IN THE PUBLIC INTEREST: PROTECTIONS AND RISKS IN WHISTLEBLOWING TO THE MEDIA

REBECCA ANANIAN-WELSH,* ROSE CRONIN** AND PETER GRESTE***

Whistleblowing and a free press are vital to facilitating public accountability for powerful institutions and thereby improving integrity across the public and private sectors. But when is a whistleblower permitted to disclose information to the media? Once a whistleblower speaks to a journalist, what protections and assurances will they be entitled to? This article addresses these questions by examining existing protections for private and public sector whistleblowers and, relatedly, journalists' confidential sources under federal law. In this way, it explores the intersection between whistleblowing and press freedom and reveals gaps and weaknesses in existing legal frameworks.

I INTRODUCTION

Together, whistleblowing and a free press are vital to facilitating public accountability for powerful institutions and thereby improving integrity across the public and private sectors. But when is a whistleblower permitted to disclose information to the media? If they do, what protections and assurances will they be entitled to? This article addresses these questions by examining existing protections for private and public sector whistleblowers and, relatedly, journalists' confidential sources under federal law. In this way, it explores the intersections between whistleblowing and press freedom.

While these issues are by no means new, they have particular importance in Australia today. The relevant laws have been amended in recent years with persistent calls for further reforms.[1] Moreover, the adequacy of protections for press freedom and whistleblowers attracted unprecedented global attention as

* Associate Professor, University of Queensland School of Law.

** Research Assistant, University of Queensland School of Law.

*** Professor and UNESCO Chair in Journalism and Communications, University of Queensland School of Communication and Arts. The authors are indebted to Harry Meixner for his research assistance. The authors wish to acknowledge a donation from the Estate of Douglas Slatter and Elizabeth Chambers and a donation from David and Diane Brown in support of this work.

1 See, eg, 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* (Report, August 2020) xx ('*Inquiry into the Impact of the Exercise of Law Enforcement Report*'); Senate Environment and Communications References Committee, Parliament of Australia, *Inquiry into Press Freedom* (Report, May 2021) x–xi ('*Inquiry into Press Freedom Report*').

recently as 2019. In that year, the Australian Federal Police ('AFP') raided the home of News Corp journalist Annika Smethurst and the Sydney headquarters of the Australian Broadcasting Corporation ('ABC'). Later, the Australian Law Reform Commission identified 'press freedom and whistleblowers', together, as one of five priority areas for 'The Future of Law Reform'.[2] The linking of these two concerns reflected not only their close relationship, but that the primary targets of the AFP raids had not been the journalists, but their confidential sources. Moreover, a core concern for media organisations is the protection of confidential sources (including whistleblowers). In 2021, the prosecution of the intelligence whistleblower known as 'Witness K' came to a head, whilst that of his lawyer Bernard Collaery attracted widespread controversy.

This article begins by examining the nature and importance of whistleblowing, drawing on the AFP raids, the Witness K affair and other scenarios to explain some of the intersections between whistleblowing and press freedom. Part III provides an overview of the dynamic and complex frameworks under federal law that regulate private and public sector whistleblower protections. Part III closes by summarising the circumstances in which a whistleblower may make a protected disclosure to a journalist and identifying five reform priorities.

Once a person discloses information to a journalist, they become a 'source'. Part IV examines and critiques the legal protections owed to journalists' confidential sources. These protections complement whistleblower protections and serve a particularly important role if the source's entitlement to those protections is uncertain. Nonetheless, confidential sources (including whistleblowers) are vulnerable to identification by government agents.

Our analysis reveals the intersecting nature of whistleblower and source protection frameworks and the need to consider them together as facilitating a chain of disclosure which supports democracy, accountability, institutional integrity, and safe disclosure practices. It also reveals critical gaps and inconsistencies in legal protections and concludes by identifying key areas for law reform.

---

2 Australian Law Reform Commission, *The Future of Law Reform: A Suggested Program of Work 2020–25* (Report, December 2019) 42. See also broader concerns voiced in, eg, Fergus Hunter, '"A Culture of Secrecy": What Is the Right to Know Campaign about?', *The Sydney Morning Herald* (online, 21 October 2019) <https://www.smh.com.au/national/a-culture-of-secrecy-what-is-the-right-to-know-campaign-about-20191018-p5323v.html>; Alliance for Journalists' Freedom, 'Press Freedom in Australia' (White Paper, May 2019) <https://www.journalistsfreedom.com/wp-content/uploads/2019/06/AJF-Press-Freedom-In-Australia-2019.pdf>; Rebecca Ananian-Welsh, 'Australia Needs a Media Freedom Act. Here's How It Could Work', *The Conversation* (online, 22 October 2019) <https://theconversation.com/australia-needs-a-media-freedom-act-heres-how-it-could-work-125315>; AJ Brown, 'Safeguarding Our Democracy: Whistleblower Protection after the Australian Federal Police Raids' (Henry Parkes Oration, Tenterfield, 26 October 2019).

II WHISTLEBLOWERS, SOURCES AND PUBLIC ACCOUNTABILITY

A free and independent press is a core component of any liberal democracy grounded in the rule of law.[3] As the United Nations Human Rights Committee ('UNHRC') articulated:

> 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 Covenant rights … The Covenant embraces a right whereby the media may receive information on the basis of which it can carry out its function.[4]

This basic capacity for the media to 'receive information' depends, at least in part, on whether journalists can ensure source confidentiality. Thus, the UNHRC recognised that giving effect to the right to free expression requires the enforcement of a limited journalistic privilege to protect the identity of sources.[5]

Whistleblowers also play a vital role in upholding the rule of law and public accountability. Whistleblowing is 'the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action'.[6] As Marcia Miceli, Janet Near and Terry Morehead Dworkin said: 'If the individual does not consider the action to be wrong, but only misguided or stupid, it is not whistle-blowing'.[7]

Whistleblowers facilitate both internal and external accountability across the public and private sectors. An extensive empirical study of whistleblowing in Australia, led by AJ Brown, revealed that whistleblowers 'are the single most important way that wrongdoing or other problems come to light in organisations'.[8] In addition to its practical, organisational importance, whistleblowing can help to avoid the considerable financial costs of organisational wrongdoing. Writing in 2008, Miceli, Near and Dworkin estimated that such costs, in the US alone

> include $5 billion in employee theft, $350 billion attributable to antitrust violations, $300 billion in tax fraud, and $100 billion in health care fraud. Around the world, annual costs of corruption have been estimated at $1 trillion.[9]

Whistleblowing, particularly in the public sector, also plays a democratic role. Democracy thrives on information: responsible and representative government rely on Parliament and voters being informed about the workings of government. The information required by Parliament and the electorate is not limited to summaries of policy, outputs and successes. It necessarily includes information about

---

3 Tom Bingham, *The Rule of Law* (Penguin Books, 2011) 78.

4 Human Rights Committee, *General Comment No 34: Article 19, Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) 3–4 [13].

5 Ibid 5 [19], 11 [45].

6 Marcia Miceli and Janet Near, 'Organizational Dissidence: The Case of Whistleblowing' (1985) 4(1) *Journal of Business Ethics* 1, 4. The use of this definition is discussed in Marcia Miceli, Janet Near and Terry Dworkin, *Whistle-Blowing in Organizations* (Routledge, 2008) 6.

7 Miceli, Near and Dworkin (n 6) 6.

8 Brown (n 2) 7.

9 Miceli, Near and Dworkin (n 6) 2 (citations omitted).

misconduct, corruption, incompetence, and the abuse of power; information that governments might be inclined to withhold. While formal systems of accountability such as the courts and oversight committees are vital mechanisms for policing governments, the informal watchdog roles of whistleblowers and the press remain key components of the system. In some instances, they expose conduct that is neither illegal nor incompetent (and so is not necessarily 'whistleblowing') but that nonetheless deserves democratic scrutiny.[10]

The importance of public accountability is not limited to the public sector. Employees speaking out against organisational wrongdoing led to major inquiries, such as the Banking Royal Commission, and revealed serious misconduct by organisations as diverse as Enron, Boeing, WorldCom, Global Crossing and Australian Reserve Bank-owned companies Securency Ltd and Note Printing Australia.[11] The considerable economic and public power wielded by private actors heightens the social importance of whistleblowers and public accountability in this sphere.

Whilst whistleblowing serves an undeniably important role in maintaining public and private organisational integrity, it is not 'an unqualified good': 'frivolous or poorly articulated claims can cause needless disruption to important public institutions'.[12] Processes and protections for whistleblowing must therefore be carefully calibrated to maximise accountability and integrity, and minimise unjustified or unnecessary negative consequences at a systemic level as well as for the organisations and the individuals concerned.

The disclosure of certain kinds of information can render a whistleblower vulnerable to a range of serious consequences, especially if their anonymity is compromised and they are 'dragged or forced into the public domain'.[13] In addition to unemployment and personal reprisals, the individual may become the subject of legal action, such as for breach of contract or even criminal offences. These repercussions are not only serious for the individual, they have a more far-reaching impact. Reprisals on whistleblowers can have a 'chilling effect' on future whistleblowing, convincing people not to speak out about misconduct or abuse of power.[14]

Most whistleblower concerns are handled internally, within an organisation. It is reasonable to assume that there will be times when internal systems of accountability fail or are somehow inadequate or inappropriate for the problem at hand, or when individuals may lack faith in whistleblower protections and feel too exposed to use formal internal channels. Moreover, those in positions of power

10 For example, Smethurst revealed that two government departments were considering expanding the powers of the nation's international electronic eavesdropping agency, the Australian Signals Directorate ('ASD'), so it could target Australian citizens: see 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>.

