RISK AND UNCERTAINTY IN PUBLIC INTEREST JOURNALISM: THE IMPACT OF ESPIONAGE LAW ON PRESS FREEDOM

Rebecca Ananian-Welsh,* Sarah Kendall† and Richard Murray‡

This article draws together legal analysis and qualitative interviews with newsroom professionals to examine the impact of Australia's extensive suite of espionage offences on press freedom. This two-pronged analysis reveals that the espionage laws introduced in 2018 pose a significant risk of criminalising legitimate journalism and that this, in combination with their staggering complexity and uncertain scope, is contributing to the 'chilling' of public interest journalism in Australia. The article concludes with recommendations for law reform to protect national security without unduly encroaching on press freedom.

Contents

* Senior Lecturer, The University of Queensland School of Law.

† PhD Candidate, The University of Queensland School of Law.

‡ Research Fellow in Journalism, The University of Queensland School of Communication and Arts.

Cite as:
Ananian-Welsh, Kendall and Murray, 'Risk and Uncertainty in Public Interest Journalism: The Impact of Espionage Law on Press Freedom'
(2021) 44(3) *Melbourne University Law Review* (advance)

I Introduction

On 4 September 2019, outgoing Director General of the Australian Security Intelligence Organisation ('ASIO'), Duncan Lewis, described espionage and foreign interference as 'by far and away the most serious issue going forward' for Australia's national security.[1] Espionage, as defined by ASIO, concerns 'the theft of Australian information by someone either acting on behalf of a foreign power, or intending to provide information to a foreign power which is seeking advantage'.[2] This pre-eminent threat, Lewis said, outstripped even the threat of terrorism.[3] Only a year earlier, the federal government had overhauled Commonwealth espionage and foreign interference laws. This included the introduction of a complex suite of new espionage offences, justified on the basis that law enforcement and intelligence agencies 'lacked the legislative tools they

[1] Ben Doherty, 'Spy Chief Says Foreign Espionage and Interference an "Existential Threat" to Australia', *The Guardian* (online, 5 September 2019) <https://www.theguardian.com/australia-news/2019/sep/05/spy-chief-says-foreign-espionage-and-interference-an-existential-threat-to-australia>, archived at <https://perma.cc/6HHX-WKV8>.

[2] 'Counter Espionage and Foreign Interference', *Australian Security Intelligence Organisation* (Web Page) <https://www.asio.gov.au/counter-espionage.html>, archived at <https://perma.cc/ZRF4-SDY8>.

[3] Jade Macmillan, 'Foreign Interference More of "an Existential Threat" to Australia than Terrorism: ASIO Chief', *ABC News* (Web Page, 4 September 2019) <https://www.abc.net.au/news/2019-09-04/asio-chief-foreign-interference-more-of-a-threat-than-terrorism/11479796>, archived at <https://perma.cc/8X4Y-DP33>.

needed to act' in order to protect Australia's national security.[4] However, the reforms attracted criticism as being over-broad, highly complex, and posing a risk to fundamental freedoms and democratic principles.[5]

Mere hours before Lewis made these comments, Australian Federal Police ('AFP') officers had raided the Canberra home of former intelligence officer Cameron Gill on suspicion he had leaked classified documents to News Corp journalist Annika Smethurst.[6] Those documents included a top-secret departmental memo concerning a proposal to grant unprecedented domestic surveillance powers to the Australian Signals Directorate ('ASD').[7] Based on the leaked memo, Smethurst and *The Daily Telegraph* published a series of articles and, on 4 June 2019, the AFP had raided the journalist's home to search for evidence that would identify Smethurst's confidential source.[8] While Gill's alleged actions were not traditional espionage, it arguably had the same effect: the sharing of classified information with a journalist resulted in its dissemination to the

[4] Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13145 (Malcolm Turnbull, Prime Minister). For an overview and analysis of the history of Australia's counter-espionage laws, see Sarah Kendall, 'Australia's New Espionage Laws: Another Case of Hyper-Legislation and Over-Criminalisation' (2019) 38(1) *University of Queensland Law Journal* 125, 129–41.

[5] See, eg, Kendall (n 4); Alliance for Journalists' Freedom, *Press Freedom in Australia* (White Paper, May 2019); Law Council of Australia, Submission No 5 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018); Australian Lawyers for Human Rights, Submission No 7 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 6 [8.1]–[8.2]; Human Rights Watch, Submission No 10 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018); Whistleblowers Australia, Submission No 51 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (26 March 2018) 3–4; Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Human Rights Scrutiny Report* (Report No 3 of 2018, 27 March 2018) 246–54 [2.369]–[2.411].

[6] Max Koslowski and Kylar Loussikian, 'AFP Raids Home Owned by Defence Department Official', *The Sydney Morning Herald* (online, 4 September 2019) <https://www.smh.com.au/politics/federal/afp-raids-home-of-commonwealth-official-20190904-p52nv8.html>, archived at <https://perma.cc/CEH3-WA4V>.

[7] For the functions of the Australian Signals Directorate ('ASD'), see *Intelligence Services Act 2001* (Cth) s 7.

[8] The High Court later ruled the search warrant invalid and, accordingly, the search an unlawful trespass: *Smethurst v Commissioner of Police* (2020) 376 ALR 575 ('*Smethurst*'). For discussion, see generally Rebecca Ananian-Welsh, '*Smethurst v Commissioner of Police* and the Unlawful Seizure of Journalists' Private Information' (2020) 24(1) *Media and Arts Law Review* 60 ('Unlawful Seizure').

wider public, which includes foreign powers who might use that information to their advantage.

Within 24 hours of the Smethurst raid, the AFP executed a raid on the Sydney headquarters of the Australian Broadcasting Corporation ('ABC'), also seeking evidence relating to leaked classified documents and the publications that followed. Together, these raids drew global attention to the fragility of press freedom in Australia and, specifically, the impact of law enforcement and national security frameworks on Australian journalism.[9] The government initially expressed its support of the raids and left open the possibility of charges being laid against the journalists involved.[10] In the wake of Smethurst's successful High Court challenge to the raid, the AFP confirmed that it would not be laying charges against her. However, the AFP maintained that it would continue to pursue cases like Smethurst's because they involve a serious breach of national security.[11] More broadly, criticism of the raids prompted a series of ministerial directions to the AFP,[12] two parliamentary inquiries on the impact of law enforcement powers on press freedom,[13] a campaign led by an unlikely coalition

[9] See, eg, Damien Cave, 'Australia May Well Be the World's Most Secretive Democracy', *The New York Times* (online, 5 June 2019) <https://www.nytimes.com/2019/06/05/world/australia/journalist-raids.html>, archived at <https://perma.cc/86G9-HRE4>.

[10] Bevan Shields, '"Nobody Is above the Law": Journalists Committed a Crime, Says Peter Dutton', *The Sydney Morning Herald* (online, 12 July 2019) <https://www.smh.com.au/politics/federal/nobody-is-above-the-law-journalists-committed-a-crime-says-peter-dutton-20190712-p526il.html>, archived at <https://perma.cc/J5XU-8ANU>; Elizabeth Byrne and Matthew Doran, 'Charges against News Corp Journalist Annika Smethurst Still Possible after High Court Throws Out AFP Warrant', *ABC News* (Web Page, 17 April 2020) <https://www.abc.net.au/news/2020-04-15/annika-smethurst-wins-afp-fight-high-court/12147706>, archived at <https://perma.cc/K59X-NTEZ>; Jordan Hayne, 'AFP Will Not Lay Charges against Annika Smethurst over Publishing of Classified Intelligence Documents', *ABC News* (Web Page, 27 May 2020) <https://www.abc.net.au/news/2020-05-27/afp-will-not-lay-charges-annika-smethurst-raid/12291238>, archived at <https://perma.cc/647X-AQT9>.

[11] Ian McCartney, 'AFP Says They Will Continue to Pursue Cases like that of Annika Smethurst' (Press Conference, 27 May 2020) <https://www.abc.net.au/news/2020-05-27/afp-says-they-will-continue-to-pursue-cases-like/12292164?nw=0>, archived at <https://perma.cc/75HK-GK6H>.

[12] See, eg, Minister for Home Affairs, *Ministerial Direction to Australian Federal Police Commissioner Relating to Investigative Action Involving a Professional Journalist or News Media Organisation in the Context of an Unauthorised Disclosure of Material Made or Obtained by a Current or Former Commonwealth Officer* (8 August 2019); Brett Worthington, 'Attorney-General Orders Prosecutors Seek His Approval Before Charging ABC, News Corp Journalists', *ABC News* (Web Page, 30 September 2019) <https://www.abc.net.au/news/2019-09-30/attorney-general-grants-journalists-limited-protection/11560888>, archived at <https://perma.cc/NGG2-RWD2>.

[13] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of*

of Australian media organisations,[14] and legal challenges by both Smethurst and the ABC.[15]

Both press freedom and counter-espionage are critical to the health of Australian democracy. It is therefore imperative to design effective espionage laws that do not unnecessarily undermine press freedom. This article draws together legal analysis and qualitative interviews to examine the impact of the 2018 espionage laws on press freedom and provide recommendations for law reform to protect national security without unduly encroaching on press freedom. It reveals that current espionage offences pose a significant risk of criminalising legitimate journalism and that this, in combination with their staggering complexity and uncertain scope, is contributing to the 'chilling' of public interest journalism in Australia.

We begin, in Part II, by introducing the notion of press freedom and detailing the AFP raids and other examples of investigative reporting based on leaked material, which demonstrate the potential for public interest journalism and national security to intersect. Then, in Part III, we turn to the 2018 espionage offences. Part IV examines the real-world impact of the espionage laws on Australian journalism, drawing on semi-structured interviews with leading newsroom professionals from across Australian media organisations. The results of this empirical research frame the legal analysis, in Part V, which engages statutory interpretation to assess whether, and how, the provisions threaten legitimate journalism. This two-pronged, legal and empirical, approach reveals that journalists' concerns regarding the espionage laws are justified and, if anything, underestimate the threat to press freedom posed by the espionage offences. We conclude with recommendations for reform to protect national security without unduly undermining press freedom.

II Press Freedom

A *Principles and Protections*

The importance of a free and independent press in a liberal democracy cannot be overstated. As the United Nations Human Rights Committee recognised:

the Press (Report, 26 August 2020) ('*PJCIS Inquiry*'); Senate Standing Committees on Environment and Communications, Parliament of Australia, *Press Freedom Inquiry* (commenced 23 July 2019). At the time of writing the Senate Inquiry is yet to report.

[14] Matthew Doran, 'Media Unites to Rally for Press Freedom, Taking Campaign to Front Pages and Airwaves', *ABC News* (Web Page, 21 October 2019) <https://www.abc.net.au/news/2019-10-21/media-unites-to-rally-for-press-freedom/11621806>, archived at <https://perma.cc/T9JL-CMNY>.

[15] *Smethurst* (n 8); *Australian Broadcasting Corporation v Kane [No 2]* (2020) 377 ALR 711 ('*Kane*').

> A free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other [International Covenant on Civil and Political Rights ('ICCPR')] rights. It constitutes one of the cornerstones of a democratic society.[16]

Thus, a free and independent press is fundamental to the rule of law and plays a vital 'fourth estate' role in supporting government transparency and democratic accountability.[17]

Press freedom is, therefore, a broad and substantive notion. It encompasses the protection of journalists and media organisations in the conduct of their work, particularly in their capacity to facilitate government accountability, as well as the protection of journalistic sources and the public's right to know.

Press freedom is closely related to the human right to free expression. This right is protected under art 19 of the ICCPR and in human rights instruments the world over, including in the United Kingdom,[18] Canada,[19] New Zealand[20] and in Australia's three human rights Acts: the *Human Rights Act 2004* (ACT),[21] the *Charter of Human Rights and Responsibilities Act 2006* (Vic)[22] and the *Human Rights Act 2019* (Qld).[23] The United States ('US') Bill of Rights protects both freedom of speech and freedom of the press.[24]

However, neither freedom of expression nor a free press is granted express protection under the *Australian Constitution* or federal human rights legislation. The closest protection arises from the implied freedom of political communication derived from ss 7, 24, 64 and 128 of the *Constitution*, which limits the scope of legislative power to effect unjustified or disproportionate burdens on political communication.[25] Notably, the ABC invoked the implied freedom in its challenge to the AFP's June 2019 raid. Specifically, it claimed that the search warrant provisions in s 3E of the *Crimes Act 1914* (Cth) ('*Crimes Act*')

[16] Human Rights Committee, *General Comment No 34: Article 19 — Freedoms of Opinion and Expression*, UN Doc CCPR/C/GC/34 (12 September 2011) 3–4 [13] ('*General Comment No 34*').

