).

²³¹ *New York Times Co v United States* (1971) 403 US 713.

The US First Amendment does not provide a blanket protection for speech in the form of disclosure of protected information. Chelsea Manning, in her military prosecution for unauthorised disclosure, sought to rely on the First Amendment to support an argument that the espionage provision she was charged with was overly broad and violated the First Amendment. The Military Court rejected that argument, referring to *United States v Morrison* 844 F.2d 1057, 1075 (4th Cir 1988), which upheld Espionage Act convictions of an intelligence employee who violated a non-disclosure agreement. The Military Court found that a soldier who wilfully communicated information relating to the national defence ‘is not entitled to invoke the First Amendment as a shield to immunise his (sic) act of thievery’.²³²

Australia does not have a federal Human Rights Act or Charter. However, the High Court has found that there is an implied freedom of communication in relation to political and government matters.²³³ The implied freedom is not a personal right of the kind that one might find in a human rights instrument. Rather, it operates as a fetter on the powers of the executive and the legislature.

The implied freedom has its textual basis in the phrase ‘directly chosen by the people’, which appears in ss 7 and 24 of the Constitution. In other words, it is vital to the public’s ability to choose who represents them in Parliament that there be freedom to discuss political matters. As Assange puts it, it is the information flow that ‘lubricates the whole system’.

Any burden on the implied freedom must be directed at a legitimate objective, and must be reasonably appropriate and adapted to that end.²³⁴ In *McCloy*,²³⁵ and refined subsequently in *Brown v Tasmania*,²³⁶ the ‘reasonably appropriate and adapted’ part of the test was reformulated to one of ‘structured proportionality’ involving the following questions:²³⁷

1. is the purpose of the law legitimate in the sense that it is compatible with the maintenance of the constitutionally

²³² *US v Manning* (2018) US Army Court of Criminal Appeals, 844 F.2d 1069-70 (Morrison).

²³³ *Nationwide News v Wills* (1992) 177 CLR 1; *Australian Capital Television v Commonwealth* (1992) 177 CLR 106; *Coleman v Power* (2004) 209 ALR 182; *Mulholland v Australian Electoral Commission* (2004) 209 ALR 582.

²³⁴ *Lange v Australian Broadcasting Corporation* (1997) 196 CLR 520; *Hogan v Hinch* (2011) 275 ALR 408 [50] (French CJ), [98]-[99] (Gummow, Hayne, Heydon, Crennan, Kiefel and Bell JJ).

²³⁵ *McCloy v New South Wales* [2015] HCA 34.

²³⁶ *Brown v Tasmania* (2017) 349 ALR 398 [278]. See also *Unions NSW v New South Wales* (2019) 363 ALR 1 [42], [110] and *Clubb v Edwards* (2019) 366 ALR 1 [5]-[6], [266], [462]-[463].

²³⁷ *Brown v Tasmania* (2017) 349 ALR 398 [104], [123]-[127] per Kiefel CJ, Bell and Keane JJ and [278], [280] per Justice Nettle; Shipra Chordia, ‘Proportionality and *McCloy v New South Wales*: Close but Not Quite?’, *Australian Public Law* (Blog Post, 2016); Shipra Chordia, ‘The Trajectory of Structured Proportionality in Implied Freedom of Political Communication Cases: *Brown v Tasmania*’, *Australian Public Law* (Blog Post, 2017).

prescribed system of representative and responsible government; and

2. if yes, is the law reasonably appropriate and adapted to advance that legitimate object in a manner that is compatible with the constitutionally prescribed system of representative and responsible government, which may be answered by reference to whether the law is suitable, necessary and adequate in its balance?

Griffiths has observed that differing approaches to the implied freedom have created uncertainty as to its application in particular cases.²³⁸ In particular, where a law targets political communication, as opposed to burdening it incidentally, a higher degree of scrutiny is involved.

In *Bennett v President, Human Rights and Equal Opportunity Commission*,²³⁹ the official secrecy provisions of the Public Service Regulations were successfully challenged on the basis that they infringed the implied freedom of political communication. The regulation provided that an employee of the Australian Public Service must not 'give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge'.

The regulation was found to be invalid on the basis that it was not reasonably and appropriately adapted to the legitimate purpose of protecting the efficient operation of government. It impaired that freedom in an unreasonable way because it impeded the flow of information that could only serve to enlarge the public's knowledge and understanding of the operation, practices and policies of executive government, without prejudicing the interests of the Commonwealth.²⁴⁰

At 255, Finn J said,

The vices of excessive secrecy in the conduct of government, its effect on the quality of public debate and, ultimately, on the practice of democracy itself, have more recently been both exposed and addressed ...

The progressive advent of Freedom of Information legislation has provided the principal governmental accommodation of the 'changing community standards' ... That sentiment is equally reflected in judicial responses to claims made to protect 'government secrets' from disclosure in legal proceedings ...