11 See Brown (n 2) 8; Miceli, Near and Dworkin (n 6) 1.

12 Danielle Ireland-Piper and Jonathan Crowe, 'Whistleblowing, National Security and the Constitutional Freedom of Political Communication' (2018) 46(3) *Federal Law Review* 341, 342.

13 Brown (n 2) 9.

14 Ibid 12.

may not volunteer information about internal misconduct or abuse of power more widely, for example, to Parliament, shareholders, or the public at large.

When embarrassing (or even damning) information finds its way into the public sphere, it may be through the joint operation of whistleblowers and the free press. Under these circumstances, the media becomes a kind of whistle-of-last-resort 'for those who feel disempowered by formal accountability processes'.[15] This last resort can only be effective if journalists are able to fulfil their professional obligation to protect confidential sources. The absence of a protected channel through which to communicate with the media may convince a potential whistleblower not to speak out at all, letting integrity and the chance for accountability and improvement – as well as the attendant democratic and economic benefits of whistleblowing – slip away. For all these reasons, Brown has emphasised the vital importance of

> comprehensive, effective whistleblowing regimes for ensuring that disclosures are properly managed, and when made to third parties (including the media) occur as much as possible in a manner that recognises and supports the wider public interest.[16]

The direct relationship between whistleblowers and the media is important, but it ought not be overstated. It has been reported that only 1% of whistleblowers disclose information directly to a journalist, media organisation or public website.[17] Clearly, not all whistleblowers are journalists' sources; and few sources are whistleblowers. The rarity of whistleblower disclosures to the media does not, however, detract from their critical public function.

Identifying the overlap between whistleblowers and sources is not necessarily straightforward. The nature of this intersection is illuminated in five case studies which attracted considerable controversy and prompted calls for the review of both whistleblower and press freedom protections, namely the disclosures by: Allan Kessing, Andrew Wilkie, David McBride, Annika Smethurst's unknown source, and Witness K. These case studies – among others – demonstrate the continued relevance of whistleblowing to the media, as well as the range of governmental responses and 'public interest' concerns in play.

A Allan Kessing

Allan Kessing was as a Sydney Airport customs officer who, in 2003, wrote two confidential reports detailing serious security lapses. The reports were initially buried, but two years later *The Australian* obtained them and published damning details which triggered an inquiry and an AUD220 million upgrade to airport security. The reports also prompted a police investigation which identified Kessing as the journalist's confidential source through telephone records showing a call from a public phone box near his home to *The Australian* a few days before the story was published. Kessing – who always maintained he was not responsible for

15 Ireland-Piper and Crowe (n 12) 342.

16 Brown (n 2) 12.

17 Brown et al, *Clean as a Whistle: A Five Step Guide to Better Whistleblowing Policy and Practice in Business and Government* (Report, Griffith University, August 2019) 48.

the leak – was charged under the now repealed section 70 of the *Crimes Act 1914* (Cth) and received a nine-month suspended sentence.[18]

B Andrew Wilkie

In 2003, former military officer Andrew Wilkie was working at the Office of National Assessments ('ONA'), processing intelligence related to the search for weapons of mass destruction ('WMDs') in Iraq. Then Prime Minister John Howard had committed Australia to supporting the United States of America ('US') led invasion of Iraq, on the understanding that Iraqi President Saddam Hussein had WMDs and links to Al-Qaeda and so posed a threat to regional stability. On 13 March 2003, the Prime Minister told the National Press Club, '[w]e believe that it is very much in the national interest of Australia that Iraq have taken from her chemical and biological weapons'.[19]

Wilkie said he could see no evidence to support these claims, and believed the Prime Minister was leading the nation into war on a false premise. He resigned from the ONA and told Channel Nine's chief political correspondent Laurie Oakes, '[Iraq's] military is very small, their weapons of mass destruction program is fragmented and contained … and there is no hard evidence for any active co-operation between Iraq and Al-Qaeda'.[20]

Wilkie later dismissed claims that he should have taken his complaint to the Inspector-General of Intelligence and Security ('IGIS'): 'IGIS is irrelevant in this matter because [her office's] remit is the activities of the intelligence agencies, while my complaint was with the conduct of the government'.[21] In light of the gravity of the unfolding situation and with no option for internal disclosure, he took his concerns to the media.

Wilkie has admitted that his disclosure to Laurie Oakes amounted to illegal conduct, but argued that there was a compelling public interest in his disclosure. Wilkie believes he ultimately escaped prosecution because the government judged the political cost of prosecuting him to be higher than the damage caused by his leaks.[22] An assessment of this nature may have saved Wilkie from a jail term and, incidentally, paved the way for his subsequent election as an Independent Federal MP – a position he has held since 2010.

---

18 *R v Kessing* (2008) 73 NSWLR 22, 24 [4]–[9] (Bell JA, Rothman J agreeing at 43 [88], Price J agreeing at 43 [89]); The offence of disclosure of information by Commonwealth officers, contained in section 70 of the *Crimes Act 1914* (Cth), was repealed by the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), and replaced with provisions in part 5.6 of the *Criminal Code Act 1995* (Cth) schedule 1 dealing with secrecy of information.

19 John Howard, 'Address to the National Press Club' (Speech, National Press Club, 13 March 2003) 1 <https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/PDS86/upload_binary/pds865.pdf;fileType=application%2Fpdf#search=%22media/pressrel/PDS86%22>.

20 Matthew Moore and Mathew Murphy, 'Top Advisor Quits over War Stance' *The Age* (online, 12 March 2013) <https://www.theage.com.au/national/top-adviser-quits-over-war-stance-20030312-gdvd2s.html>.

21 Peter Greste, *The First Casualty* (Penguin Random House, 2017) 233, quoting Email from Andrew Wilkie to Peter Greste, 9 February 2017.

22 Ibid 232.

C David McBride

On 5 June 2019, the AFP executed an eight-hour raid on the ABC's Sydney headquarters. The raid concerned a July 2017 report, 'The Afghan Files', by investigative journalists Dan Oakes and Sam Clark, which expanded on earlier reporting in ABC's *7.30* program. Oakes and Clark opened their report by citing

> Hundreds of pages of secret defence force documents leaked to the ABC [which] give an unprecedented insight into the clandestine operations of Australia's elite special forces in Afghanistan.[23]

The leaked documents revealed shocking incidents of troops killing unarmed men and children, 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.

Nine months before the raids, David McBride had been charged with a range of criminal offences over his alleged role in leaking to the ABC the information that would form the basis of 'The Afghan Files' reports.[24] Over several months in 2014, while employed as a security cleared military lawyer for the Australian Defence Force ('ADF'), McBride compiled an extensive dossier of classified material which revealed potential war crimes committed by Australian Special Forces soldiers in Afghanistan. McBride pursued his complaint through internal channels and then the AFP.[25] Following this, McBride claimed that his career 'went downhill' whilst the internal inquiry 'went nowhere', prompting his eventual disclosure to the ABC.[26]

At the time of writing, McBride's trial is ongoing in the Australian Capital Territory ('ACT') Supreme Court where the matter has been split into two proceedings. The first is a civil hearing, at which McBride will argue that he is entitled to whistleblower protections. The second is his criminal trial for a range of offences to which he has pleaded not guilty. These include: theft of Commonwealth property (the information),[27] the unauthorised disclosure of a Commonwealth document,[28] and unlawfully giving information about Australia's

---

23 Dan Oakes and Sam Clark, 'The Afghan Files', *ABC News* (online, 11 July 2017) <https://www.abc.net.au/news/2017-07-11/killings-of-unarmed-afghans-by-australian-special-forces/8466642?pfmredir=sm>.

24 *Australian Broadcasting Corporation v Kane [No 2]* (2020) 377 ALR 711, 714 [11] (Abraham J) ('*Kane [No 2]*'); 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>.

25 David Wroe, '"What I've Done Makes Sense to Me": The Complicated, Colourful Life of David McBride', *The Sydney Morning Herald* (online, 23 June 2019) <https://www.smh.com.au/politics/federal/what-i-ve-done-makes-sense-to-me-the-complicated-colourful-life-of-david-mcbride-20190621-p5204h.html>.

26 Rod McGuirk, 'Australian Whistleblower to Represent Himself at Trial', *The Diplomat* (online, 7 November 2019) <https://thediplomat.com/2019/11/australian-whistleblower-to-represent-himself-at-trial/>.

27 *Criminal Code Act 1995* (Cth) s 131.1(1).