[17] Tom Bingham, *The Rule of Law* (Penguin Books, 2011) 80–1.

[18] *Human Rights Act 1998* (UK) s 12.

[19] *Canada Act 1982* (UK) c 11, sch B pt I s 2(b) ('*Canadian Charter of Rights and Freedoms*').

[20] *New Zealand Bill of Rights Act 1990* (NZ) s 14.

[21] *Human Rights Act 2004* (ACT) s 16.

[22] *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 15.

[23] *Human Rights Act 2019* (Qld) s 21.

[24] *United States Constitution* amend I.

[25] See, eg, *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520 ('*Lange*'); *McCloy v New South Wales* (2015) 257 CLR 178.

effected a disproportionate burden on political communication. This argument, and the ABC's challenge to the raid, was unsuccessful.[26]

As the jurisprudence reflects, press freedom and free expression are of vital importance, but are by no means absolute. Under the *Constitution*, all that is needed to undermine political communication is a legitimate reason and proportionate restriction. Under international law, the right to free expression is broader and more robust. Nonetheless, art 19(3) of the ICCPR relevantly provides that freedom of expression may be subject to restrictions under law as necessary 'for the protection of national security or of public order (*ordre public*), or of public health or morals'. This does not convey a broad basis of exemption, and the United Nations Human Rights Committee observed that it would violate art 19 to invoke national security laws 'to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists … for having disseminated such information'.[27]

B *Leaks and Raids*

An understanding of press freedom and its potential intersection with national security is assisted by considering the AFP's June 2019 raids on Smethurst and the ABC. Over the course of seven hours on 4 June, AFP officers completed a thorough search of Smethurst's home, seeking information that might reveal the identity of one of her sources. The raids were prompted by stories published by *The Daily Telegraph* in April 2018 which discussed (and contained images of) a top-secret departmental memo. The memo concerned a proposal to expand the powers of the ASD beyond its existing mandate: namely, the collection of intelligence on foreign nationals, the provision of intelligence support to military operations, cyber warfare and information security. Smethurst reported

[26] *Kane* (n 15) 712–13 [3]–[4] (Abraham J). Smethurst also raised an implied freedom challenge to the AFP raid on her property; however, she challenged the validity of the offence under investigation rather than taking aim at the warrant provisions themselves. It was unnecessary for the High Court to address Smethurst's constitutional arguments, having established that the warrant failed to comply with s 3E of the *Crimes Act 1914* (Cth) ('*Crimes Act*') and was unlawful. For discussion, see Rebecca Ananian-Welsh and Joseph Orange, 'The Confidentiality of Journalists' Sources in Police Investigations: Privacy, Privilege and the Freedom of Political Communication' (2020) 94(10) *Australian Law Journal* 777.

[27] *General Comment No 34*, UN Doc CCPR/C/GC/34 (n 16) 7 [30].

that the proposed new powers could enable the ASD to secretly access Australians' digital information without a warrant, including financial transactions, health data and telecommunications records.[28]

The public interest in the story was clear: turning the ASD's extensive surveillance powers inward would have important implications for privacy and civil liberties in Australia. However, both the sharing of classified information with Smethurst and her publication of that information appeared to contravene s 79(3) of the *Crimes Act* — a provision which was subsequently repealed in December 2018 and replaced with a differently framed secrecy offence which, notably, contained a new journalism-based defence.[29] Section 79(3) was a 'highly open-textured provision'[30] which criminalised certain communications of 'prescribed documents, articles or information', defined to include defence secrets and documents obtained by a Commonwealth officer (owing to their position as such) that it was their duty to keep secret.[31]

Smethurst launched a High Court challenge to the raid and, in April 2020, the Court unanimously ruled that the warrant failed to adequately describe the offence to which it related.[32] The warrant was therefore invalid, and the unlawful search constituted a trespass.[33] Smethurst was, however, denied an equitable injunction compelling the return or destruction of the data seized by the AFP, leaving open the possibility that the unlawfully seized information could be used against Smethurst or her sources.[34]

On 5 June 2019, the AFP executed an eight-hour raid on the Sydney headquarters of the ABC. The ABC raid concerned a July 2017 report, 'The Afghan Files', by investigative journalists Dan Oakes and Sam Clark. The report expanded on allegations previously aired on the ABC's '7:30' program that members of the Australian Defence Force had been involved in the commission of

[28] Annika Smethurst, 'Spying Shock: Shades of Big Brother as Cyber-Security Vision Comes to Light', *The 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>, archived at <https://perma.cc/4Q5J-UC9A>.

[29] *Crimes Act* (n 26) s 79(3), repealed and replaced by *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) sch 2 pt 1.

[30] *Smethurst* (n 8) 631 [217] (Edelman J).

[31] *Crimes Act* (n 26) s 79(3) stipulated two exceptions, namely, when the communication was to an authorised person or to 'a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his or her duty to communicate it'.

[32] *Smethurst* (n 8) 587 [43] (Kiefel CJ, Bell and Keane JJ). Justice Edelman concluded, in similar terms: at 628 [204].

[33] Ibid 592 [67] (Kiefel CJ, Bell and Keane JJ), 604 [119] (Gageler J), 639 [246]–[247] (Edelman J).

[34] For discussion of this case, see Ananian-Welsh, 'Unlawful Seizure' (n 8) 67–8.

severe human rights violations in Afghanistan. The alleged violations included the mistaken targeting of unarmed civilians, the execution of an unarmed detainee, and the mutilation of the bodies of enemy combatants. The reports also examined how a 'code of silence' within the defence community enabled those responsible to escape prosecution.

Like Smethurst's article, 'The Afghan Files' declared itself to be based on leaked classified information, opening with the statement that

> Hundreds of pages of secret defence force documents leaked to the ABC give an unprecedented insight into the clandestine operations of Australia's elite special forces in Afghanistan, including incidents of troops killing unarmed men and children.[35]

Again, the public interest in the story was acute. Again, the contravention of Commonwealth secrecy offences seemed clear. Indeed, nine months before the raids, former Australian Army Major David McBride had been charged with a number of criminal offences over his role in leaking classified information to the ABC.[36] McBride had earlier brought his complaint to the attention of the Department of Defence and the AFP, after which he claimed his career 'went downhill' while the internal inquiry 'went nowhere'.[37] At the time of writing, McBride is awaiting trial for a number of offences, including unlawfully disclosing a Commonwealth document and information about Australia's defence capabilities,[38] and theft of Commonwealth property (being the classified material).[39] Shortly after McBride was charged, Oakes and Clark were informed that they were under investigation for criminal conduct related to the disclosure,[40] including unlawfully obtaining information regarding Australia's defence capabilities, receiving 'prescribed' information and receipt of stolen goods.[41]

[35] Dan Oakes and Sam Clark, 'The Afghan Files', *ABC News* (Web Page, 11 July 2017) <https://www.abc.net.au/news/2017-07-11/killings-of-unarmed-afghans-by-australian-special-forces/8466642?pfmredir=sm>, archived at <https://perma.cc/3GTT-K9T8>.

[36] *Kane* (n 15) 714 [11] (Abraham J); Rory Callinan, 'Military Lawyer on Theft Charge', *The Australian* (online, 1 March 2019) <https://www.theaustralian.com.au/nation/defence/military-lawyer-on-theft-charge/news-story/710b70ca6851fa9819434fcc780ea9d7>, archived at <https://perma.cc/8Z4G-BNRG>.

[37] Rod McGuirk, 'Australian Whistleblower to Represent Himself at Trial', *The Diplomat* (Web Page, 7 November 2019) <https://thediplomat.com/2019/11/australian-whistleblower-to-represent-himself-at-trial/>, archived at <https://perma.cc/TC3Z-N95W>.

[38] *Kane* (n 15) 714 [11]. See also *Crimes Act* (n 26) s 70(1); *Defence Act 1903* (Cth) s 73A(1).

[39] *Criminal Code Act 1995* (Cth) s 131.1 ('*Criminal Code*').

[40] 'Statement of Agreed Facts', *Australian Broadcasting Corporation v Kane [No 2]*, NSD989/2019, 24 September 2019, 488–9.

[41] *Defence Act 1903* (Cth) s 73A(2); *Crimes Act* (n 26) s 79(6); *Criminal Code* (n 39) s 131.2(1).

In the aftermath of the raids, Minister for Home Affairs Peter Dutton indicated that the journalists could face prosecution, declaring that 'if you've got top-secret documents and they've been leaked, it is an offence under the law' and '[n]obody is above the law'.[42] However, the primary targets appeared not to be the journalists, but their sources. At the time of writing, McBride remains the only person charged in relation to either the ASD or Afghan Files leaks or publications. However, as indicated by the AFP, investigations of this kind will continue where information continues to be leaked.[43]

Smethurst's ASD reporting and 'The Afghan Files' are but two examples of public interest reporting based on leaked material. A host of further examples exist to demonstrate the prevalence and role of such reporting in the Australian context.

In 2003, Andrew Wilkie, now an independent federal Member of Parliament, had been working for the Office of National Assessments ('ONA'), evaluating intelligence related to Iraq's weapons of mass destruction ('WMD'). Contrary to statements by Prime Minister John Howard, Wilkie could see no evidence of WMD in the reports he was handling. On this basis, Wilkie leaked his classified assessments to journalist Laurie Oakes.[44]

As recently as 2015, journalist Paul Farrell, then with *The Guardian*, published a map showing that an Australian Border Force ('ABF') customs ship, the *Ocean Protector*, had sailed into Indonesian waters to push back asylum seekers.[45] Subsequently, the immigration Secretary wrote to the AFP asking them to find the source of the leak and prosecute them under s 70 of the *Crimes Act*. Farrell later learned that the AFP had accessed his metadata in an (unsuccessful) attempt to identify his confidential source.

Farrell was also involved in 'The Nauru Files' — a 'cache of 2,000 leaked reports' detailing the examples of trauma and abuse inflicted on the asylum seekers held in the offshore detention centre. At the time, the offshore detention

[42] Shields (n 10).

[43] McCartney (n 11).

[44] Caroline Overington, 'In the Name of Truth', *The Age* (online, 22 July 2003) <https://www.theage.com.au/national/in-the-name-of-truth-20030722-gdw34i.html>, archived at <https://perma.cc/5Q4K-A95K>.

[45] Paul Farrell, 'Australian Ship Went Far Deeper into Indonesian Waters than Disclosed', *The Guardian* (online, 17 April 2014) <https://www.theguardian.com/world/2014/apr/17/australian-ship-went-far-deeper-into-indonesian-waters-than-disclosed>, archived at <https://perma.cc/5Q4K-A95K>.

centres were under ABF supervision, so conduct at the centres — and related documents — were treated as part of classified ABF operations.[46]

Leaked reports are not always targeted at government misconduct. In 2005, *The Australian* published the details of a secret report into security lapses at Sydney Airport. In this case, the report detailed how biker gangs had managed to get airside passes to move drugs and weapons. The author of the report, Allan Kessing, was convicted under s 70 of the *Crimes Act* for leaking the reports and given a four-year suspended sentence, even though the stories triggered a series of inquiries and a significant security upgrade. Kessing continues to deny the leak and maintain his innocence.[47]

Australia has long been considered a strong rule of law nation, with a thriving media built on a basic respect for free speech, accountability and independence from government. The 2019 AFP raids drew unprecedented attention to the fragile state of press freedom in Australia and the capacity for our staggering national security framework to undermine that freedom. News Corp described the Smethurst raid as 'a dangerous act of intimidation towards those committed to telling uncomfortable truths'[48] and *The New York Times* questioned whether Australia was 'the world's most secretive democracy'.[49] Prime Minister Scott Morrison was quick to distance his government from the AFP's actions, while Opposition Leader Anthony Albanese condemned the raids.[50] Parliamentary inquiries were convened to examine the impact of national security laws on

[46] Paul Farrell, Nick Evershed and Helen Davidson, 'The Nauru Files: Cache of 2,000 Leaked Reports Reveal Scale of Abuse of Children in Australian Offshore Detention', *The Guardian* (online, 10 August 2016) <https://www.theguardian.com/australia-news/2016/aug/10/the-nauru-files-2000-leaked-reports-reveal-scale-of-abuse-of-children-in-australian-offshore-detention>, archived at <https://perma.cc/K2E3-CWKX>.

[47] 'Whistleblower Allan Kessing "Vindicated" by Airport Customs Raid', *The Daily Telegraph* (online, 21 December 2012) <https://www.dailytelegraph.com.au/whistleblower-allan-kessing-vindicated-by-airport-customs-raid/news-story/c73d699e2cd944ca361aec1ad8286a91?sv=44fd12af33ed20d23338d18936eaa12d>, archived at <https://perma.cc/WWR5-H2GM>.