In *R v Goreng-Goreng*,²⁴¹ a public servant was charged with disclosing information obtained in the course of her employment. The charges were brought pursuant to regulation 2.1 of the *Public Service*

²³⁸ Leanne Griffiths, 'The Implied Freedom of Political Communication: The State of the Law Post Coleman and Mulholland' (2005) 12 *James Cook University Law Review* 93, 109.

²³⁹ *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119.

²⁴⁰ *Ibid* [98], [99].

²⁴¹ *R v Goreng-Goreng* (2008) 220 FLR 21.

Regulations 1999 (Cth). The provision prohibits an APS employee disclosing information obtained in connection with their employment if it was reasonably foreseeable that the disclosure could be prejudicial to the effective working of government. It further prohibits disclosing such information if it was to be communicated in confidence within the government or was received in confidence by the government.

An attempt to rely upon the implied freedom as was done in *Bennett's case* was unsuccessful. Refshauge J noted that while the starting point of the FOI legislation was that information was to be available unless a specific prohibition applied, that applied to documents and not to information, and his Honour also noted that FOI legislation is subject to extensive exemptions. He found that regulation 2.1 was much more limited and targeted than a catch-all provision, and was similar in scope to a South Australian provision that had been referred to with approval in *Bennett*.²⁴²

Ireland-Piper and Crowe have argued that the blanket criminalisation of unauthorised disclosure under (previous) s 70 of the Crimes Act, s 35P of the ASIO Act and s 42 of the Australian Border Force Act offend the implied freedom of communication in relation to political matters and should be read down. They argue that the absence of public interest exceptions in the ASIO Act or the Australian Border Force Act makes it unlikely that those provisions strike an adequate balance with the implied freedom.²⁴³

However, as *Bennett's case* and *Goreng-Goreng* illustrate, the protection offered by the implied freedom of political communication is limited. The provision upheld in *Goreng-Goreng* was of fairly general scope, and included prohibition of disclosure of any information received by the government in confidence, regardless of whether or not any harm would be caused to the government as a result. If such a provision is found valid, it is likely that other, similarly broad provisions will be.

The implied freedom, it must be kept in mind, is not a right, like a right contained in a human rights instrument. It is simply a fetter on legislative and executive power. If an anti-disclosure provision is directed at a legitimate purpose (which will include the efficient working of government or the protection of national security), and it meets the tests outlined above, then the provision will not be invalidated. It is therefore only prohibitions of very broad scope that will potentially be subject to a successful challenge.

This is particularly the case for provisions that expressly or in their effect prohibit disclosure of intelligence information. Given the broad scope of national security information, and the deference paid to official

²⁴² Ibid [18]-[38].

²⁴³ Ireland-Piper and Crowe (n 227) 362-3.

views on that score, it is more likely that broad-based prohibitions on disclosure will be found suitable, necessary and balanced for that purpose. If, as has been argued in support of such limitations, intelligence information is like a ‘mosaic’ and nobody can objectively discern the significance or need for secrecy in relation to that information, then a broad prohibition is more likely to be justified.

Given the unlikelihood of Australia’s adopting a Bill of Rights any time soon, it is therefore only through legislative change that there is likely to be comprehensive protection provided for whistleblowers.

Further, recent events have demonstrated that there is at least the potential for prosecution of journalists for publishing information as to government misconduct, although to date that has not occurred. In the United States, there has never been a prosecution of a journalist (not including the prosecution of Julian Assange who, as noted above, may or may not be considered a journalist). It is a matter for discussion in another forum how far the express protection provided to journalists in the US First Amendment is responsible for this, and how it will be applied in the Assange case.

VI Conclusion

It is important not to be blasé about the consequences of government secrecy on our society. Between 1952 and 1957, a series of nuclear bombs was exploded in Australia by the British. While the public knew that tests were being carried out, it was not until two decades later that information about the toxic impacts of the tests became known. Troops and civilians had been deliberately exposed to radiation with the possible impacts being kept secret.²⁴⁴

The preservation of rights to open and fair justice requires constant vigilance. This means continued scrutiny over government claims that information must be suppressed in the ‘public interest’. It is easy to rely too heavily on the ethereal notion that we live in a ‘free and democratic society’ and that the government will always act in the best interests of its people.

It is no riposte to concerns about Australia’s increasing secretisation that there is a freer flow of information here than in some other countries. Public access to information relevant to governance is key to the preservation of a true democracy. Furthermore, the overly broad application of secrecy imperils the very national security that it seeks to protect because it causes people to lose faith in the government’s authority to make decisions about what information should be kept out of the public domain. This can then become the catalyst for leaks of

²⁴⁴ Brian Toohey, ‘Menzies’ Gift’ in Brian Toohey, *Secret: The Making of Australia’s Security State* (Melbourne University Press, 2019).

information on a massive scale, as has occurred with Wikileaks and Chelsea Manning.

If Australia wishes to earn, and maintain, its reputation as a free democracy, eternal vigilance will be the price.