28 *Crimes Act 1914* (Cth) s 70(1). McBride was charged with this offence on 7 March 2019: *Kane [No 2]* (2020) 377 ALR 711, 714 [11] (Abraham J). Section 70 of the *Crimes Act 1914* (Cth) was repealed by schedule 2 of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), effective 29 December 2018. Sections 70 and 79 of the *Crimes Act 1914* (Cth), the latter containing the offence of unlawful disclosure of official secrets, were replaced by provisions in part 5.6 of the *Criminal Code Act 1995* (Cth) dealing with secrecy of information.

defence capabilities.[29] The trial has attracted considerable controversy, with a Senate Committee recommending 'that that the Commonwealth Director of Public Prosecutions [('CDPP')] urgently reconsider, on strong public interest grounds, whether the prosecution' should continue.[30]

The commission of war crimes by members of the ADF, as disclosed by McBride, has since been supported in the Inspector-General of the Australian Defence Force Afghanistan Inquiry Report ('Brereton Report'), released in November 2020.[31] The inquiry recommended that the Chief of the Defence Force refer 36 matters, relating to the 25 incidents and involving 19 individuals, to the AFP for investigation.[32]

The journalists who received and ultimately published the sensitive material from McBride also risked prosecution. In July 2020, the AFP referred its brief of evidence in relation to Dan Oakes to the CDPP. In response, Oakes tweeted:

> Whether or not we are ever charged or convicted over our stories, the most important thing is that those who broke our laws and the laws of armed conflict are held to account. Our nation should be better.[33]

The CDPP dropped the charges against Oakes in October 2020 on public interest grounds, despite 'reasonable prospects of conviction'.[34]

---

29 *Defence Act 1903* (Cth) s 73A(1). As noted in *Kane [No 2]* (2020) 377 ALR 711, 715 [19] (Abraham J):

> On 13 June 2019, the Guardian published an article about the McBride Proceedings, with statements in the article being attributed to Mr McBride, noting that Mr McBride did not dispute leaking the material but that he intended to argue he was acting on his duty to report illegal conduct by the government.

30 *Inquiry into Press Freedom Report* (n 1) xii.

31 Inspector-General of the Australian Defence Force, *Afghanistan Inquiry* (Report, 10 November 2020). Report findings include credible information of 23 incidents in which members of the Special Operations Task Group unlawfully killed, or directed the unlawful killing of, non-combatants, occurring between 2009 and 2013. These incidents were perpetrated by 25 current or former members of the ADF, acting either as principals or accessories, and resulted in the murder of 39 individuals as well as cruel treatment of a further 2 individuals: at 29.

32 Ibid 29.

33 Jordan Hayne, 'Investigation into Afghan Files That Sparked ABC Raids Enters Next Phase with Brief of Evidence Sent to Prosecutors', *ABC News* (online, 2 July 2020) <https://www.abc.net.au/news/2020-07-02/federal-police-seek-charges-abc-investigation-afghan-files-dpp/12415930>.

34 Australian Federal Police, 'AFP Statement on Investigation into ABC Journalist' (Media Release, 15 October 2020) <https://www.afp.gov.au/news-media/media-releases/afp-statement-investigation-abc-journalist>. Notably, 2019 reforms designed to protect journalists (introduced in the wake of the initial AFP raids) had also required the personal approval of the Commonwealth Attorney-General before any such prosecution could proceed: Attorney-General (Cth), 'Ministerial Direction (Commonwealth Director of Public Prosecutions)' in Commonwealth of Australia, *Government Notices Gazette*, No C2019G00878, 19 September 2019. This direction requires the CDPP to obtain the consent of the Attorney-General prior to charging journalists working in a 'professional capacity' with unauthorised disclosure of information relating to a special intelligence operation (*Australian Security Intelligence Organisation Act 1979* (Cth) s 35P); unauthorised disclosure of information relating to a delayed notification search warrant (*Crimes Act 1914* (Cth) s 3ZZHA); unauthorised disclosure of information relating to a controlled operation (*Crimes Act 1914* (Cth) s 15HK); theft and receipt of Commonwealth property (*Criminal Code Act 1995* (Cth) ss 131.1, 132.1.); and communicating or obtaining information about Defence bases or work (*Defence Act 1903* (Cth) s 73A).

D Annika Smethurst

The raid on the ABC in relation to Oakes and Clarke's Afghan Files investigation came less than 24 hours after AFP officers had searched News Corp journalist Annika Smethurst's Canberra home, seeking information that might reveal the identity of one of her confidential sources. This raid had been prompted by a series of stories published by *The Daily Telegraph* in April 2018, based on a departmental memo marked Top Secret which concerned a proposal to significantly expand the powers of the Australian Signals Directorate ('ASD').[35] Smethurst reported that the proposed new powers would enable the ASD to covertly access Australians' digital information – including financial transactions, health data, and telecommunications records – without a warrant. Absent judicial oversight, the expanded powers risked civil liberties and were of considerable public interest.[36]

The raid on Smethurst appeared to be focused on identifying her confidential source. Three months later, a raid was conducted on the home of former intelligence officer Cameron Jon Gill on the suspicion that he was responsible for leaking documents, including the Top Secret memo, to Smethurst.[37] The investigation into Gill – who maintains his innocence – was subsequently dropped for lack of evidence, and Smethurst still refuses to name her source.[38] It was not until 27 May 2020, following Smethurst's successful High Court challenge to the warrant,[39] that the AFP announced it would not pursue charges against Smethurst or her anonymous source.[40]

The June raids on Smethurst and the ABC attracted global attention, calling into question the capacity of Australian media to effectively engage in journalism of acute public interest, but that may be controversial or embarrassing to government.[41] Criticism of the AFP – particularly regarding its independence

35 Smethurst (n 10). For the powers of the ASD, see *Intelligence Services Act 2001* (Cth) s 7.

36 Smethurst (n 10).

37 Paul Karp, 'High Court Rules AFP Warrant for Raid on News Corp Journalist's Home Was Invalid', *The Guardian* (online, 15 April 2020) <https://www.theguardian.com/australia-news/2020/apr/15/high-court-rules-afp-warrant-for-raid-on-news-corp-journalists-home-was-invalid>.

38 Fergus Hunter, 'Police Rule Out Charging News Corp Journalist Annika Smethurst', *The Sydney Morning Herald* (online, 27 May 2020) <https://www.smh.com.au/politics/federal/police-rule-out-charging-news-corp-journalist-annika-smethurst-20200527-p54wwd.html>.

39 In *Smethurst v Commissioner of Police* (2020) 376 ALR 575, the High Court unanimously held that the search warrant over Smethurst's property failed to properly identify the offence under investigation, rendering the warrant invalid and the search an unlawful trespass. By narrow majority, the Court rejected Smethurst's claim for a mandatory injunction to compel the destruction or return of the information seized under the warrant. Smethurst's constitutional challenge to the underlying secrecy offence under investigation was not addressed by the Court. For discussion of the case, see 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.

40 See Jordan Hayne, 'AFP Will Not Lay Charges against Annika Smethurst over Publishing of Classified Intelligence Documents', *ABC News* (online, 27 May 2020) <https://www.abc.net.au/news/2020-05-27/afp-will-not-lay-charges-annika-smethurst-raid/12291238>. This ABC story quoted Deputy AFP Commissioner McCartney as saying the evidence seized by police would not be used in any future investigations: '"Under our guidelines and procedures, that evidence has now been destroyed," he said'.

41 See, eg, Jamie Tarabay, 'Australian Police Raids Target News Media over Leaked Documents', *The New York Times* (online, 4 June 2019) <https://www.nytimes.com/2019/06/04/world/australia/journalist-raid-annika-smethurst.html>; 'Australia: Police Raid ABC Headquarters over Afghanistan Stories', *Al Jazeera*

from government – was heightened by apparent inconsistencies in their approach which seemed to favour government interests. On the one hand, prosecutions against Witness K, Collaery and McBride had commenced, and investigations into journalists, including Dan Oakes, were then ongoing. On the other hand, the agency had controversially dropped an investigation into doctored documents used by Federal Minister for Energy and Emissions Reduction, Angus Taylor, and had failed to interview Taylor in that investigation.[42]

In addition to legal challenges,[43] the AFP's June 2019 raids prompted two parliamentary inquiries.[44] Relevantly, both inquiries emphasised 'recognised deficiencies' in federal public sector whistleblower protections,[45] including a lack of clarity, inconsistencies between public and private sector protections, and problems with the public interest test and reprisal protections.[46]

Even in clear instances of government leaks to the media, the relationship between whistleblowers and confidential sources may not be entirely straightforward. It is uncertain whether the information leaked to Smethurst contained allegations of misconduct and, therefore, amounted to whistleblowing – despite the clear public interest in the information contained in the ASD memo. Both McBride and Smethurst's source were 'confidential sources', though McBride's identity would become known as he admitted, and attempted to justify, his decision to leak classified documents to the ABC.[47]

E Witness K and Bernard Collaery

On 6 August 2019, one month after the raids on Smethurst and the ABC, 'Witness K' informed the ACT Magistrates' Court that he would be pleading guilty to breaching section 39 of the *Intelligence Services Act 2001* (Cth). Witness K's crime involved revealing to his security cleared barrister, Bernard Collaery, secret information obtained in the course of his duties as an Australian Secret Intelligence Service ('ASIS') agent. This information concerned the bugging of Timor-Leste government rooms, including Cabinet offices, by ASIS agents in 2004. This conduct

(online, 5 June 2019) <https://www.aljazeera.com/news/2019/6/5/australia-police-raid-abc-headquarters-over-afghanistan-stories>.

42 Paul Karp and Anne Davies, 'Angus Taylor: AFP Drops Investigation into Doctored Documents Scandal', *The Guardian* (online, 6 February 2020) <https://www.theguardian.com/australia-news/2020/feb/06/angus-taylor-afp-drops-investigation-into-doctored-documents-scandal>.

43 Both Smethurst and the ABC launched legal challenges to the raids. Justice Abraham of the Federal Court upheld the warrants that supported the ABC raid and rejected the ABC's constitutional challenge to the validity of the search warrant provisions in the *Crimes Act 1914* (Cth): *Kane [No 2]* (2020) 377 ALR 711.