[48] See, eg, 'Australian Federal Police Raid News Corp Journalist Annika Smethurst's Home Over Alleged National Security Leak', *ABC News* (Web Page, 4 June 2019) <https://www.abc.net.au/news/2019-06-04/afp-raid-news-corp-journalist-annika-smethurst-home/11177052>, archived at <https://perma.cc/T7AY-BGKB>; The Associated Press, 'Police Raid Australian Public Broadcaster Over Afghan Leak', *NBC News* (Web Page, 6 June 2019) <https://www.nbcnews.com/news/all/police-raid-australian-public-broadcaster-over-afghan-leak-n1014071>, archived at <https://perma.cc/AUN8-93A5>.

[49] Cave (n 9).

[50] Rebecca Ananian-Welsh, 'Why the Raids on Australian Media Present a Clear Threat to Democracy', *The Conversation* (Web Page, 5 June 2019) <https://theconversation.com/why-the-raids-on-australian-media-present-a-clear-threat-to-democracy-118334>, archived at <https://perma.cc/Y9KY-KDA8>.

press freedom, one before the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') and the second before the Senate Standing Committees on Environment and Communications ('Senate Committee'). Dutton and Attorney-General Christian Porter issued a series of public directives to the AFP concerning how they should approach investigations concerning journalists and journalistic materials.[51] Before the PJCIS, however, representatives of the Department of Home Affairs insisted that law reform was unnecessary as the laws in place were 'appropriate'.[52] Nonetheless, in August 2020, the PJCIS recommended a wide range of reforms, capable of enhancing government openness and press freedom. This included a recommendation that the Attorney-General's Department specifically consider whether secrecy provisions in Commonwealth legislation adequately protect press freedom.[53]

Although the espionage laws were not invoked in the 2019 AFP raids, they had a prominent place in the debate that followed. A range of groups from the media and legal communities pointed to the espionage offences as a prime example of legislative overreach capable of undermining press freedom.[54] This focus was reflected in our interviews with newsroom professionals, discussed in Part IV. In the next Part we explain these complex laws, before assessing their impact on press freedom in the remainder of the article.

III The 2018 Espionage Offences

Over the course of three days in June 2018, the federal Parliament debated and enacted the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) ('*Espionage Act*').[55] This Act repealed Australia's four existing espionage offences and introduced seven new espionage offences into the *Criminal Code Act 1995* (Cth) ('*Criminal Code*'): five 'underlying' offences and two 'espionage-related' offences.[56] Each of these offences has varying

[51] Minister for Home Affairs (n 12); Worthington (n 12).

[52] See, eg, Department of Home Affairs, Submission No 32 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (August 2019) 7.

[53] Parliamentary Joint Committee on Intelligence and Security (n 13) xix [3.194].

[54] See, eg, Alliance for Journalists' Freedom (n 5) 8–9; Law Council of Australia, Submission No 40 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (7 August 2019).

[55] National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth).

[56] *National Security Legislation (Espionage and Foreign Interference) Act 2018* (Cth) sch 1 item 17 ('*Espionage Act*'), amending *Criminal Code* (n 39) div 91.

fault elements. The *Espionage Act* also introduced four aggravating circumstances which apply to selected espionage offences, creating, in total, a highly complex suite of 27 new espionage offences.[57] This Part summarises these offences and explains the core terms and criteria they rest upon.

A *Underlying Espionage Offences*

The 2018 suite of espionage offences rests on five, somewhat overlapping, criminalised acts. These are:

- Dealing with security classified or national security information to be communicated to a foreign principal ('Core Espionage Offence');[58]
- Dealing with information to be communicated to a foreign principal ('Communication Espionage');[59]
- Dealing with security classified information for the primary purpose of communicating it to a foreign principal ('Classified Information Espionage');[60]
- Dealing with information on behalf of, in collaboration with, or under the direction, funding or supervision of a foreign principal, reckless as to whether an espionage offence is being committed ('Espionage on Behalf of a Foreign Principal');[61]
- Theft of trade secrets involving a foreign government principal ('Trade Secrets Espionage').[62]

Each offence applies to conduct within and outside Australia,[63] except for Trade Secrets Espionage which only applies to conduct within Australia, or conduct that occurred outside Australia and the result occurred in Australia or the person was an Australian citizen or resident at the time the conduct occurred.[64] When the various fault elements of intention and recklessness, outlined below,

[57] There are varying approaches to calculating the number of new offences. The total of 27 (nine underlying offences, two espionage-related offences and 16 aggravated offences) is adopted in Kendall (n 4) 143–4. See also Department of Defence, 'National Security Legislation Amendment Act 2018: Espionage and Foreign Interference' (Summary of Offences, 2018).

[58] *Criminal Code* (n 39) s 91.1.

[59] Ibid s 91.2.

[60] Ibid s 91.3.

[61] Ibid s 91.8.

[62] Ibid div 92A.

[63] Ibid ss 15.4, 91.7, 91.10, 91.14.

[64] Ibid ss 15.2, 92A.2(1). However, note that ss 15.2(2) and 15.2(4) (defences for primary and ancillary offences) do not apply: at s 92A.2(2).

are applied, the scheme may be approached as creating a total of nine separate offences.[65]

1 *Key Terms*

The underlying espionage offences hinge on certain key terms, most prominently: *dealing* with *information or articles* on behalf of, or to communicate to, a *foreign principal*.

The term 'dealing with' is defined with exceptional breadth. 'Deal' includes receiving, obtaining, collecting, possessing, making a record, copying, altering, concealing, communicating, publishing or making available.[66] The final term, 'making available', is defined to mean placing the information or article somewhere to be accessed by another, giving it to an intermediary to give to a recipient, or describing how to obtain access to it or methods that are likely to facilitate access to it.[67] It would seem that even passive receipt and possession of the information or article may amount to 'dealing' for the purposes of the espionage offences.

The offences capture dealings with 'information' and 'articles'. These terms encompass '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',[68] as well as 'any thing, substance or material'.[69] Dealing with such information or articles encompasses dealing with all or part of it, or even dealing with the 'substance, effect or description' of it.[70] Naturally, these broad definitions are sufficient to capture the type of information that sources provide and journalists gather and publish. For simplicity, this article will use the word 'information' to refer to both information and articles as defined in the *Criminal Code*.

[65] These offences are:
1. Core Espionage Offence, intending to prejudice Australia's national security or advantage the national security of a foreign country;
2. Core Espionage Offence, reckless as to this prejudice or advantage;
3. Communication Espionage, intending to prejudice Australia's national security;
4. Communication Espionage, reckless as to this prejudice;
5. Classified Information Espionage;
6. Espionage of Behalf of a Foreign Principal, intending to prejudice Australia's national security or advantage the national security of a foreign country;
7. Espionage on Behalf of a Foreign Principal, reckless as to this prejudice or advantage;
8. Espionage on Behalf of a Foreign Principal, with no fault element as to prejudice or advantage; and
9. Trade Secrets Espionage.

[66] *Criminal Code* (n 39) s 90.1(1) (definition of 'deal').

[67] Ibid s 90.1(1) (definition of 'make available').

[68] Ibid s 90.1(1) (definition of 'information').

[69] Ibid s 90.1(1) (definition of 'article').

[70] Ibid s 90.1(2).

The crux of 'espionage' is that it involves a 'foreign principal'. 'Foreign principal' is defined to include a foreign government principal or political organisation, as well as any public international organisation or entity owned, directed or controlled by any of these foreign principals.[71] Terrorist organisations are also included in this definition, although such organisations may have no foreign element.[72] 'Foreign government principal' includes foreign governments (including local governments) and their authorities.[73] It also includes 'foreign public enterprises',[74] that is: companies where a foreign government holds more than 50% of its issued share capital, more than 50% of its voting power or can appoint more than 50% of its directors, where the directors are accustomed to act according with the wishes of the foreign government, or where the foreign government is in a position to exercise control over the company.[75] The company must also enjoy special legal rights or benefits because of the relationship of the company with the foreign government.[76]

To amount to espionage, a person's conduct must (or will) result in the relevant information being communicated to a foreign principal or a person acting on its behalf. It is not necessary that the person have in mind a particular foreign country or foreign principal.[77] It is conceivable that information placed in the public domain will effectively and intentionally have been communicated to a foreign principal — we return to this important point in Part V.[78]

2 *The Core Espionage Offence*

The Core Espionage Offence criminalises dealing with security classified or national security information to be communicated to a foreign principal. The identification of security classified information will be relatively straightforward: it refers to information with a classification of 'secret' or 'top-secret'.[79] Notably, the publications that prompted the raids on both Smethurst and the ABC

[71] Ibid s 90.2.

[72] Ibid ss 90.2(c), 102.1 (definition of 'terrorist organisation'). Division 102 creates a number of broadly framed terrorist organisation offences, which may overlap with the espionage offences (insofar as those offences involve providing information to a foreign principal which is a terrorist organisation). For example, providing support or resources to a terrorist organisation: at s 102.7.

[73] Ibid ss 90.3(a)–(d).

[74] Ibid ss 90.3(e)–(f).

[75] Ibid s 70.1 (definition of 'foreign public enterprise').

[76] Ibid.

[77] Ibid ss 91.1(4)–(5), 91.2(3), 91.3(2), 91.8(4)–(5), 91.11(2).

[78] See below Part V(A)(1).

[79] *Criminal Code* (n 39) s 90.5(1).

concerned classified information of this kind. 'National security information' is a vaguer notion.

'National security' in the espionage context is defined to encompass defence of the country, protection of its borders from serious threats, and protection of the country and its people from activities such as espionage, terrorism, foreign interference and conduct obstructing operations of the country's defence force.[80] National security further includes the 'carrying out of the country's responsibilities to any other country' and the country's 'political, military or economic relations with another country'.[81] This essentially draws Australia's international relations within the field of national security.

This definition of national security is as broad as that found in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ('*NSI Act*'), designed to prevent the disclosure of information likely to prejudice national security in court proceedings.[82] Under the *NSI Act*, national security includes Australia's defence, security, international relations and law enforcement interests.[83] 'International relations' under the *NSI Act* includes political, military and economic relations with foreign governments and international organisations.[84] In *Thomas v Mowbray* — a case concerning the constitutional validity of anti-terrorism control order legislation — Gummow and Crennan JJ queried whether in this provision 'the Parliament has sought to over-reach the bounds of the understanding of "national security"'.[85] The definition found in the espionage provisions risks the same criticism.

The scope of actions captured by the Core Espionage Offence is extremely broad, with legislative definitions operating to extend this reach beyond the

[80] Ibid ss 90.4(1)(a)–(c), 90.4(2).

[81] Ibid ss 90.4(1)(d)–(e).

[82] *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) s 3 ('*NSI Act*').

[83] Ibid s 8. Section 9 provides that 'security' has the same meaning as in s 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*') which defines 'security' as:

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from
  (i) espionage;
  (ii) sabotage;
  (iii) politically motivated violence;
  (iv) promotion of communal violence;
  (v) attacks on Australia's defence system or acts of foreign interference;
whether directed from, or committed within, Australia or not; and

(aa) the protection of Australia's territorial and border integrity from serious threats; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

[84] *NSI Act* (n 82) s 10.

[85] (2007) 233 CLR 307, 358 [124].

provisions' plain meaning. Dealing with information, even 'national security' information, is conduct many people, including journalists, would engage in on a daily basis, particularly as 'information' includes opinions and summaries. Therefore, the fault element of the offence is a crucial limiting feature.

In the case of the Core Espionage Offence, the information must be dealt with intending to either: prejudice Australia's national security, or advantage the national security of a foreign country.[86] 'Prejudice' has not been overtly defined, although 'embarrassment alone is not sufficient to prejudice Australia's national security'.[87] If such an intention is made out, this espionage offence attracts a prescribed penalty of life imprisonment. Alternatively, the person must be reckless as to this prejudice or advantage, attracting the lesser prescribed penalty of 25 years' imprisonment.[88] The broad definition of national security, outlined above, sets the scope of these fault elements.

3 *The Remaining Underlying Offences*

The remaining four underlying espionage offences are: Communication Espionage, Classified Information Espionage, Espionage on Behalf of a Foreign Principal, and Trade Secrets Espionage.

Communication Espionage resembles the Core Espionage Offence, but applies to all information, not just security classified or national security information. Communication Espionage merely requires that a person deals with information and that conduct 'results or will result in the information … being communicated or made available to a foreign principal or a person acting on behalf of a foreign principal'.[89] The fault element of this offence is limited to intention (or recklessness) that the conduct will prejudice Australia's national security; no mention is made of an intention to advantage the national security of a foreign country.

Conversely, Classified Information Espionage and Trade Secrets Espionage apply to a restricted scope of information. If a person deals with information that is security classified, for the primary purpose of communicating it to a foreign principal, and the person's conduct does (or will) result in the relevant in-

[86] *Criminal Code* (n 39) s 91.1(1)(c). Intention is defined in s 5.2 as follows:
(1) A person has intention with respect to conduct if he or she means to engage in that conduct.
(2) A person has intention with respect to a circumstance if he or she believes that it exists or will exist.
(3) A person has intention with respect to a result if he or she means to bring it about or is aware that it will occur in the ordinary course of events.

[87] Ibid s 90.1 (definition of 'prejudice').

[88] Ibid s 91.1(2).

[89] Ibid s 91.2.

formation being communicated to a foreign principal, they will have committed Classified Information Espionage.[90] There are no additional fault elements. Similarly, the theft of trade secrets involving a foreign government principal will amount to Trade Secrets Espionage, regardless of the person's motive or intent.[91] Each of these forms of espionage carries a significant prescribed penalty: 15 years' imprisonment for Trade Secrets Espionage, and 20 years' for Classified Information Espionage.

Espionage on Behalf of a Foreign Principal involves a closer relationship with the foreign principal and a more complex, tiered set of fault elements. At its core, this offence involves dealing with information on behalf of, in collaboration with, or under the direction, funding or supervision of a foreign principal.[92] In addition, the person must be reckless as to whether their conduct involves the commission of an espionage offence by themselves or by 'any other person'.[93] The presence of these elements alone will constitute an offence punishable by up to 15 years' imprisonment.[94] However, higher penalties apply if the person intends or is reckless as to their conduct either prejudicing Australia's national security or giving advantage to a foreign country's national security.[95]

B *Espionage-Related Offences*

Two 'espionage-related offences' exist.[96] Both apply even where an espionage offence has not yet been committed.[97] Section 91.11 makes it an offence to intentionally solicit or procure, or make it easier to solicit or procure, an espionage offence on behalf of, in collaboration with, or under the direction, funding or supervision of a foreign principal or person acting on its behalf.[98] This 'Solicitation Offence' carries a prescribed penalty of 15 years' imprisonment.[99]

The Solicitation Offence sits awkwardly alongside s 11.2 of the *Criminal Code* which criminalises, amongst other things, procurement of a criminal offence. The two provisions overlap significantly, both requiring an intention to

[90] Ibid s 91.3.

[91] Ibid s 92A.

[92] Ibid ss 91.8(1)(d), 91.8(2)(d), 91.8(3)(c).

[93] Ibid ss 91.8(1)(c), 91.8(2)(c), 91.8(3)(b).

[94] Ibid s 91.8(3).

[95] Ibid ss 91.8(1), 91.8(2).

[96] Ibid ss 91.11–91.12.

[97] Ibid ss 91.11(3)(a), 91.12(3)(a).

[98] Ibid s 91.11(1)(b).

[99] Ibid s 91.11(1).

procure (or solicit) the offence.[100] However, the provisions also differ: s 11.2 requires actual commission of the procured offence and actual procurement of the offence,[101] while this is not required for the Solicitation Offence. In contrast, the Solicitation Offence can be committed: even where an espionage offence is not committed; even if it is impossible for the target to commit an espionage offence; even if the person does not have in mind particular information or a particular dealing; and whether the person intends to solicit or procure single or multiple dealings.[102] The unique purpose of the Solicitation Offence therefore appears to be the criminalisation of solicitation where no offence is or may be committed. In this way, the Solicitation Offence extends notions of criminalised solicitation beyond the orthodox boundaries that apply to offences throughout the *Criminal Code*.

It is possible for the Solicitation Offence to be paired with the inchoate liability provisions. Part 2.4 of the *Criminal Code* contains a set of provisions which extend criminal responsibility by criminalising: attempt,[103] aiding, abetting, counselling or procuring the commission of an offence by another person,[104] the joint commission of an offence,[105] the commission of an offence 'by proxy',[106] incitement,[107] and conspiracy.[108] All of these offences, except for incitement, attract the same punishment as the primary offence. So, a person could be prosecuted for conspiracy or incitement to solicit an espionage offence, and face the same potential sentence as for the Solicitation Offence itself.[109] A person could even be charged with procuring the solicitation of espionage — a somewhat mind-boggling offence that would introduce a complex overlay of fault and physical elements. This coupling of inchoate liability with

[100] Ibid ss 11.2(3), 91.11(1)(b).

[101] Ibid s 11.2(2). However, a person can be found guilty of procuring the commission of an offence even if the other person has not been prosecuted or has not been found guilty: at s 11.2(5).

[102] Ibid ss 91.11(3)(b)–(d).

[103] Ibid s 11.1.

[104] Ibid s 11.2.

[105] Ibid s 11.2A.

[106] Ibid s 11.3.

[107] Ibid s 11.4.

[108] Ibid s 11.5.

[109] Although 'attempt' does not apply: ibid s 91.11(4).

the espionage-related offences greatly extends the scope of criminalised conduct — a trend that has attracted significant attention and controversy in the field of terrorism law.[110]

The second espionage-related offence criminalises conduct intentionally engaged in to prepare for or plan an espionage offence ('Preparatory Offence').[111] It also carries a prescribed penalty of 15 years' imprisonment.[112] This is the most far-reaching of the espionage offences and resembles the 'catch-all' preparatory terrorism offence over which many concerns have been raised.[113] Despite these concerns, the preparatory terrorism offence has supported a significant number of terrorism prosecutions, especially when coupled with the inchoate offence of conspiracy, to create the 'ludicrous'[114] offence of conspiracy to do an act in preparation for a terrorist act.[115]

Conspiracy requires two or more people to agree to commit an offence and at least one of the conspirators engages in overt conduct in pursuance of the agreement.[116] Where found guilty of conspiracy, the offender is liable to the same punishment prescribed for the substantive offence.[117] This inchoate offence therefore criminalises the very early stages of a possible criminal act where a crime has not been committed or even attempted, no evidence exists of a plan to commit a specific crime,[118] and the person may not have decided precisely what they intend to do.[119] A person found guilty of conspiracy to commit the Core Espionage Offence, for example, could face life imprisonment.

110 See, eg, Tamara Tulich, 'Prevention and Pre-Emption in Australia's Domestic Anti-Terrorism Legislation' (2012) 1(1) *International Journal for Crime and Justice* 52, 56–7.

111 *Criminal Code* (n 39) s 91.12(1).

112 Ibid.

113 See ibid s 101.6; Tulich (n 110) 60–1.

114 Bernadette McSherry, 'Terrorism Offences in the *Criminal Code*: Broadening the Boundaries of Australian Criminal Laws' (2004) 27(2) *University of New South Wales Law Journal* 354, 366.

115 Andrew Lynch, Nicola McGarrity and George Williams, *Inside Australia's Anti-Terrorism Laws and Trials* (NewSouth, 2015) 38–40. 'Attempt' does not apply to the espionage-related offences, though conspiracy does apply: *Criminal Code* (n 39) ss 91.11(4), 91.12(2).

116 *Criminal Code* (n 39) s 11.5(2).

117 Ibid s 11.5(1).

118 See Carmel O'Sullivan and Mark Lauchs, 'A Spoiled Mixture: The Excessive Favouring of Police Discretion over Clear Rules by Queensland's Consorting Laws' (2018) 42(2) *Criminal Law Journal* 108, 110; *R v Bayda [No 8]* [2019] NSWSC 24, [112] (Fagan J) ('*R v Bayda*').

119 Council of Australian Governments, *Council of Australian Governments Review of Counter-Terrorism Legislation* (Final Report, 1 March 2013) 12–13; Independent National Security Legislation Monitor, *Annual Report: 16 December 2011* (Report, 2012) 50, 58; Jude McCulloch, 'Human Rights and Terror Laws' [2015] (128) *Precedent* 26, 28–9; Lynch, McGarrity and Williams (n 115) 33. See, eg, *Lodhi v The Queen* (2006) 199 FLR 303, 318 [66] (Spigelman CJ); *R v Bayda* (n 118) [112].

However, the inclusion of the espionage-related offences means a person may also commit conspiracy to solicit, procure, prepare or plan an espionage offence, and face up to 15 years in prison. Therefore, it is not only dealings with sensitive material that risk prosecution, but *discussions* regarding *preparations* for a *potential* future dealing with sensitive material.

C *Aggravated Espionage Offences*

The *Espionage Act* further introduced four aggravating circumstances which apply to some of the underlying espionage offences. Where an offence is found to be aggravated, the prescribed penalty is increased either to life imprisonment from 25 years, or to 25 years' imprisonment from 20 years.[120] Aggravating circumstances are:

- Dealing with information from a foreign intelligence agency;
- Dealing with five or more security classified records;
- Altering a record to remove or conceal its security classification; and
- Holding an Australian Government security clearance allowing access to at least 'secret' security classified information, at the time the person dealt with the information.[121]

These four aggravations each apply to the Core Espionage Offence (when the fault element is recklessness), Communication Espionage and Classified Information Espionage.[122] They do not apply to Trade Secrets Espionage, Espionage on Behalf of a Foreign Principal or the espionage-related offences.

D *Defences to Espionage*

Three defences are included in the espionage provisions of the *Criminal Code*, although none apply to Trade Secrets Espionage.

First, espionage will be lawful when the person dealt with information: according to a Commonwealth law, according to an agreement to which the Commonwealth is a party allowing exchange of such information, or in their capacity as a public official.[123] This defence applies to all espionage offences (with the

[120] *Criminal Code* (n 39) s 91.6(1).

[121] Ibid.

[122] Ibid ss 91.1(2), 91.2(1), 91.3(1).

[123] Ibid s 91.4(1).

exception of Trade Secrets Espionage) and is the only valid defence with respect to the Solicitation and Preparatory Offences.[124]

The second defence arises where the information was already communicated to the public *with Commonwealth authority*.[125] It applies only to the Core Espionage Offence, Communication Espionage, Classified Information Espionage and Espionage on Behalf of a Foreign Principal.[126] The limited application of these first two defences means that if a person has committed Trade Secrets Espionage, they will not avoid criminal liability even if their conduct was authorised by a Commonwealth law.

The third defence of 'Prior Publication' applies to Classified Information Espionage, as well as to the Core Espionage Offence where the prosecution relies on the fault element of intention or recklessness as to giving advantage to the national security of a foreign country.[127] This defence may be particularly relevant to the media as it concerns information that has already been communicated to the public.[128] For the defence to be available, the person must not have been involved in the initial public dissemination of the information; nor did they make or obtain the information as a result of being a Commonwealth officer; nor, most broadly, could they believe their dealing with the information would prejudice Australia's national security.[129] The person must have reasonable grounds for this final belief, taking into account the nature, extent and place of prior publication.[130] While this defence is sufficiently broad to make it potentially useful in practice, it has limited application: the defence does not apply to Communication Espionage, nor to the Core Espionage Offence where the prosecution relies on the fault element of intention or recklessness as to prejudice to Australia's national security. This means that, for example, where information has already been disseminated to the public, a journalist who re-publishes that information with intention or recklessness as to prejudice to Australia's national security (in contravention of the Communication Espionage offence)[131] will not be afforded the protection of the Prior Publication defence.

Concerns arise over the scope and appropriateness of these defences, particularly regarding the adequacy of protections for investigative journalists,

[124] Ibid ss 91.4(1), 91.9, 91.13.

[125] Ibid s 91.4(2).

[126] Ibid ss 91.4(2), 91.9(2).

[127] Ibid s 91.4(3).

[128] Ibid s 91.4(3)(b).

[129] Ibid s 91.4(3).

[130] Ibid ss 91.4(3)(d)–(e).

[131] See our discussion in Part V(B) below of the application of Communication Espionage to journalists and sources.

their sources, and whistleblowers.[132] Specifically, there exists no defence for legitimate journalistic reporting.[133]

IV How Have Journalists Been Impacted by the 2018 Espionage Laws?

Over 2019, we interviewed 20 journalists and senior newsroom figures reporting in the public interest from across Australian news media including the ABC, News Corp, Nine Entertainment (formerly Fairfax), The Conversation, Seven, Ten and the Special Broadcasting Service ('SBS'). This was followed by a series of interviews with legal advisors to major media organisations, including in-house counsel, solicitors employed by law firms, and barristers. These interviews explored whether and how Australian national security law was impacting the day-to-day work of journalists. They also explored the role of lawyers and legal advice in navigating these impacts. Espionage laws were repeatedly identified as a core concern for journalists and editors, leading to a tangible chilling effect on public interest journalism. In this Part, we outline our approach and findings as to the real-world impacts of espionage laws on press freedom.