44 *Inquiry into Press Freedom Report* (n 1); *Inquiry into the Impact of the Exercise of Law Enforcement Report* (n 1).

45 *Inquiry into Press Freedom Report* (n 1) x–xi.

46 *Inquiry into the Impact of the Exercise of Law Enforcement Report* (n 1) xx.

47 David McBride, '"My Duty Was to Stand and Be Counted": Why I Leaked to the ABC', *The Sydney Morning Herald* (online, 9 June 2019) <https://www.smh.com.au/national/my-duty-was-to-stand-and-be-counted-why-i-leaked-to-the-abc-20190608-p51vte.html>.

had been undertaken in the context of treaty negotiations between the two countries, concerning oil and gas reserves reportedly worth AUD40 to AUD50 billion.[48]

Witness K's deep discomfort about the operation prompted him to approach the IGIS who then referred him to Collaery for legal advice.[49] Based on this information, Collaery assisted Timor-Leste to build a case against Australia at the Hague, seeking to void the treaty on the basis of Australia's breach of international law.[50]

In March 2017, some two months after a new treaty was signed, and 13 years after the bugging occurred, Witness K and Collaery were charged with secrecy offences under the *Intelligence Services Act 2001* (Cth). Though Witness K pleaded guilty in 2019, it was not until June 2021 that the ACT Magistrates' Court brought the matter to its conclusion – sentencing him to a mere three month suspended sentence.[51] Following the decision, former President José Ramos-Horta called on Timor-Leste to award Witness K that nation's highest honour: 'the Medal of Honor of the Republic in recognition of his integrity and courage'.[52] At the time of writing, Collaery's trial has commenced in the ACT Supreme Court, under hotly contested conditions of secrecy imposed by provisions of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).[53]

---

48 Christopher Knaus, 'Witness K and the "Outrageous" Spy Scandal that Failed to Shame Australia', *The Guardian* (online, 10 August 2019) <https://www.theguardian.com/australia-news/2019/aug/10/witness-k-and-the-outrageous-spy-scandal-that-failed-to-shame-australia>.

49 Bernard Keane, 'Open and Shut: ASIS' Crime, and the Labor-Liberal Cover-Up', *Crikey* (online, 12 June 2015) <https://www.crikey.com.au/2015/06/12/open-and-shut-asis-crime-and-the-labor-liberal-cover-up/>:

> Witness K went to great lengths to secure from the then-Inspector General of Intelligence and Security, Ian Carnell, approval under the highly restrictive framework governing intelligence officers to conduct, *inter alia*, "private legal action" in relation to his workplace complaint, with Collaery approved to act for him. Witness K's statements about the bugging of East Timor form part of this IGIS-approved complaint.

50 Ibid. The International Court of Justice ordered Australia to cease impugned spying activities and seal documents and data relating to the case that had been seized in an ASIO raid on Collaery: *Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia) (Provisional Measures)* [2014] ICJ Rep 147, 160–1 [55]. More broadly, Timor-Leste withdrew its case against the Australian government as an act of good faith when treaty negotiations resumed between the countries: *Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia) (Order on 11 June 2015)* [2015] ICJ Rep 572.

51 Elizabeth Byrne, 'Former Australian Spy Witness K Spared Jail Time Over Conspiracy Charges Relating to Alleged Spying on East Timor', *ABC News* (online, 18 June 2021) <https://www.abc.net.au/news/2021-06-18/act-witness-k-sentencing-hearing/100226438>.

52 Christopher Knaus, 'José Ramos-Horta Calls on Timor-Leste to Award Australia's Witness K Top Honour', *The Guardian* (online, 21 June 2021) <https://www.theguardian.com/australia-news/2021/jun/21/jose-ramos-horta-calls-on-timor-leste-to-award-australias-witness-k-top-honour>.

53 The *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ('*NSI Act*') guides federal criminal and civil proceedings involving national security information with the objective of preventing the disclosure of information likely to prejudice national security, to the extent that the administration of justice is not seriously interfered with: at s 3. The processes established by the *NSI Act* require the court to give significant weight to the opinion of the Attorney-General, particularly regarding the importance of relevant matters and information to national security. A key mechanism of public accountability is found in section 47 of the *NSI Act*, which provides that the Attorney-General must make an annual report to Parliament on, among other matters, the number of certificates issued by the Attorney-General to prevent the disclosure of information. Former Attorney-General Christian Porter failed to comply with this reporting requirement since being appointed in 2017: Kieran Adair, 'Attorney General Christian Porter Breaches Law over Three Years, Claims It Was a Mistake', *Michael West Media* (online, 21 August 2020) <https://www.michaelwest.com.au/christian-porter-nsi-orders/>. For discussion

Witness K is certainly a whistleblower, though his disclosures had been to the IGIS and Collaery, not to a journalist. Collaery revealed the information more widely and has become a source of information for the media (though seemingly not a confidential one). However, Collaery's position outside the Australian government means he is not a whistleblower.

The multifaceted dynamic between whistleblowers and sources – including where a whistleblower can disclose to another person who then becomes a source – demonstrates the importance of compatible and effective whistleblower *and* source protections. The chain of disclosure necessary to achieve accountability and integrity requires safe and appropriate channels for the communication of information, from internal complaint management through to, in some cases, public dissemination through a free and independent press.

III WHISTLEBLOWER PROTECTIONS: THE LEGAL FRAMEWORKS

Commonwealth law establishes frameworks for protected public and private sector whistleblower disclosures under the *Public Interest Disclosure Act 2013* (Cth) ('*PIDA*') and the *Corporations Act 2001* (Cth) ('*Corporations Act*'), respectively. These protections have evolved over time and both Acts have been subject to relatively recent amendment. The adoption of *PIDA* in 2013 was part of an extensive overhaul of public sector whistleblowing laws.[54] Legal protections for private sector whistleblowers were amended in July 2019.[55] Nonetheless, Australia's existing whistleblower protection frameworks have been described as 'a well-motivated but largely dysfunctional mess' that 'works in some respects, but often, not when it really matters'.[56] In this Part, we provide an overview of existing legal protections for private sector and public sector whistleblowers, then focus on the scope of protected disclosures to the media.

A Private Sector Disclosures

Private sector whistleblowing is predominantly governed by the *Corporations Act*, which grants a robust set of protections. Private sector whistleblowers may not

---

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

54 Sulette Lombard and Vivienne Brand, 'Corporate Whistleblowing: Public Lessons for Private Disclosure' (2014) 42(5) *Australian Business Law Review* 351, 354.

55 *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019* (Cth), amending: *Corporations Act 2001* (Cth); *Taxation Administration Act 1953* (Cth); *Banking Act 1959* (Cth); *Insurance Act 1973* (Cth); *Life Insurance Act 1995* (Cth); and *Superannuation Industry (Supervision) Act 1993* (Cth). These amendments expanded the range of people eligible to make and receive protected disclosures and redefined the subject matter of protected disclosures to a broader range of conduct, previously restricted to breaches of the *Corporations Act 2001* (Cth) or the *Australian Securities and Investments Commission Act 2001* (Cth). The amendments also removed the requirement that disclosures be made in good faith and created avenues for emergency and public interest disclosures to be made to journalists or Members of Parliament in prescribed circumstances.

56 Brown (n 2) 13–14.

be subject to any civil, criminal or administrative liability, or disciplinary action, for making a protected disclosure under the Act.[57] No remedy may be enforced, and no legal right exercised, against a whistleblower on the basis of their disclosure.[58] Where a disclosure is made to an 'eligible recipient' (defined below), the disclosed information will not be admissible as evidence in a proceeding against the whistleblower, except where that proceeding concerns the falsity of the information.[59]

The *Corporations Act* offers a general form of protection by criminalising the disclosure of a protected whistleblower's identity.[60] In addition to protecting anonymity, the Act creates a victimisation offence. This offence prohibits conduct that causes or threatens detriment to a person on the basis of a belief or suspicion that they (or someone else) 'made, may have made, proposes to make or could make' a protected disclosure.[61] Where a person is found to have engaged in victimisation, the court is empowered to make appropriate remedial orders.[62] This may include orders for injunctive relief, an apology,[63] or the payment of compensation to the discloser, potential discloser, or any other person.[64] Where the victimisation involves the termination of the discloser's employment, the court may order their reinstatement.[65]

These are significant protections. However, they do not attach to every disclosure of misconduct in the private sector.

1 General Principles and Disclosures to Eligible Recipients

The scope of private sector whistleblower protections hinges on four defined terms. Only disclosures of a 'disclosable matter' about a 'regulated entity' are protected. In addition, that disclosure must be made by an 'eligible whistleblower' to an 'eligible recipient'.