The methods used in gathering data from journalists and lawyers conformed to Silverman's principles of qualitative research.[134] Silverman's work positions qualitative research as a means of gathering small data sets in the service of deeply analysing phenomena in a certain time and place. Unlike quantitative studies, which often draw upon large data sets, studies like this make no claims to general or large-scale analysis.

Care was taken to ensure data collection and analysis was replicable across this study and further studies. The interviews were semi-structured and theme-based, forming part of a wider study examining the impacts of national security law on Australian journalism. The interviews were coded into categories, focusing on specific laws and more general concerns and impacts. While a range of themes were explored, four concerns arose regarding the 2018 espionage laws.

[132] See Australian Lawyers for Human Rights (n 5) 6 [8.1]–[8.2]; Whistleblowers Australia (n 5) 3–4; Human Rights Watch (n 5) 6–7; Parliamentary Joint Committee on Human Rights (n 5) 246–54 [2.369]–[2.411].

[133] See further discussion below in Part V(H).

[134] See generally David Silverman, *Qualitative Research* (SAGE Publications, 4th ed, 2016).

A *Contributing to a Broader Chilling Effect*

Throughout the interviews, apprehension around the potential for the *Espionage Act* to impact the practice of journalism emerged. It is important to note that these concerns were expressed in the context of a larger conversation around the multifaceted consequences of changes in laws and the media landscape, contributing to a broader 'chilling effect' on Australian journalism.[135]

At a general level, the interviews demonstrated that the chilling effect is real and journalists have been inhibited in their pursuit of public interest journalism by changing legal frameworks. Mark Maley, the Editorial Policy Director at the ABC, said:

> It's a real problem and I don't think there's any doubt that there's been stories which could have been told or should have been told which haven't been told because of a combination of the *ASIO Act*, the Espionage Bill and metadata laws. That's the chilling effect in practice. The chilling effect is a real thing … We have killed stories off because of these laws. We're not talking about trivial stories, we're talking about the important stories.

Two laws dominated the conversation around the chilling of journalism. The first was the system of mandatory data retention and metadata access implemented under the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth). Interviewees expressed concern over the impact that data retention laws would have on the safety and anonymity of sources. This, in turn, was attributed to a diminishing willingness on the part of many sources to come forward. The potential for data retention laws to threaten source confidentiality trumped journalists' concerns for any impacts on themselves.[136] The same was not true for the second law, the *Espionage Act*, which was perceived as threatening both journalists and their sources.

B *Journalism in a High-Risk Environment*

Interviewees said the *Espionage Act* had the potential to criminalise core aspects of legitimate public interest journalism. No specific provisions were identified,

[135] On this 'chilling effect', see, eg, Mark Pearson and Joseph M Fernandez, 'Surveillance and National Security "Hyper-Legislation": Calibrating Restraints on Rights with a Freedom of Expression Threshold' in Johan Lidberg and Denis Muller (eds), *In the Name of Security: Secrecy, Surveillance and Journalism* (Anthem Press, 2018) 51, 55.

[136] For discussion, see, eg, Madelaine Wall, 'Data Retention and Its Implications for Journalists and Their Sources: A Way Forward' (2018) 22(3) *Media and Arts Law Review* 315; Rebecca Ananian-Welsh, 'Journalistic Confidentiality in an Age of Data Surveillance' (2019) 41(2) *Australian Journalism Review* 225, 233.

and none of the interviewees expressed a sophisticated understanding of the 2018 offences. Rather, the laws were perceived as presenting a generalised but tangible threat to both sources and journalists. This threat-perception impacted interactions between journalists and their sources, as well as within media organisations. In relation to receiving sensitive information, one senior newsroom figure said:

> I think we're more cautious and I think this is leading to stories being changed and watered down, and, in some cases, killed off. There is legislation which is actually preventing stories — the [*Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*')] and last year's Espionage Bill. They make stories too risky to do because you're exposing people to criminal sanctions, whether your own journalists or whether your sources. I think you'll find that most experienced investigative journalists now will tell you that they've been contacted by sources in a way which has been insecure with stories and they've gone back to the source and said, 'Forget it, if we run this story on the basis of your information, you will be caught and you will, at the very least, lose your job and find yourself in jail'.

None of those interviewed admitted to having changed a story in reaction to the *Espionage Act*. However, almost all interviewees said they had been pressured by senior editorial staff, or had advised junior staff, to change the ways in which they exchanged information with sources or structured a story out of concern for their own safety. For the senior journalists interviewed, the prospect of exposing colleagues to criminal sanctions for what they viewed as everyday journalism was an unacceptable risk.

C *Uncertainty*

Adding to the insecurity felt by many of the interviewees was the nebulous and untested nature of the *Espionage Act*. The Act was at once perceived as threatening and uncertain. Across the interviews, there was an acceptance that any impacts on journalists were an unintended consequence of the Act, but this did not reassure interviewees. One said they could foresee a time when a less scrupulous and more draconian government than the present Morrison government could use the *Espionage Act* to target and jail journalists.

At issue was widespread uncertainty on how to interpret the *Espionage Act*. An unexpected contrast was made to s 35P of the *ASIO Act*, which had attracted consistent criticism for its impact on press freedom since its introduction in

2014.[137] This provision allows for the designation of certain law enforcement and intelligence operations as 'special intelligence operations' ('SIO'). The SIO designation was designed to allow ASIO officers to break the law in the course of their work, without risking prosecution. Anybody disclosing even the existence of an SIO could face up to five years in prison; 10 years if the disclosure was 'aggravated' (endangering the health or safety of any person, prejudicing an SIO, or if the person intended as much).[138] Not only is it illegal to say anything about an SIO, but the prohibition extends to 'related' information which could include operations by regular law enforcement agencies working to support ASIO.[139]

While the introduction of s 35P was seen as deeply obtrusive to the process of public interest journalism, the journalists interviewed regarded that provision as clear in its scope and, therefore, comparatively easy to accommodate in the day-to-day processes of doing public interest journalism. Once something had been designated an SIO, journalists knew to leave it alone. This was not true of the *Espionage Act*. In reckoning with the scope of conduct captured by the *Espionage Act*, journalists were responding to something uncertain, unseen and untested, but potentially ruinous for them and their sources.

D *Budget Implications: Training and Legal Fees*

Beyond anxieties around the unintended and unknown impacts of the *Espionage Act* were the structural impacts. The story of contemporary journalism is a story of doing more with less. The digital disruption of journalism has seen the once coveted rivers of advertising gold dry up. This has left Australia's newsrooms in a constant state of flux as they scramble to maintain relevance and fight for survival. At the same time, working conditions for journalists have been deteriorating, a situation exacerbated since 2001 by an increasingly fraught legal environment.

This rapidly evolving legal context has seen newsrooms devoting a bigger share of their resources to training, in what one interviewee described as a game of invisible cat and mouse in responding to legislative change. Several interviewees expressed concern over the cost of understanding the potential impacts of legislative change, as well as the cost to newsrooms of round after round of staff training. News Corp's Chris Merritt put it best, saying, '[a]t a time when our budgets have never been more stretched, spending money on this kind of

[137] See, eg, Keiran Hardy and George Williams, 'Special Intelligence Operations and Freedom of the Press' (2016) 41(3) *Alternative Law Journal* 160.

[138] Ibid 161.

[139] Ibid.

thing means a journalist's career could come to a premature end, or, worse, a news career in journalism might never begin'.

On top of this, senior newsroom figures identified the cost and quality of their legal advice as an issue. Larger organisations including the ABC, SBS, News Corp, Nine Entertainment, and most recently, The Guardian Australia, maintain in-house counsel. Matters that cannot be handled in-house go to external counsel, centred around three key firms. While the interviewees singled out their in-house counsel for high praise as essential parts of editorial processes, there was a concern on the part of editorial staff and legal counsel alike about their lack of expertise in national security laws. This lack of expertise also applied to external counsel, for whom (much like their in-house counterparts) the emphasis was on pre-publication and litigation advice, primarily regarding defamation and suppression orders. The uncertain and largely untested scope of national security law impacted the nature of legal advice in this field. In our interviews with in-house legal counsel, a senior journalist-turned-lawyer said, 'I don't see a problem in offering advice on matters of national security. My team is as bad at it as anybody else'.

E *Summary*

Across our interviews, the *Espionage Act* was consistently identified as one of the key contributors to a chilling effect on public interest journalism. Interviews were characterised by a perception that the Act criminalised core aspects of legitimate journalism and created a high-risk environment for both journalists and their sources. Yet discussions of the Act, even with legal counsel, were also characterised by uncertainty over the nature and scope of the espionage offences.

This combination of fear and risk-aversion has serious implications. First, these factors in combination could mean that journalists' fears are founded on a misunderstanding of the laws' actual scope. The perceived risks to journalists and their sources may be unjustified. Alternatively, media organisations may have overlooked important risks posed by the legislation. We test these concerns in Part V.

Second, fear and uncertainty lead to a chilling effect. Specifically, these factors were reported to: dissuade sources (including whistleblowers) from coming forward with potentially important material; prompt journalists to drop stories out of fear for their sources; and drive editors, legal counsel and journalists to advise against publications or interactions perceived as risking criminality. While interviewees expressed a fair, or even high, risk tolerance in the pur-

suit of public interest journalism, there was no tolerance for engaging in conduct that placed either journalists or sources at risk of criminal prosecution. In this way, the *Espionage Act* had the capacity for effecting a significant chilling effect on journalism even though other laws, such as defamation law, were encountered far more frequently.

Third, fear and uncertainty over the *Espionage Act* has practical implications by placing ongoing demands on already stretched training and legal budgets. Together, these three concerns undermine public interest journalism and democratic accountability by making journalists more reliant on government channels and less able, willing or safe to run counter-narratives on, especially, national security, international relations or law enforcement issues. What follows is a stifling of free speech and democratic accountability.

V Do the Offence Provisions Threaten Press Freedom?

In this Part, we critique each of the espionage offences for its potential to impact press freedom. In doing so, we focus on two key concerns raised by journalists, namely: the complexity and uncertain scope of the offences, and the capacity for the provisions to criminalise legitimate journalism. In all, statutory analysis reveals that interviewees' concerns were legitimate, justified and, if anything, a mild reflection of the offences' potential impact.

The espionage offences capture dealings with information and articles. Information gathering, synthesis and reporting is at the heart of journalism. By taking aim at dealings with information, almost every aspect of some journalists' work could be affected by the espionage laws, from research and interactions with sources, through to publication. The broad definitions attaching to 'deal', 'information' and 'article' mean that a journalist may satisfy the physical element for an espionage offence by merely receiving or possessing a description or summary of a document or interviewing a source regarding their personal opinions. Editorial, administrative and legal personnel would also be 'dealing' with information if they receive, possess, copy, summarise or make efforts to maintain the confidentiality of information.

Of course, merely dealing with information does not amount to espionage. Espionage may require the information to be of a certain kind and the dealing to have some relationship to a foreign principal. Further, some of the espionage offences require a fault element of intention or recklessness as to potential prejudice to Australia's national security or advantage to foreign security. While almost all the espionage offences have the potential to criminalise legitimate journalism, a few offences are of particular concern; these are: Communication Espionage, which applies to all information; Classified Information Espionage,

which has no fault element; the espionage-related offences, which criminalise conduct at its earliest stages; and, to a lesser extent, the Core Espionage Offence. First though, we explore how the key components of espionage apply in the media context by examining the Core Espionage Offence.

A *The Core Espionage Offence*

The Core Espionage Offence concerns dealings with national security or security classified information where this must (or will) result in the relevant information being communicated to a foreign principal or a person acting on its behalf, and the person intends to (or is reckless as to whether their conduct will) prejudice Australia's national security or advantage the national security of a foreign country. There is a real risk that journalists and sources will engage in conduct criminalised under this provision of the *Criminal Code*. This risk is heightened by the possibility that some media organisations may themselves qualify as foreign principals.

Security classified information is not often communicated to journalists, but it can be and when it is, it might disclose information of particular public interest. Smethurst's ASD stories, 'The Afghan Files' and Laurie Oakes' reporting on a lack of evidence of Iraqi WMD, for example, were based on security classified information and led to important investigative reporting widely considered to be in the public interest.

A more concerning aspect of the Core Espionage Offence is the broad scope of 'national security information'. As national security is defined to encompass Australia's political and economic international relations, journalists who report on these vast areas should be wary when undertaking research, interacting with sources, and generally preparing stories for publication. A considerable portion of media reporting concerns 'national security information', so defined, and this kind of public interest journalism is integral to maintaining governmental accountability and an informed populace. For example, information relating to Australia's negotiations with foreign countries regarding COVID-19 could qualify as national security information under the Act. Also, journalistic sources could be expected to 'deal' with national security information when liaising with journalists on a regular basis by, for example, discussing international affairs or global politics — especially as 'opinion' is included in the definition of information.

Whether such dealings with classified or national security information amount to espionage turns on only two things. First, whether the dealing does (or will) result in the relevant information being communicated to a foreign

principal. Second, whether the person has the requisite intention (or recklessness) as to the national security consequences of their conduct.

1 *Publication as Communication to a Foreign Principal*

The Core Espionage Offence requires that dealing with the information results or will result in the relevant information being communicated to a foreign principal, or a person acting on its behalf. This requirement is a central component of espionage and is easily satisfied in the media context where communication to a foreign principal may be achieved by open publication to the public at large.

This interpretation applies the plain meaning of the term 'communicate' and supports the purpose of the legislation, which is to ensure certain information is withheld from foreign powers. While preparing and publishing public interest stories does not resemble espionage as traditionally conceived, it would make little sense to criminalise a covert attempt to communicate a document to a foreign government, but not a public broadcast of the same document to all governments.

This conception of espionage aligns with case law and prosecutorial trends in the US.[140] Since at least 2009, the disclosure of confidential government information has been increasingly prosecuted as a violation of the *Espionage Act*.[141] Espionage prosecutions have concerned, for example, leaks to *The Baltimore Sun*, *The New York Times*, Fox News, and Associated Press, as well as freelance journalists and bloggers.[142] Perhaps the most notorious espionage prosecutions of the modern age have been against US Army Private Chelsea Manning and Julian Assange for their roles in the WikiLeaks affair; and against Edward Snowden for leaking troves of top-secret National Security Agency documents to journalists from *The Guardian*.

The groundwork was laid for these prosecutions in the 1985 case of *United States v Morison* ('*Morison*').[143] In *Morison*, the defendant was charged with espionage for sending classified information to the British magazine *Jane's Defense Weekly*. Morison drew on parliamentary materials and amicus briefs (submitted by members of the press) to argue that espionage law was concerned with the release of information to spies and saboteurs, not with 'leaks to the

[140] Analogues can also be found in prosecutions under the *Official Secrets Acts 1989* (UK): see Katherine Feuer, 'Protecting Government Secrets: A Comparison of the Espionage Act and the Official Secrets Act' (2015) 38(1) *Boston College International and Comparative Law Review* 91, 113–15.

[141] Feuer (n 140) 91. See generally 18 USC § 798 (2012).

[142] For discussion of each of these cases, see Feuer (n 140) 99–110.

[143] 604 F Supp 655, 657 (Young DJ) (D Md, 1985) ('*Morison*'). For discussion, see Charles D Ablard, 'Judicial Review of National Security Decisions: United States and United Kingdom' (1986) 27(4) *William and Mary Law Review* 753, 763–4.

press'. The Court rejected this argument, favouring the plain meaning of the provisions. Thus, as Charles Ablard summarised, 'the law concerning espionage should apply to anyone who uses a security clearance to obtain classified information to release it to the world'.[144] Despite being set against a backdrop of First Amendment rights to free speech and a free press, the US jurisprudence reflects a conception of espionage that encompasses publication *as* communication to foreign entities — a conception that aligns with the text and purpose of the Australian espionage offences. Not only does this understanding of espionage threaten journalistic sources, it also sees journalists and media organisations as key actors in espionage activities.

In addition to these concerns, it is arguable that whenever a journalist or media organisation deals with information, they do so with a view to potential publication; that is, with the intention to communicate it to foreign principals (as members of the public at large). Therefore, this requirement could be easily met by journalists, editors and arguably even sources; not only once information has been published, but also when steps are being taken with a view to publication.

The Core Espionage Offence could capture the handling — from receipt, to reading, summarisation, internal communication, editing, and eventual publication — of all information regarding Australia's international relations, for the purpose of public dissemination. This is exactly the kind of conduct many journalists engage in on a daily basis. For sources, it could be argued that by communicating information to a journalist, the source reflects an intention that the information (or some part of it) will be made public, and thereby communicated to foreign entities. On this interpretation of the provisions, much rests on the mental elements of the offence.

2 *Media Organisations as Foreign Principals*

The scope of 'foreign principal' impacts press freedom in a second, more complex, way: a number of media organisations may themselves qualify as foreign principals. In this case, a source communicating information to a journalist may constitute communication with a foreign principal. Similar concerns would arise with respect to freelance journalists and journalists who work for 'foreign principals' when they communicate information to editors and colleagues.

As outlined above, 'foreign principal' includes 'foreign government principal' which has been defined to include 'foreign public enterprises',[145] which are

[144] Ablard (n 143) 764, citing *Morison* (n 143) 659.

[145] *Criminal Code* (n 39) ss 90.2, 90.3(e).

effectively controlled by the state government and enjoy special legal rights or benefits.[146] 'Foreign public enterprises' may therefore include foreign-owned media that are controlled by the state's government and enjoy special legal status. This description arguably applies to news organisations such as China Central Television,[147] Al Jazeera,[148] Russia Today[149] and Pakistan Television Corporation.[150] The definition also extends to certain media organisations in Western liberal democracies with which Australians could be expected to share information without entertaining the notion that their conduct could amount to espionage. For example, Radio New Zealand,[151] Germany's Deutsche Welle,[152] France 24[153] and Voice of America[154] each might qualify as a foreign public enterprise. We do not argue here that these organisations are foreign principals, nor do we suggest that they are involved in espionage. Our core point is that the scope of the term 'foreign principal' could have unexpected (arguably absurd) results. This casts a shadow of risk and uncertainty over dealings with such media organisations, as described by interviewees.

3 *Intention and Recklessness as to National Security Consequences*

The key limitation to establishing the Core Espionage Offence is whether it can be shown that the person intends or is reckless as to whether their conduct will either prejudice Australia's national security or advantage the national security

[146] Ibid s 70.1 (definition of 'foreign public enterprise').

[147] 'China Profile: Media', *BBC News* (Web Page, 6 March 2018) <https://www.bbc.com/news/world-asia-pacific-13017881>, archived at <https://perma.cc/LZW3-H3YP>.

[148] 'Qatar Profile: Media', *BBC News* (Web Page, 25 February 2019) <https://www.bbc.com/news/world-middle-east-14702519>, archived at <https://perma.cc/5KLW-MGFU>.

[149] 'Russia Profile: Media', *BBC News* (Web Page, 7 January 2020) <https://www.bbc.com/news/world-europe-17840134>, archived at <https://perma.cc/7WDM-Q4VN>.

[150] 'Pakistan Profile: Media', *BBC News* (Web Page, 2 March 2017) <https://www.bbc.com/news/world-south-asia-12965785>, archived at <https://perma.cc/7Y98-4UYU>.

[151] 'About Radio New Zealand (RNZ)', *Radio New Zealand* (Web Page, 2020) <https://www.rnz.co.nz/about>, archived at <https://perma.cc/8XGX-6XD3>.

[152] 'Who Finances DW?', *Deutsche Welle*, (Web Page, 26 February 2019) <https://www.dw.com/en/who-finances-dw/a-36767785>, archived at <https://perma.cc/B6AF-W5LM>.

[153] 'France Profile: Media', *BBC News* (Web Page, 25 April 2017) <https://www.bbc.com/news/world-europe-17299010>, archived at <https://perma.cc/CRV7-9XYZ>.

[154] 'Mission and Values', *Voice of America* (Web Page, 2020) <https://www.insidevoa.com/p/5831.html>, archived at <https://perma.cc/AU79-ZX7R>.

of a foreign country. The high standard of proof required to show 'intention' may render this offence difficult to establish where a journalist and source have engaged in legitimate, good faith, public interest-based interactions. This will, however, depend on how 'prejudice' and 'advantage' are interpreted. 'Prejudice' is defined to mean more than mere embarrassment, although no further guidance is given as to what sort of conduct could be 'prejudicial'.[155] A journalist may publish a story with the intention to reveal systemic corruption or misconduct, for example, but the statutory definition of 'prejudice' makes it unclear whether this would amount to an intention to prejudice Australia's national security. 'The Afghan Files' made allegations of war crimes against Australian soldiers as well as efforts to 'cover up' the misconduct. The impact of this kind of hard-hitting reporting goes beyond mere embarrassment. Whether it 'prejudices' Australia's international relations is, however, unclear. Again, this uncertainty could prompt journalists to drop stories of this kind for fear that their intention to facilitate government accountability might amount to an intention to prejudice Australia's interests.

The second potential motivation is more abstract: an intention to advantage the national security of a foreign country. 'Advantage' has been defined so that 'conduct will not *advantage* the national security of a foreign country if it would advantage Australia's national security to an equivalent extent'.[156] However, this still means that conduct may be criminalised where it would benefit another country, including Australia's allies, but have a neutral effect on Australia; or where the advantage to Australia is not 'equivalent to' the advantage to another country.

Reporting around the alleged bugging of the Timor-Leste Cabinet by the Australian Secret Intelligence Service — leading to the prosecution of intelligence whistleblower Witness K and his security cleared legal counsel Bernard Collaery — could have amounted to the communication of national security information intended to advantage Timor-Leste or, relatedly, to prejudice Australia in future treaty negotiations. Wilkie's leaking of the ONA assessments revealing a lack of evidence of WMD in Iraq, and Farrell's decision to publish an ABF navigation map showing Australian ships inside Indonesian waters could likely 'advantage the national security' of foreign powers (at least, Iraq and Indonesia respectively). This reporting also constituted vitally important public interest journalism, symbolic of a free and independent press.

155 *Criminal Code* (n 39) s 90.1 (definition of 'prejudice').

156 Ibid s 90.1(1) (definition of 'advantage').

An intention to prejudice Australia or advantage a foreign country in international relations may be difficult to establish. However, 'recklessness' criminalises a person's conduct where they have a much lower level of personal culpability. A person will be reckless where they were aware of a substantial risk and it was unjustifiable for them to take that risk in the circumstances.[157]

To a degree, establishing 'recklessness' as to prejudice or advantage in this context will depend on the nature of the information. The formal classification of sensitive material indicates that its mere release could have harmful consequences.[158] In its submission to the *PJCIS Inquiry*, ASIO emphasised that the risks associated with revealing classified information 'would be very difficult — if not impossible — for the recipient of a national security classified document to identify'. 'Sophisticated adversaries such as foreign intelligence services,' ASIO argued, 'can learn far more from its content than might be evident to others, particularly taking into account mosaic analysis, where many seemingly disparate pieces of information are brought together to form a complete picture'.[159] This would suggest that the public dissemination of seemingly innocuous information carrying a formal security classification could itself demonstrate recklessness as to potential negative impacts on Australia's national security, or advantages to the national security of a foreign country. Similarly, the publication of highly sensitive information — for instance, concerning intelligence agencies (like the ASD) or military operations — could indicate recklessness as to the national security consequences.

For sources, the simple act of discussing classified or sensitive information with a *journalist* (especially if that information was obtained in the course of one's Commonwealth employment) could suggest recklessness as to prejudice to Australia or advantage to a foreign country. After all, journalists are in the business of making information available to the public and editors will make publication decisions based on a range of ethical, economic and other considerations beyond the source's control.

Conversely, the publication of innocuous non-classified information regarding Australia's international relations could be unlikely to demonstrate the

[157] Ibid s 5.4.

[158] Attorney-General's Department, *Protective Security Policy Framework: Sensitive and Security Classified Information* (Policy Document No 8, 2018) 7 [23]–[24].

[159] Australian Security Intelligence Organisation, Submission No 22.1 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (9 August 2019) 4 [26]–[27].

requisite intention or recklessness needed to prosecute the Core Espionage Offence. Yet it must be acknowledged that innocuous information plays a minimal role in public interest journalism or, relatedly, democratic accountability.

Between the extremes of highly sensitive and innocuous information lies a vast expanse of other forms of national security information. Whether a journalist has been reckless in publishing such information may then depend on how the news article has been written. An article might invite the reader to criticise or pass judgment on Australia, or expose corruption or misconduct by Australian officials, thereby risking prejudice to Australia's international relations. It is an even vaguer standard, and a far more complex thought process, to consider whether the publication of such information could advantage the national security of a foreign country; that is, any foreign country, including Australia's allies.