Both 'regulated entity' and 'eligible whistleblower' are defined broadly in the Act. The first term encompasses all companies, general and life insurers, superannuation entities, and any other entities prescribed by regulation.[66] A person is an 'eligible whistleblower' if they are, or have been, an officer, employee, associate or supplier of goods and services to a regulated entity,[67] or the relatives, dependent or spouse of such a person.[68]

---

57 *Corporations Act 2001* (Cth) s 1317AB(1)(a).
58 Ibid s 1317AB(1)(b).
59 Ibid s 1317AB(1)(c).
60 Ibid s 1317AAE.
61 Ibid s 1317AC. This offence extends to threats that are express, implied, conditional or unconditional: at s 1317AC(4).
62 Ibid ss 1317AD, 1317AE(1)(g).
63 Ibid ss 1317AE(1)(c)–(d).
64 Ibid ss 1317AE(1)(a)–(b).
65 Ibid s 1317AE(1)(g).
66 Ibid s 1317AAB.
67 Ibid ss 1317AAA(a)–(e).
68 Ibid ss 1317AAA(g)–(h). Distinct qualifications exist for whistleblowers in superannuation entities. An 'eligible whistleblower' within a superannuation entity includes an individual who is a trustee of the entity, within the meaning of the *Superannuation Industry (Supervision) Act 1993* (Cth), or an officer of a body corporate that is a trustee, custodian or investment manager of the superannuation entity, or an

The term 'disclosable matter' is defined more narrowly. A protected private sector disclosure will include information that:

- the discloser suspects on reasonable grounds concerns misconduct, or an improper state of affairs or circumstances, in relation to a regulated entity;[69]
- relates to an offence against or contravention of prescribed legislation;[70]
- relates an offence punishable by at least 12 months' imprisonment;[71] or
- relates to a matter that represents a danger to the public or the financial system.[72]

If a whistleblower meets these criteria, they may disclose the information to an 'eligible recipient'. This includes: the Australian Securities and Investments Commission, the Australian Prudential Regulation Authority, prescribed Commonwealth authorities, and eligible recipients (for example, senior managers or trustees) within a body corporate or superannuation entity.[73]

2 Private Sector Public Interest Disclosures

A 'public interest disclosure' under the *Corporations Act* may be made to a journalist or a Member of Parliament in very limited circumstances. First, a disclosure must have been made to an eligible recipient at least 90 days prior. Second, the regulated entity must be given written notice of the intention to make further disclosure. Third, the whistleblower must 'not have reasonable grounds to believe that action is being, or has been, taken to address the matters to which the previous disclosure related'.[74] Fourth, the whistleblower must have reasonable grounds to believe that the disclosure is in the public interest.[75] If these criteria are met, the disclosure qualifies as a protected public interest disclosure. Importantly, however, the extent of the information disclosed must be no greater than necessary to inform the recipient of the misconduct or improper state of affairs.[76]

A private sector public interest disclosure may only be made to a journalist who satisfies the definition of 'journalist' in the *Corporations Act*, namely: a person working in a professional capacity for a newspaper, magazine, radio or

---

individual who supplies goods and services to any aforementioned individual: *Corporations Act 2001* (Cth) s 1317AAA(f).

69 *Corporations Act 2001* (Cth) s 1317AA(4).

70 Ibid s 1317AA(5)(c) for the prescribed legislation, eg, *Corporations Act 2001* (Cth); *Australian Securities and Investments Commission Act 2001* (Cth); *Banking Act 1959* (Cth); *Financial Sector (Collection of Data) Act 2001* (Cth); *Insurance Act 1973* (Cth); *Life Insurance Act 1995* (Cth); *National Consumer Credit Protection Act 2009* (Cth); and *Superannuation Industry (Supervision) Act 1993* (Cth).

71 *Corporations Act 2001* (Cth) ss 1317AA(5)(d).

72 Ibid s 1317AA(5)(e).

73 Ibid ss 1317AA(1)(b), (2). An 'eligible recipient' within a body corporate includes an officer, senior manager, auditor or actuary of a body corporate, or a person authorised by the body corporate to receive disclosures: s 1317AAC(1). An 'eligible recipient' within a superannuation entity includes an officer, auditor, actuary or trustee of a superannuation entity, or a person authorised by the trustee or trustees to receive disclosures: s 1317AAC(2).

74 Ibid s 1317AAD(1)(c).

75 Ibid s 1317AAD(1). Cf *Public Interest Disclosure Act 2013* (Cth) ss 26(3)(ad), (ae)(a)(i)–(vi) ('*PIDA*').

76 *Corporations Act 2001* (Cth) s 1317AAD(1)(g).

television broadcasting services, or an electronic news service which is 'operated on a commercial basis'.[77] A disclosure to a blogger or otherwise 'non-professional' journalist or, arguably, to a media organisation run on a not-for-profit basis (such as a community radio station or online news site) may not be protected under the *Corporations Act*.

3 Emergency Disclosures and Legal Advice

There are two further forms of protected disclosure for private sector whistleblowers. An 'emergency disclosure' may be made when a whistleblower has reasonable grounds to believe that the information concerns a substantial and imminent danger to the natural environment or the health or safety of one or more persons.[78] As with external disclosures, emergency disclosures may only be made to a journalist (as defined in the *Corporations Act*) or a Member of an Australian Parliament.[79] An emergency disclosure will only be protected, however, if it is first made to an eligible recipient, and the entity is given written notice of the intention to make the further disclosure.[80] In a situation of emergency, this would entail a rapid succession of disclosures and notifications in order for the disclosure to a journalist or MP to qualify for protection. As with private sector public interest disclosures, only information 'necessary to inform the recipient … of the substantial and imminent danger' may be disclosed.[81]

Finally, a person may disclose information to a legal practitioner for the purpose of obtaining legal advice or representation in relation to the operation and application of the whistleblower provisions in the *Corporations Act*.[82]

B Public Sector Disclosures

Public sector whistleblowing is governed by *PIDA*, which adopts a distinct approach to whistleblower protections. Like the *Corporations Act*, *PIDA* protects the discloser's identity and provides immunity from liability in civil or criminal proceedings. It protects whistleblowers from reprisals (rather than 'victimisation'), creating a criminal offence of undertaking or threatening a reprisal, punishable by up to 2 years' imprisonment.[83] Reprisals occur where detrimental action is taken against a person due to a belief or suspicion that they have made, or propose to make, a public interest disclosure. Section 13 of *PIDA* lists specific examples of reprisals, including dismissal, injury, discrimination, or alteration of employment.[84] As under the *Corporations Act*, courts are given a wide discretion as to potential relief that

77 Ibid s 1317AAD(3).
78 Ibid s 1317AAD(2)(b).
79 Ibid s 1317AAD(2)(d).
80 Ibid s 1317AAD(2). Unlike *PIDA 2013* (Cth), the *Corporations Act 2001* (Cth) does not stipulate a timeframe (ie 90 days).
81 *Corporations Act 2001* (Cth) s 1317AAD(2)(e).
82 Ibid s 1317AA(3).
83 *PIDA 2013* (Cth) ss 13, 19.
84 Ibid s 13(2).

may be granted for a reprisal and may grant, for example, compensation,[85] an injunction, an apology,[86] or reinstatement where the reprisal involved dismissal.[87]

Confusingly, when viewed in the broader context of whistleblower protections, *PIDA* protects four forms of 'public interest disclosure': internal disclosures, external disclosures, emergency disclosures and legal practitioner disclosures.[88] These four public interest disclosures are distinct from public interest disclosures under the *Corporations Act* (which, for clarity we call private sector public interest disclosures). As outlined above, a private sector public interest disclosure is a discrete form of protected disclosure, separate to emergency disclosures, internal disclosures, and so on. Conversely, under *PIDA*, *all* forms of protected disclosure are 'public interest disclosures' including, for example, emergency disclosures and internal disclosures.

1 General Principles and Internal Disclosures

Reminiscent of the private sector whistleblower laws, *PIDA* protections hinge on the identity of the whistleblower, as well as the subject, recipient, and content of the disclosure. Only the disclosure of 'disclosable conduct' by a 'public official' to a specified recipient will qualify for protection under *PIDA*. Of these criteria, disclosable conduct is the most complex.

'Public official' is given an expansive definition in section 69 of *PIDA* in the form of an extended table. Public officials include Australian Public Service employees, members of the Defence Force, contracted service providers for Commonwealth contracts, and a range of individuals holding statutory office or performing statutory functions. *PIDA* is narrower than the *Corporations Act*, however, in not extending whistleblower protections to the relatives, dependents or spouses of public officials. Thus, a public sector whistleblower should be wary of making disclosures even to close family – for their own sake, and because subsequent disclosures by the family member would not be protected.

The scope and operation of *PIDA* protections turn on the concept of 'disclosable conduct'. 'Disclosable conduct' must be engaged in by an agency, public official, or contracted service provider for a Commonwealth contract.[89] 'Agency' is given a broad scope under *PIDA* and is defined as a government department, an Executive Agency or a prescribed authority.[90] 'Prescribed authority' in turn refers to a vast range of government agencies, including: statutory agencies, Commonwealth authorities and companies, Ombudsmen, federal courts, the AFP, the Australian Security Intelligence Organisation ('ASIO'), ASIS, ASD, ONA, IGIS, and any other body established by Commonwealth law and prescribed as such by *PIDA*.[91]

85 Ibid s 14.
86 Ibid s 15.
87 Ibid s 16.
88 Ibid ss 25, 26(1).
89 Ibid ss 29(1)(a)–(c).
90 Ibid ss 8 (definition of 'agency'), 71.
91 Ibid s 72.

The notable exception is Royal Commissions, which are excluded from the definition of prescribed authority.[92]

Disclosable conduct is defined in section 29 to include 'conduct engaged in by a public official that involves, or is engaged in for the purpose of, the public official abusing his or her position as a public official' as well as, 'conduct engaged in by a public official that could, if proved, give reasonable grounds for disciplinary action against the public official'.[93] In addition to these terms, *PIDA* includes a table which sets out ten additional categories of disclosable conduct, including conduct which:

- contravenes Australian or applicable foreign law;
- perverts or attempts to pervert the course of justice;
- is engaged in for corrupt purposes;
- constitutes maladministration or an abuse of public trust;
- results in the wastage of public money or property; or
- unreasonably results in or increases a risk of danger to the health and safety of persons.[94]

Some conduct is specifically excluded from the scope of disclosable conduct under *PIDA*. First, *PIDA* excludes disclosures based on mere disagreement with conduct or policy from the definition of disclosable conduct. This includes conduct that relates to a policy, or proposed policy, of the Commonwealth government, or a past, present or proposed action taken by a Minister, the Speaker of the House of Representatives or the President of the Senate. The amounts, purposes or priorities of expenditure related to a policy or a proposed policy are also excluded from the scope of disclosable conduct.[95]

Second, conduct relating to a federal court or tribunal is subject to specific exclusions.[96] For instance, such conduct cannot amount to disclosable conduct unless it is of an administrative nature or relates to the management or hearing of matters before the court or tribunal.[97]

Finally, conduct engaged in by an intelligence agency, or a public official belonging to an intelligence agency, that is within the proper performance or exercise of the agency's functions or powers, is also excluded from the definition of disclosable conduct.[98] This exclusion captures Witness K's disclosure of the government sanctioned actions of ASIS operatives in Timor-Leste. It may also be relevant to the disclosure of the ASD memo to Smethurst, insofar as that leak contained information relating to the conduct of the ASD.

---

92 Ibid s 72(3).

93 Ibid s 29(2). 'Disciplinary action' is not defined in *PIDA 2013* (Cth). 'Public official' means one of the individuals listed in column 1 of the table contained in section 69.

94 Ibid s 29(1).

95 Ibid s 31.

96 Ibid s 32(1).

97 Ibid s 32(d).

98 Ibid s 33.

2 Internal Disclosures

A public official may make an internal disclosure to their supervisor, or an authorised internal recipient, provided that the disclosed information tends to show (or the discloser believes on reasonable grounds that it tends to show) disclosable conduct.[99] If the whistleblower reasonably believes the disclosure should be investigated, authorised recipients include the Ombudsman and other similarly empowered investigative agencies.[100] Disclosures of conduct relating to the Ombudsman or IGIS may be disclosed to an authorised officer within those bodies.[101]

3 Internal Disclosures of Intelligence Information

Internal disclosures are the only available form of protected disclosure with respect to 'intelligence information' or conduct relating to intelligence agencies, including ASIS. One effect of this is that the 'public interest' – a critical feature in determining whether external disclosures are protected under *PIDA* and the *Corporations Act* – is irrelevant to the protection (or otherwise) of intelligence disclosures. It must also be recalled that the proper performance or exercise of an intelligence agency's functions or powers is excluded from the scope of disclosable conduct and therefore cannot be the subject of a protected disclosure, internal or otherwise. Not only did Witness K's disclosure concern intelligence information and operations (excluding the possibility of a protected external, emergency, or legal advice disclosure), it concerned conduct performed with proper authority, excluded from the scope of disclosable conduct.

Intelligence information is defined in section 41 of *PIDA* to include: information that could be used to identify a current or former ASIO employee, affiliate, or a source of information from an intelligence agency; information that originates or is received from an intelligence agency, or from a foreign authority with similar functions to an intelligence agency; and information concerning certain technologies or operations.[102]

Beyond this expected scope of intelligence information, the term also includes 'sensitive law enforcement information', defined broadly as 'information the disclosure of which is reasonably likely to prejudice Australia's law enforcement interests'.[103] This extends the scope of intelligence information considerably, taking it beyond traditional intelligence and into policing. 'Sensitive law enforcement information' is elaborated in section 41 of *PIDA*. It includes national and international efforts relating to law enforcement, the protection of informants and witnesses, the protection of certain technologies and intelligence handling methods, and 'ensuring that intelligence and law enforcement agencies are not discouraged from giving information to a nation's government and government agencies'.[104]

---

99 Ibid s 29(1) item 1.
100 Ibid s 34 item 1.
101 Ibid s 34 items 3–4.
102 Ibid s 41(1).
103 Ibid s 41(2).
104 Ibid.

Of these components, information relating to national law enforcement efforts is particularly striking in its breadth and would be capable of capturing material outside the traditional scope of 'intelligence' information.

Disclosable conduct, such as conduct beyond an intelligence agency's powers, may be disclosed to an authorised officer within the intelligence agency.[105] It may also be disclosed to the IGIS if the whistleblower reasonably believes that the disclosure should be investigated, as happened in the case of Witness K. These are the only avenues for the protected disclosure of intelligence information. Disclosable conduct relating to an intelligence agency may only be disclosed to an investigative agency (other than the IGIS or Ombudsman) where two criteria are met. First, the investigative agency must be empowered to investigate a disclosure relating to the conduct of an intelligence agency and, second, the disclosure must not contain intelligence information.[106]

It is unsurprising that there is no provision for intelligence information to be communicated to the media, and subsequently to the public, in the form of a protected disclosure, though the scope of this exclusion is vitally important to the maintenance of integrity and accountability in the national security sphere. The limited availability of even internal disclosures for intelligence information is a further cause for concern, and we return to these issues below.

4 External Disclosures

External public sector disclosures may be made to any person other than a foreign public official.[107] This includes journalists, extending to non-professional journalists who cannot receive a protected private sector public interest disclosure under the *Corporations Act*. In brief, the external disclosure of necessary information will be protected, provided that a preceding internal disclosure was inadequate and the further disclosure is not contrary to the public interest.

The scope of information which may be disclosed in a protected external disclosure is strictly limited. Information must tend to show disclosable conduct, or the discloser must believe as much on reasonable grounds.[108] Moreover, the disclosure must not contain information more than reasonably necessary to identify the disclosable conduct, must not include intelligence information, and must not relate to an intelligence agency.[109]

To qualify for protection, the information must first have been disclosed internally. There is no set time period that the whistleblower must allow between the internal and external disclosure (unlike under private sector public interest disclosure rules). Rather, the whistleblower must believe on reasonable grounds that the internal investigation was inadequate or that the internal investigation was not conducted within prescribed time limits. This requirement implies that a

105 Ibid s 34 item 2.

106 Ibid.

107 Ibid ss 8 (definition of 'foreign public official'), 26(1) item 2. *PIDA 2013* (Cth) adopts the definition of 'foreign public official' contained in section 70.1 of the *Criminal Code Act 1995* (Cth).

108 *PIDA 2013* (Cth) s 26(1) item 2.

109 Ibid ss 26(1) item 2, 33.

whistleblower would need to wait a 'reasonable' period of time after their internal disclosure before making an external disclosure. McBride, for instance, was of the view that a reasonable time had elapsed between his internal disclosure and his communication to the ABC. *PIDA* deems certain internal disclosures to be adequate (that is, incapable of being *inadequate*) – including all disclosures that involve action by a Minister, the Speaker of the House of Representatives, or the President of the Senate[110] – thereby closing off the opportunity for a protected external disclosure.

External disclosures under *PIDA* are subject to a public interest test. Whilst private sector public interest disclosures require that the whistleblower has reasonable grounds to believe that the disclosure is *in* the public interest,[111] an external disclosure under *PIDA* must, 'on balance', *not be contrary to* the public interest.[112] Not only is the test framed in the negative, it also involves an objective assessment rather than focusing on the whistleblower's reasonable belief.

The public interest is a notoriously vague concept.[113] In determining whether a disclosure is contrary to the public interest, *PIDA* directs that regard must be had to a range of considerations. These include:

- the promotion of public sector integrity and accountability;
- that disclosures should be properly investigated and dealt with;
- the nature and seriousness of the conduct;
- Cabinet secrecy;
- whether the communication was in confidence with foreign governments or authorities;
- potential impacts on the administration of justice; and
- risks to Commonwealth security, defence, international relations or relations with a state or territory.[114]

These considerations prompt decision-makers to weigh the need for accountability and secrecy in assessing the public interest. Notably, accountability and integrity are mentioned generally, aligning with the broad purposes of the whistleblower protection framework. There is no specific reference, however, to *public* accountability or democratic concerns.[115] Moreover, the final consideration is particularly broad. It is conceivable that any negative story based on a leak that damages the reputation of a Commonwealth, state or territory government risks damaging 'relations', let alone more specific stories about Australia's international relations or trade.

---

110 Ibid s 26(2A).

111 *Corporations Act 2001* (Cth) s 1317AAD(1).

112 *PIDA 2013* (Cth) ss 26(1) item 2, 26(3).

113 See, eg, Chris Wheeler, 'The Public Interest We Know It's Important, But Do We Know What It Means?' (2006) 48 *Australian Institute of Administrative Law Forum* 12; Senate Standing Committee on Constitutional and Legal Affairs, Parliament of Australia, *Freedom of Information* (Report, 1979) 64–7 [5.20]–[5.30]; Ireland-Piper and Crowe (n 12) 363; Senate Select Committee on the Future of Public Interest Journalism, Parliament of Australia, *Report* (Report, February 2018) 2 [1.8].

114 *PIDA 2013* (Cth) ss 26(3)(ad), (ae)(a)(i)–(vi).