Against this backdrop it can be seen that any journalist investigating key events in international relations, such as Australian trade negotiations, risks being reckless with regard to possible prejudice or advantage to national security — especially if they uncover something that makes Australia look bad. The information must be more than merely embarrassing; however, it need not be as damning as covertly bugging the Timor-Leste Cabinet offices or the commission of war crimes by Australian soldiers. Reporting that Australians were using intimidation in negotiations with a small Pacific Island state could be reckless as to advantaging that state in the negotiations — it might even reflect an intent to prejudice Australia's interests. Similarly, reporting that a member of an Australian team negotiating a wheat trade deal has an undisclosed interest in a wheat export company could compromise those negotiations and harm 'national security'. It might also recklessly advantage the national security of another country. Considering the sensitivity attached to the entire defence and national security apparatus, investigative reporting into anything negative related to those areas could present a tangible risk of contravening an espionage offence.

4 *Summary: Scope and Uncertainty*

In all, the operation of the Core Espionage Offence requires journalists and sources to ask themselves three questions. First, am I dealing with information that is security classified or concerns national security (as broadly defined in the Act)? If yes, will doing so result in public dissemination (or otherwise communication to a 'foreign principal', including foreign government-controlled media organisations)? Finally, could my conduct prejudice Australia's national security or advantage the national security of a foreign country? If the answer to all three questions is 'yes', then there is a real risk of prosecution for the Core

Espionage Offence which attracts a sentence of imprisonment for up to 25 years (for recklessness) or life (for intention).

Legitimate public interest journalism regularly involves conduct satisfying the first two criteria. Much, therefore, rests on the third, fault, element. If investigative reporting that is critical of the Australian government qualifies as 'reckless' as to prejudice to Australia's national security or advantage to the national security of a foreign country, this could amount to espionage. The criminalisation of such reporting sounds a dire note for press freedom, effective journalism, and Australian democracy. Moreover, even the *chance* that such conduct could be criminalised creates a high-risk environment for journalists and their sources, which our interviews reveal leads to the dropping of stories and the chilling of speech and accountability.

B *Communication Espionage*

Communication Espionage is broader than the Core Espionage Offence as it applies to conduct that has resulted or will result in the communication of any kind of information to a foreign principal. It therefore has a greater capacity to impact the practice of journalism, resting entirely on whether the person intends or is reckless as to whether their conduct will prejudice Australia's national security. If communication to a foreign principal includes public dissemination, then this offence would effectively criminalise all media publications intended to prejudice Australia's international relations and national security; as well as those where the journalist (and potentially the source, editors and other media workers involved) were reckless as to any resulting prejudice to Australia's national security.

C *Classified Information Espionage*

Classified Information Espionage involves a dealing with security classified information which results (or will result) in the information being communicated to a foreign principal, and the conduct has the *primary* purpose of communicating it to a foreign principal. It is arguable that if a journalist or source's primary purpose in dealing with information is to communicate it to the public, this amounts to having the primary purpose of communication to a foreign principal. On the one hand, this conduct is a far cry from the covert spy tactics of traditional espionage; a court might distinguish the public at large from 'foreign principals' by reference to such considerations.[160] On the other hand, this

[160] For discussion of the shift from traditional espionage to modern espionage, see Kendall (n 4) pt II.

interpretation aligns with the purpose of the Classified Information Espionage offence, being to prevent security classified information from being obtained by foreign governments. Thus, the provisions might be interpreted to include foreign principals within the cohort of the general public. Without judicial consideration, it is uncertain whether a primary purpose of public dissemination would amount to also having a primary purpose of communication to a foreign principal. Therefore, journalists and sources should be cautious in all their dealings with security classified information for potential publication; this alone could amount to Classified Information Espionage and be punishable by up to 20 years' imprisonment.

Each of the publications that led to the AFP raids would meet these criteria. Smethurst's story was based on a top-secret classified document, a redacted version of which was printed with the story. The ABC's 'The Afghan Files' reporting was based on '[h]undreds of pages of secret defence force documents'.[161] By publishing (and maintaining) these summaries of security classified information in open access formats, the journalists and media organisations may well have committed Classified Information Espionage.

D *Espionage on Behalf of a Foreign Principal*

Espionage on Behalf of a Foreign Principal involves dealing with information on behalf of, in collaboration with, or where directed, funded or supervised by a foreign principal or person acting on its behalf, reckless as to whether the conduct involves commission of an espionage offence. Two forms of this offence also require establishment of a fault element regarding prejudice to Australia's national security or advantage to the national security of a foreign country (intention or recklessness), while a third does not. Naturally, it will be more difficult to prove intention, compared to recklessness or indeed no fault element. However, as described in relation to the Core Espionage Offence, there are circumstances in which both fault elements may be established in relation to the conduct of journalists and sources.

Central to these offences, and a key limiting factor, is the scope of the term 'foreign principal'. In the context of Espionage on Behalf of a Foreign Principal, 'foreign principal' does not refer to the recipient of the information, but whether the conduct has occurred *on behalf of* a foreign principal. If a journalist is working for a media organisation that may qualify as a foreign principal, it would seem that their dealings with information would be on behalf of, in collaboration with, or directed, funded or supervised by a foreign principal. This

[161] Oakes and Clark (n 35).

element may even apply to sources who provide information to such journalists, as 'collaborators' with foreign principals — particularly those sources who develop close working relationships with journalists over a number of years and, in this way, become integral to informed journalism and public interest reporting.

However, for Espionage on Behalf of a Foreign Principal to arise, it is also necessary that the person was reckless as to whether their conduct involved commission of an espionage offence. Similar to our discussion in relation to the Core Espionage Offence and its fault elements, establishing this particular fault element will largely depend on the type of information and how it is reported. There is no requirement that the information be national security or security classified information; though if the information was of this kind, it could suggest that the journalist or source was aware of a substantial risk of committing an espionage offence in dealing with or publishing the information. However, if the information was more mundane, such as reporting on the lifting of COVID-19 travel restrictions between Australia and another country, it is arguable that the journalist or source would not even consider that there was a risk they were committing an espionage offence, thus placing such conduct outside the scope of the Espionage on Behalf of a Foreign Principal offence, even if the journalist or source works for a 'foreign principal'. Therefore, journalists and/or sources who work for, or have been paid by, foreign government-controlled media are especially vulnerable to being captured by these offences, where the information they deal with is security classified or highly sensitive.

E *Trade Secrets Espionage*

Trade Secrets Espionage also requires that the person's conduct be engaged in on behalf of, in collaboration with, or under the direction, funding or supervision of a foreign principal.[162] In the context of press freedom, this means the person must work for, or have been paid by, foreign government-controlled media. Additionally, the person must dishonestly receive, obtain, take, copy, duplicate, sell, buy or disclose trade secrets information.[163] There is no fault element associated with this offence.

Trade Secrets Espionage focuses on trade secrets (instead of national security or security classified information) and aims to prevent such information from being acquired by foreign entities. While this is the strictest of the offences, both in scope and the absence of available defences, it is less likely to fall

[162] *Criminal Code* (n 39) s 92A.1(1)(c).

[163] Ibid s 92A.1(1)(a).

within the kind of information generally handled in public interest journalism. Therefore, the offence does not pose as great a risk to legitimate journalism.

F *Espionage-Related Offences*

The Solicitation and Preparatory Offences pose particular threats to press freedom, especially in light of the inchoate liability provisions of the *Criminal Code*. The Solicitation Offence requires that a person intentionally solicit or procure an espionage offence on behalf of, in collaboration with, or where directed, funded or supervised by a foreign principal (or person acting on behalf of a foreign principal).[164] As with Espionage on Behalf of a Foreign Principal and Trade Secrets Espionage, this offence will only present issues for journalists and sources working for, or being paid by, media organisations that qualify as foreign principals; those engaged in legitimate, good faith journalism for other media organisations need not be concerned.

While the Solicitation Offence appears to condemn the conduct of the foreign principal, it equally applies to, for example, senior journalists who instruct junior journalists to investigate a story, or any journalist who requests information from a source. However, the offence requires an 'intention' to solicit or procure an espionage offence. Intention may be difficult to prove where the journalist was working in good faith and could turn on the nature of the information. If a journalist works for a foreign government-controlled media organisation and intentionally solicits security classified or highly sensitive material from a government source, the Solicitation Offence may be engaged.

Unlike procurement under s 11.2 of the *Criminal Code*, the Solicitation Offence criminalises conduct where no offence has been (or may ever be) committed. Moreover, the interaction between the Solicitation Offence and the inchoate liability provisions opens up the possibility that a person could be prosecuted for conspiracy or incitement to solicit an espionage offence, or even the procurement of the solicitation of an espionage offence. This heightens the complexity and uncertainty inherent in these provisions. For journalists, this criminalises conduct at the earliest stages of investigative reporting — even before a story has been *identified*, let alone pursued. However, it is far from clear what exact conduct could be captured by the Solicitation Offence (especially when coupled with inchoate liability). Following up a lead on a story regarding classified information would appear to contravene the offence provisions, but what about discussing the potential story with an editor or senior journalist? Or gathering information from a source in order to decide whether publication

[164] Ibid s 91.11(1)(c).

is a safe or appropriate possibility? The uncertainty and risk for investigative journalists is palpable and presents a strong deterrent for journalists to even begin to pursue stories based on sensitive information.

The Preparatory Offence criminalises preparing for or planning an espionage offence. This pre-espionage offence could capture the conduct of people who have not yet committed, and may never commit, an espionage offence. The breadth of this offence means that it will be easier to prove than one of the underlying espionage offences, and could capture a journalist's conduct *before* they even begin interacting with sources or colleagues in respect of a possible story. The offence may be engaged where a journalist considers writing a story on Australia's international relations and begins to compile a list of possible sources or conducts preliminary research. Preparing to follow a lead on misconduct by Australian officials in treaty negotiations, overseas military or intelligence operations, or diplomatic relations could conceivably qualify as preparing for espionage, as could researching security cleared personnel who may have access to information that could corroborate a story on, for instance, misconduct in an intelligence operation. Thus, the offence is capable of criminalising a journalist's conduct even where they have not yet accessed information, let alone published it.

The Preparatory Offence also attracts inchoate liability.[165] In the terrorism context, the coupling of conspiracy with the preparatory offence has been regularly harnessed in prosecutions and led to lengthy prison sentences for those convicted. Conspiracy criminalises an even broader range of conduct that most would not consider to be criminal, at the point of merely talking to another person. When preparatory terrorism offences were enacted, concerns were raised regarding their capacity to 'criminalise "talk" or, arguably, even "thought"'.[166] Conspiracy to prepare for espionage may therefore arise where a source contacts a journalist and indicates that they may have information that could pertain to, for example, Australia's defence force or international relations. These two offences — which might be conceived as pre-espionage and pre-pre-espionage — have a disturbing potential to criminalise the daily conduct of journalists and their sources, regardless of whether such conduct is actually likely to harm Australia's national interests. It also sounds a chilling note for sources who are at the earliest stages of considering whether to, like Wilkie and McBride, reveal important information to the media in the public interest.

[165] Except for 'attempt': ibid s 91.12(2).

[166] Lynch, McGarrity and Williams (n 115) 39.

The criminalisation of this conduct by journalists and sources will have a serious chilling effect on public interest journalism, with uncertain national security benefits.

G *Aggravations*

The four aggravations operate to increase the applicable penalties where the person's conduct involves information from a foreign intelligence agency, five or more security classified records, altering a record to remove or conceal its security classification, or where the person held secret or top-secret security clearance at the time they dealt with the relevant information. These aggravations only apply to the Core Espionage Offence (where the fault element is recklessness), Communication Espionage and Classified Information Espionage.

Both journalists and sources are vulnerable to the operation of these aggravations. Journalists may deal with information from foreign intelligence agencies or with numerous security classified records, depending on the nature of the story. Indeed, 'The Afghan Files' was based on 'hundreds' of classified documents. Of core concern to journalists is the increased risk these aggravations pose to their sources. Where a source holds an Australian Government security clearance allowing access to at least secret security classified information when they dealt with the information, this alone would present an aggravating circumstance. Thus, the espionage offences are likely to have a particular chilling effect on security cleared sources speaking to journalists. Notably these sources are likely to be sophisticated actors, experienced in working with sensitive information and, potentially, capable of liaising with journalists in a fruitful, appropriate way. This aggravation is especially concerning because it is not necessary that the information dealt with was actually security classified: it may have been information that is not traditionally considered to be the subject of espionage, such as opinions on international relations, but which nevertheless falls within the broad definition of 'national security' which applies in the espionage context.