115 We return to a discussion of 'the public interest' in Part III(C)(4).

5 Emergency Disclosures and Legal Advice

Emergency disclosures may be made to any person (other than a foreign public official) and will be protected if the discloser believes on reasonable grounds that the information concerns a substantial, imminent danger to the health and safety of persons or the environment. However, as with all external disclosures, the extent of the information must be no greater than necessary to highlight the danger and must not include intelligence information.[116] In addition to these requirements, emergency disclosures must be justified by exceptional circumstances. If an internal disclosure has been made, exceptional circumstances must justify any further disclosure before the completion of an investigation. If no internal disclosure was made, there must be exceptional circumstances to justify this failure.[117]

Legal practitioner disclosure is protected under *PIDA*, in similar terms to the *Corporations Act*. A disclosure to an Australian legal practitioner is permitted for the purpose of obtaining legal advice or professional assistance in relation to the whistleblower having made, or proposing to make, a disclosure. If they knew (or ought reasonably to have known) that the information had a protective security classification, the legal practitioner must hold the appropriate level of security clearance. This was why the IGIS directed Witness K to consult Collaery – a security cleared barrister and, incidentally, former Attorney-General of the ACT. Furthermore, the information must not consist of, or include, intelligence information – a requirement that Witness K did not comply with.[118]

C Protected Disclosures to the Media: Summary and Critique

A thicket of technical rules surrounds public and private sector disclosures. This section distils when a whistleblower may be permitted to disclose information to a journalist or media organisation and identifies five key areas for reform.

1 Option 1: An Emergency Disclosure

The emergency disclosure provisions of the *Corporations Act* and *PIDA* provide a limited avenue by which a whistleblower may disclose information to the media. This form of disclosure is only available where a whistleblower has reasonable grounds to believe that the information concerns a substantial and imminent danger to the natural environment or to the health or safety of one or more persons. The extent of the information disclosed, however, must be no greater than necessary to highlight the danger.[119] Private sector whistleblowers must have made an earlier disclosure and provided notice of the intention to make a further disclosure. They are also restricted in disclosing to journalists who meet the statutory definition.[120] Public sector whistleblowers may make a disclosure to anyone (other than a foreign

116 *PIDA 2013* (Cth) s 26(1) items 3–4.
117 Ibid s 26(1) item 3.
118 Ibid s 26(1) item 4.
119 Ibid s 26(1) item 3; *Corporations Act 2001* (Cth) s 1317AAD(2)(e).
120 *Corporations Act 2001* (Cth) s 1317AAD(2).

public official) but will need to demonstrate exceptional circumstances, regardless of whether they have already made an internal disclosure.[121]

2 Option 2: An External Public Interest Disclosure

Recognising a clear role for whistleblower disclosures to the media, the *Corporations Act* provides a specific, more widely available, framework for disclosures to professional journalists. To summarise: if at least 90 days has passed since making an internal disclosure, and the whistleblower lacks reasonable grounds to believe that action is being taken to address the matter raised, then they may notify the regulated entity of their intention to speak to a 'journalist' (as defined in the Act), and proceed to do so. The whistleblower must, however, have reasonable grounds to believe that the disclosure is in the 'public interest'. If these criteria are met, this disclosure will attract the considerable protections offered under the *Corporations Act*. The extent of the information disclosed, however, must be no greater than necessary to inform the journalist of the misconduct or improper state of affairs.[122]

PIDA regulates disclosures to the media primarily through the external disclosure rules. As under the *Corporations Act*, the scope of information that may be externally disclosed under *PIDA* is strictly limited. It must tend to show 'disclosable conduct', or the discloser must believe on reasonable grounds that the information tends to show such conduct;[123] and it must only contain information reasonably necessary to identify the disclosable conduct. It is unknown whether the '[h]undreds of pages of secret defence force documents'[124] in McBride's report complied with this requirement – a question that may be determined in the course of his trial.[125] Where action has been taken by a Minister, the Speaker of the House of Representatives, or the President of the Senate in response to an internal disclosure, any external disclosure will not be protected, as the handling of any such internal disclosure is deemed to be adequate by *PIDA*.[126]

Public sector whistleblowers must allow a 'reasonable' period of time after their internal disclosure before speaking to a journalist. The disclosure must not, however, be contrary to the public interest 'on balance'.[127] Certainly, any conditions of confidentiality, security classification, or relevance to international relations could indicate that external disclosure is not in the public interest.

---

121 *PIDA 2013* (Cth) s 26(1) item 3.
122 *Corporations Act 2001* (Cth) s 1317AAD(1)(g).
123 *PIDA 2013* (Cth) s 26(1) item 2.
124 Oakes and Clark (n 23).
125 Paul Johnson, 'Nick Xenophon Attacks Government over Afghan Files Whistleblower David McBride on Q+A', *ABC News* (online, 23 June 2020) <https://www.abc.net.au/news/2020-06-23/nick-xenophon-afghan-files-david-mcbride-witness-j-whistleblower/12382154>.
126 *PIDA 2013* (Cth) s 26(2A).
127 Ibid s 26(3).

3 Recognising the Legitimacy of Disclosures to a Journalist

Rather than create a targeted framework for disclosures to professional journalists, *PIDA* regulates all external disclosures – that is, to any person – by a single set of rules. Hence, terms such as 'journalist', 'journalism' and 'media' do not appear in *PIDA*. In this way, the federal government avoided the thorny task of defining these contested and dynamic terms. This stands in contrast to the *Corporations Act*, as well as public sector whistleblower laws in Queensland, New South Wales ('NSW'), Western Australia ('WA'), South Australia ('SA') and the ACT. Each of those schemes establish frameworks for protected external disclosures to a targeted set of recipients, including journalists.[128]

PIDA offers wider protection than the *Corporations Act* by allowing for public interest disclosures to all journalists and to anyone else (other than a foreign public official). This breadth and avoidance of technical definitions are commendable aspects of the framework. Whilst this article is focused on disclosures to journalists, future reform should consider these advantages. In particular, expanding protection for external disclosures under the *Corporations Act* (and certain state and territory schemes) to *all* recipients deserves consideration.

On the other hand, by not creating a targeted framework for disclosures to journalists, *PIDA* fails to articulate the legitimate role served by media disclosures. This subtle distinction reflects a broader trend throughout *PIDA* of focusing on principles of accountability, integrity and secrecy, without recognising the specific role of the media in achieving these aims. Thus, it is easier to see disclosures to journalists as illegitimate, unnecessary or extreme within the regime created by *PIDA*. A narrowing of *PIDA*'s protections for external disclosures would, however, make little sense. Rather, the provisions could be simply amended to recognise the legitimacy of media disclosures by identifying professional journalists as an example of a recipient of a protected external disclosure, even in a note to the relevant provisions.

4 Grappling with the 'Public Interest'

Both private and public sector disclosures to the media are constrained by an assessment of the 'public interest': what is in the public interest, and what is contrary to it. 'Public interest' is a phrase commonly used in legislation, but never strictly defined. In *Hogan v Hinch*, the High Court observed that a determination of the public interest will be a context-specific exercise, impacted by the subject matter, scope and purpose of the statute in which the phrase appears, with regard given to the 'larger constitutional and legal context which informs the interpretation of the statute', including the effect on the principles of open justice and free speech.[129]

---

128 *Corporations Act 2001* (Cth) s 1317AAD; *Public Interest Disclosure Act 2012* (ACT) s 27; *Public Interest Disclosure Act 1994* (NSW) s 4 (definition of 'journalist'), s 19; *Public Interest Disclosure Act 2010* (Qld) s 20(4); *Public Interest Disclosure Act 2018* (SA) s 4 (definition of 'journalist'), s 6; *Public Interest Disclosure Act 2003* (WA) s 7A. Notably, only the NSW and Queensland Acts share a common definition of 'journalist'; the remaining jurisdictions adopt distinct definitions of this core term.

129 (2011) 243 CLR 506, 536–7 [31]–[32] (French CJ).

The driving 'public interests' served by the whistleblower laws are accountability and integrity; though, as discussed in Part II, these objectives have related economic, democratic, and other benefits. In the *Corporations Act*, where 'public interest' is not expanded upon, it appears that various interests will be assessed and weighed on a case-by-case basis. *PIDA*, however, articulates a range of 'public interests' that weigh for and against disclosure and secrecy. A public interest assessment under *PIDA* could be expected to seek both accountability *and* secrecy on a case-by-case basis, thereby arguably favouring the *internal* resolution of complaints over external disclosures. Again, the failure to recognise the legitimacy of media disclosures or recognise *public*, democratic accountability as a specific consideration supports this interpretation of the provisions.

A striking difference between the public interest tests under the *Corporations Act* and *PIDA* is that the former is framed positively: the whistleblower must have reasonable grounds to believe the disclosure is *in* the public interest. Conversely, *PIDA*'s negatively framed public interest test requires that the whistleblower has reasonable grounds to believe that the disclosure is *not contrary to* the public interest. Both tests are, of course, similar. Semantically, the difference is the slim distinction between a positive and a double negative. A court undertaking a contextual interpretation of 'the public interest' and engaging in the balancing exercise demanded by such a test may come to the same conclusion under either approach. However, the distinction, however slight, remains important.

First, there is an attractive clarity to a positive test over one that rests on a double negative.

Second, on its face, the negatively framed test sets a lower standard of proof. A disclosure with a neutral relationship to the public interest would be permitted under *PIDA* (as not being contrary to the public interest), but would not meet the requirement of being *in* the public interest under the *Corporations Act*. Further, close consideration reveals pertinent advantages of the positively framed test under the *Corporations Act*.