H *Defences*

Only three defences exist in relation to the espionage offences, excluding Trade Secrets Espionage. The first applies to information dealt with under Commonwealth law, a Commonwealth agreement, or in the person's capacity as a public

official.[167] This defence is likely to be more useful to sources, particularly government sources, than journalists per se. The second defence arises where the information was already communicated to the public with Commonwealth authority.[168]

The third defence, Prior Publication, concerns information that has already been made available to the public. It applies only to the Core Espionage Offence where the alleged fault element is intention or recklessness as to advantaging the national security of a foreign country, as well as Classified Information Espionage,[169] and it is not available to those who obtained the information as a result of being a Commonwealth Officer.[170] This defence could assist journalists who are effectively republishing information already publicly available, though only where they were not involved in the initial publication, and they lacked reasonable grounds to believe their dealing with the information would prejudice Australia's national security, taking into account the nature, extent and place of prior publication.[171] If information was published by one news organisation, it would be arguable that the subsequent dissemination of the same information by a second organisation could not reasonably cause prejudice to Australian security. However, if information was leaked accidentally or innocuously (for example, in a Facebook post that was deleted and not widely read), the publication of that information as national or global news could foreseeably prejudice Australian interests.

A glaring omission in the 'espionage package' is the availability of a specific defence for journalistic reporting. This is inconsistent with the secrecy offences, also introduced in 2018.[172] These offences are similar to the espionage offences but have no relationship to foreign principals. For example, the offence of 'communicating and dealing with information by non-Commonwealth officers etc' ('General Secrecy Offence') criminalises the intentional 'communication' or 'dealing' with information made or obtained by a current or former Commonwealth officer by reason of their position as such,[173] when the person is reckless

167 *Criminal Code* (n 39) ss 91.4(1), 91.9(1), 91.13.

168 Ibid ss 91.4(2), 91.9(2). This defence applies only to the Core Espionage Offence, Communication Espionage, Classified Information Espionage and Espionage on Behalf of a Foreign Principal.

169 Ibid s 91.4(3).

170 Ibid s 91.4(3)(a).

171 Ibid s 91.4(3).

172 See ibid s 122.5(6).

173 Ibid ss 122.4A(1)(a), 122.4A(1)(c), 122.4A(2)(a), 122.4A(2)(c).

as to whether the information has a security classification of secret or top-secret,[174] or whether the communication or dealing: damages the security or defence of Australia,[175] interferes with or prejudices the application of a Commonwealth criminal offence,[176] or harms or prejudices public health or safety of the Australian public.[177] This broadly-framed offence overlaps with the espionage offences but omits any reference to a foreign principal. It also carries a far lighter penalty than the espionage offences: imprisonment for up to five years for communication[178] and two years for dealing.[179]

In response to serious concerns raised about the potential for the General Secrecy Offence to impact press freedom, the provisions include a specific defence for 'News Reporting'.[180] For that defence to apply, the person must have dealt with the information in their capacity as a 'person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media'.[181] At the time, they must have reasonably believed that engaging in the conduct was in the public interest. Alternatively, they must have been an administrative staff member of an entity engaged in the business of reporting news and acted under the direction of a journalist, editor or lawyer who reasonably believed the conduct was in the public interest.[182] A person will not have reasonably believed that dealing with the information was in the public interest if the conduct was for the purpose of directly or indirectly assisting a foreign intelligence agency or military organisation (a notably narrower scope of conduct and entities than captured by the espionage offences).[183] This defence is particularly advantageous as it covers the 'business of reporting news' generally, which means both professional and non-professional journalists can utilise the defence.[184]

174 Ibid ss 122.4A(1)(d)(i), 122.4A(2)(d)(i).

175 Ibid ss 122.4A(1)(d)(ii), 122.4A(2)(d)(ii).

176 Ibid ss 122.4A(1)(d)(iii), 122.4A(2)(d)(iii).

177 Ibid ss 122.4A(1)(d)(iv), 122.4A(2)(d)(iv).

178 Ibid s 122.4A(1).

179 Ibid s 122.4A(2).

180 Ibid s 122.5(6).

181 Ibid.

182 Ibid s 122.5(6)(b).

183 Ibid s 122.5(7)(d).

184 Some legislated definitions concerning journalism and news reporting exclude non-professional journalists from their scope: see, eg, the definition of journalist in the private sector whistleblower protection provisions under s 1317AAD(3) of the *Corporations Act 2001* (Cth), and the definition of a journalist's 'source' (relevant to the operation of Journalist Information Warrants) under s 5(1) of the *Telecommunications (Interception and Access) Act 1979* (Cth).

From the practical perspective of newsroom professionals, effectively the same conduct is capable of being captured by the General Secrecy Offence and some of the espionage offences. For instance, publishing security classified information obtained from a Department of Defence whistleblower would likely contravene the General Secrecy Offence and amount to Classified Information Espionage. The press freedom concerns are equally present for secrecy and espionage offences, so it is unclear and arguably inconsistent to include a News Reporting defence to the secrecy offences but not to the espionage offences.

The legitimacy of these concerns was recognised by the PJCIS in its 2020 *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press*. In Recommendation 7, the PJCIS urged the Government to consider including defences for public interest journalism — based on the News Reporting defence to the General Secrecy Offence — to other secrecy offences, such as those involving espionage.[185]

I *Summary*

Our interviews with journalists revealed two key concerns regarding the 2018 espionage offences, which contributed to a tangible chilling of Australian journalism. First, their complexity and uncertain scope and, second, their potential to criminalise legitimate journalism. Our analysis of the espionage offences confirms that these concerns are legitimate and justified.

Many elements of the espionage offences encompass the conduct of journalists and sources who are engaged in public interest journalism. Many newsroom professionals regularly obtain, discuss, investigate, share, summarise and publish information relating to Australia's national security and international relations. Relationships, sometimes close ones, with government sources who have access to sensitive material are a core component of an effective free media.

The impacts of the Core Espionage Offence, Communication Espionage, Espionage on Behalf of a Foreign Principal and the Solicitation Offence are all primarily constrained by the requisite fault element. Whether or not it can be shown that the person had the relevant intention, or was reckless, will in part depend on the nature of the information dealt with or the substance of the news article written. Where, for example, the information is formally classified or sensitive, or the article invites readers to criticise Australia, the person might be shown to have acted recklessly. This attaches a tangible risk of criminal prose-

[185] Parliamentary Joint Committee on Intelligence and Security (n 13) 100 [3.198].

cution to entire fields of reporting — such as defence and trade. Where the information does not have the capacity to prejudice Australia's international relations, conduct may yet amount to a contravention of the Core Espionage Offence or Espionage on Behalf of a Foreign Principal if the person intends or is reckless as to potential advantage to the international relations of foreign countries. The public interest served by investigative journalism — of the kind undertaken by Smethurst, Oakes and Clark, for example — does not feature in determining whether an espionage offence has been committed. Disturbingly, the defining factor of traditional espionage — that is, a relationship with a foreign principal — is circumvented because publication in news media effectively amounts to communication to such entities.

In addition to the limitations imposed because of the fault element, Espionage on Behalf of a Foreign Principal and the Solicitation Offence are also limited by the requirement that the conduct be engaged in on behalf of a foreign principal. This means that the journalist or source must be working for, or paid by, a foreign government-controlled media organisation. It may be difficult to determine which media organisations qualify as foreign principals, and whether certain sources or other individuals qualify as collaborators. The unexpected scope of the provisions in capturing such organisations compounds the uncertainty and risk for journalists trying to work within the bounds of the law.

Two offences pose a particularly serious risk to legitimate public interest journalism. First, Classified Information Espionage has no fault element and may criminalise dealings with information for the primary purpose of publication. The offence is only limited by the requirement that the information have a security classification. As the ASD, 'The Afghan Files', and Iraqi WMD reporting showed, classified documents can, and do, inform important public interest journalism. Such reports are also capable of enhancing accountability, integrity and, ultimately, legitimacy and the rule of law.

Second, the Preparatory Offence is of staggering and uncertain breadth, and may be extended further by attaching inchoate liability in the form of, for instance, conspiracy. These provisions effectively criminalise the conduct of journalists and sources far before an espionage offence is committed, extending to mere conversations or research which might be a prelude to nothing more than ruling a story out on ethical or public interest grounds. Our interviewees were correct in treating public interest stories and sensitive information with extreme caution: there is a very real risk that those involved in preparing and publishing such stories could be exposed to criminal sanctions. However, even

concerned journalists may not have fully appreciated how early in their investigations their conduct could constitute espionage, or the possibility (or consequences) of media organisations being foreign principals.

VI Conclusions and Recommendations

The introduction of a new scheme of espionage offences in 2018 has contributed to a chilling effect on public interest journalism in Australia and, it follows, diminished Australian democracy. This has been effected by the apparent criminalisation of core aspects of legitimate, good faith journalism, and by the overwhelming complexity and uncertainty of the laws' design and scope. Media organisations and journalists have perceived the risks presented by the *Espionage Act* and, quite rightly, have no risk appetite for exposing individuals to criminal prosecution. In this environment, important stories may be silenced. Sources may not be coming forward and, if they do, some journalists are refusing to engage with them. Meanwhile, the journalists and editors we interviewed have dropped stories or reframed them to comply with laws that criminalise the publication of information that 'prejudices' Australia's international relations or, remarkably, advantages the international relations of another country. Dwindling media resources are being spent on legal advice and cat and mouse attempts to train journalists to do their job in this environment of risk and uncertainty.

This analysis is not intended to downplay the threat posed by modern espionage, or to argue that the laws ought to be rolled back. Rather, there is a need to step back and consider the far-reaching and sometimes hidden impacts of overbroad national security laws on individuals and institutions, as well as the rule of law and democracy. These impacts are evident even in the absence of prosecutions. Indeed, a lack of judicial consideration only serves to heighten the uncertainty and complexity of the legislative provisions. The laws themselves — let alone extended daylight raids on journalists' homes, media headquarters and whistleblowers — chill the free speech on which accountability, integrity and democracy depend.

Others have considered the strengths and weaknesses of the espionage laws more broadly and provided recommendations for reform to address the significant rule of law and civil liberties encroachments presented by the espionage framework.[186] This article has focused on press freedom alone, recognising newsroom professionals' consistent identification of espionage laws as posing a particular threat to public interest journalism. The protection of press freedom

[186] See, eg, Kendall (n 4); Law Council of Australia (n 5); Australian Lawyers for Human Rights (n 5); Whistleblowers Australia (n 5) 3–4; Human Rights Watch (n 5) 2–3; Parliamentary Joint Committee on Human Rights (n 5) 246–54 [2.369]–[2.411].

is complex and requires multifaceted solutions. The uncertainty and risk described by journalists could be addressed by enhancing legal clarity over, for example: the criminalisation of passive receipt of information, media organisations *as* foreign principals, the meaning of 'prejudice' to Australia's national security, and whether publication amounts to communication to a foreign principal. The perception of risk could be lessened by addressing apparent overbreadth in terms such as 'deal', 'information' and 'national security', as well as the amorphous notions of 'prejudice' to Australia's security and 'advantage' to a foreign country's security (even if that country is an ally of Australia). Some of the offences have few limiting factors; the introduction of a fault or harm element to Classified Information Espionage and Trade Secrets Espionage could constrain and target the scope of those offences.

However, the most straightforward and effective way to protect press freedom would be to recognise *in law* that legitimate, good faith, public interest journalism is not a crime. This could be done by introducing a carve-out from the offence framework, mirroring the News Reporting defence to the secrecy offences.[187] That defence protects both professional and non-professional journalists who report on public interest issues, although not if this is done to assist foreign intelligence agencies or military organisations.[188] Such a defence appropriately balances protecting legitimate journalism and protecting Australia from genuine espionage. However, the defence only applies to newsroom professionals, not sources.[189] Thus, press freedom requires robust and effective whistleblower protections, which have been the subject of pointed criticism and calls for review.[190]

In all, the 2018 espionage offences are the latest demonstration of Australia's well-recognised 'hyper-legislative' approach to issues of national security,[191] combined with sparse protections for fundamental rights and liberties as well as, sadly, core components of a healthy democracy. Protecting legitimate journalism in Australia is in everybody's interest, even (if not especially) when that

[187] On the importance of a carve-out instead of a defence, see Alliance for Journalists' Freedom (n 5) 9; Rebecca Ananian-Welsh et al, Submission No 17 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Impact of Law Enforcement and Intelligence Powers on the Freedom of the Press* (26 July 2019) 5–7 [1.2].

[188] *Criminal Code* (n 39) s 122.5(7)(d).

[189] Ibid s 122.5(6).

[190] AJ Brown, 'Safeguarding Our Democracy: Whistleblower Protection after the Australian Federal Police Raids' (Speech, Henry Parkes Oration, 26 October 2019); Australian Law Reform Commission, *The Future of Law Reform: A Suggested Program of Work 2020–25* (Final Report, December 2019).

[191] Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge University Press, 2011) ch 6; Kendall (n 4).

journalism casts individuals and institutions who wield public power in a poor light.