By focusing on whether and how the disclosure may be *in* the public interest, a positively framed test is better suited to achieving the purposes of the whistleblower framework as a whole. Determining whether a disclosure is contrary to the public interest requires the interrogation of the negative consequences of the disclosure, that is, identifying and focusing on the ways in which the disclosure threatened or undermined the public interest. This approach places the positive consequences of the disclosure (how it served the public interest) on a secondary footing. A positively framed test gives primary focus to how the disclosure enhanced the public interest, including in accountability and integrity – the core aims of whistleblower laws.

The importance of this distinction is demonstrated by considering McBride's disclosure. Misconduct and a 'code of silence' within the ADF is a matter of keen public interest, raising important questions of integrity and accountability. But was his disclosure *not contrary to* the public interest? Whilst the alleged conduct was serious – to the point of alleged war crimes and a deliberate cover-up – the disclosed materials were security classified. Their communication to ABC journalists had the potential to damage security, defence and international relations. The same could be said of the disclosures by Witness K and Wilkie. Those disclosures were

decidedly in the public interest, but also contrary to the public interest as elaborated under *PIDA*.

Importantly, *PIDA* requires that public interest be assessed 'on balance'. This shapes the application of that test and means it may operate very similarly to the positively framed test under the *Corporations Act*. Whether the difference between the positively and negatively framed tests is significant or illusory, we submit that framing the test positively would enhance clarity and consistency across the whistleblower protection framework and ensure primary focus is given to the core purposes of that framework, namely, accountability and integrity.

5 Inconsistency and Scope: Disclosable Matters/Conduct

The scope of whistleblower protections hinges on the definitions of 'disclosable matter' in the *Corporations Act* and 'disclosable conduct' in *PIDA*. The definitions of these two terms are subject to important differences. Generally speaking, disclosable matter is wider in scope than disclosable conduct. Both Acts contain a catch-all provision. Under the *Corporations Act*, this extends to conduct which the discloser suspects on reasonable grounds to concern an 'improper state of affairs or circumstances';[130] whereas for *PIDA*, this rests on abuse of power and grounds for disciplinary action against a public official.[131] The phrase 'improper state of affairs' in the *Corporations Act* extends beyond abuses of power and, arguably, conduct which could prompt a form of disciplinary action; however, it overlaps with the further categories of disclosable conduct in *PIDA*, including conduct which constitutes maladministration, an abuse of public trust, misconduct in scientific research, and wastage of public money.

The focus on the discloser's state of mind in disclosable matter is absent from disclosable conduct in *PIDA*. Rather, whether the whistleblower *believes* the information to reveal disclosable conduct will be relevant to determining whether the disclosure is protected, instead of defining disclosable conduct itself. Similarly, information about misconduct or an improper state of affairs that merely 'relates to' a regulated entity amounts to a disclosable matter under the *Corporations Act*.[132] In contrast, disclosable conduct under *PIDA* must be 'engaged in' by an agency, public official, or contracted service provider.[133]

The distinctions and inconsistencies between how disclosable matter and conduct are defined prompted Brown to describe the schemes as 'almost the reverse of each other, but for no good reason'.[134] This inconsistency has the potential to create confusion, which has been avoided in many jurisdictions through the adoption of the same basic principles to guide both public and private sector disclosures.[135] Simple consistency could represent an advancement in federal whistleblower protections. This could be achieved, first, in the adoption of a positively framed

130 *Corporations Act 2001* (Cth) s 1317AA(4).
131 *PIDA 2013* (Cth) s 29(2).
132 *Corporations Act 2001* (Cth) s 1317AA(4).
133 *PIDA 2013* (Cth) s 29(1).
134 Brown (n 2) 16.
135 Ibid.

public interest test across public and private sector whistleblower laws (discussed above). Consistency could also be enhanced by incorporating the broader standard of 'improper state of affairs or circumstances' into *PIDA*.

In a 2010 Resolution, the Council of Europe urged the inclusion of a comprehensive definition of protected disclosures which would encompass serious human rights violations.[136] At present, information that relates to a human rights violation is not necessarily recognised as a disclosable matter/conduct (especially in the intelligence sphere). Preventing serious human rights violations is a key aspect of integrity and accountability, so to extend disclosable matters/conduct in this respect would assist the whistleblower protections to achieve their core purpose.

Perhaps counter-intuitively, Brown's empirical study indicated that widening the definition of 'disclosable conduct' to include human rights violations would not correspond with an increase in public complaints or allegations.[137] From a government and organisational perspective, the successful internal resolution of issues depends upon the effectiveness of whistleblowing channels. If individuals feel a human rights violation may not be disclosable they may fail to report it, sacrificing accountability and integrity; or they may report it improperly, such as by going to the media without considering whether internal channels would be more effective or appropriate.

There exists a major impediment to extending the definitions of disclosable matter and conduct to include violations of human rights. Unlike the European Union, Australia lacks national codified rights protection in the form of a Bill or Charter of human rights. Thus, the term 'human rights violation' lacks clear legal scope. This could render the extension of disclosable conduct/matter in this respect vague and difficult under federal law.[138]

6 A Gap in Protections: Intelligence Disclosures

Australia's intelligence frameworks are effectively exempt from the form of accountability presented by external, and even emergency, protected disclosures. First, conduct that amounts to the proper performance or exercise of the agency's functions or powers is excluded from the definition of disclosable conduct, which rules out the prospect of an internal protected disclosure.[139] Such conduct may even involve contravention of international law, as in the disclosures by Witness K and McBride; or be a matter of grave public importance and interest, such as Wilkie's report on Iraqi WMDs. Second, intelligence information – which includes certain law enforcement information – may not form the basis of any protected disclosure except an internal one.

---

136 Council of Europe, Parliamentary Assembly, *Protection of 'Whistle-Blowers'*, Res 1729, 17th sitting, 29 April 2010, 1 [6.1.1].

137 Brown et al (n 17) 48.

138 We note that in Australian jurisdictions with human rights Acts – Victoria, the ACT and Queensland – it would be strongly arguable that whistleblower protections should extend to disclosures of serious violations of human rights.

139 *PIDA 2013* (Cth) s 33.

The exclusion of most intelligence disclosures from whistleblower protections means that persons employed, contracted, or engaged by Australia's vast intelligence and law enforcement apparatus lack adequate protection. The principles of integrity and accountability, which inform the private and public sector whistleblowing regimes, are equally relevant to intelligence organisations. These basic principles, as well as the controversies surrounding the disclosures by Witness K and others, underscore the need for a clear, effective, and widely available framework for *internal* disclosures, encompassing conduct that amounts to the proper performance or exercise of the agency's functions or powers but nonetheless meets the criteria for disclosable conduct. An effective internal disclosure regime could have avoided the further, external disclosures made by Witness K, McBride, and others.

A more challenging set of issues is presented by the prospect of external disclosures relating to intelligence information and the conduct of Australia's intelligence agencies. At present, the external disclosure of intelligence information (including certain law enforcement information) will leave the whistleblower vulnerable to reprisals, victimisation, extended court proceedings, and criminal sanction.[140]

There is an inescapable tension between the need for secrecy within Australia's security agencies and the democratic imperative for transparency and accountability that underpins the media's role as watchdog. In recent years, legislators have tended to increase the scope and scale of those agencies' powers while curbing the ability of news organisations to hold them to account.

It is reasonable to assume that people in Australia's intelligence agencies are just as capable as anyone else of breaking the law, behaving corruptly or dishonestly, abusing public trust, falsifying evidence, or wasting public money – all behaviours that qualify as 'disclosable conduct'.[141] That behaviour could also take place outside sensitive security operations – such as in administration or training – so that disclosure would not necessarily expose sensitive information. Even in cases which involve security operations – as in the McBride disclosures – there may be a compelling public interest in disclosure. Furthermore, given the wide scope and scale of the powers vested in security agencies, there is a greater than usual public interest in ensuring they behave ethically and lawfully.

The Wilkie affair highlights these legislative and political complexities, as well as the centrality of 'the public interest' in regulating the consequences faced by

140 The external disclosure of intelligence information is conduct that may satisfy the elements of a number of offences, including: unauthorised communication, recording and dealing with information (*Australian Security Intelligence Organisation Act 1979* (Cth) ss 18–18B); unauthorised disclosure of information relating to a special intelligence operation (*Australian Security Intelligence Organisation Act 1979* (Cth) s 35P); communicating, dealing with, and recording ASIS, Australian Geospatial-Intelligence Organisation, ASD or Defence Intelligence Organisation information (*Intelligence Services Act 2001* (Cth) ss 39–40M); various secrecy of information offences in division 122 the *Criminal Code Act 1995* (Cth); and various espionage offences in division 91 of the *Criminal Code Act 1995* (Cth).

141 In this context, it is important to note the various inquiries into police corruption that have occurred across Australia, including the Kennedy Royal Commission in WA, the Fitzgerald Inquiry in Queensland, and the Wood Royal Commission in NSW.

even intelligence whistleblowers. Wilkie believes that he escaped prosecution for disclosing ONA reports to Laurie Oakes because the government sought to avoid the political cost of prosecuting him.[142] In this sense, the Attorney-General's personal determination of 'the public interest' may have saved Wilkie from a jail term. A calculation of political cost and public interest can similarly be observed in the belated charges brought against Witness K and Collaery, while the public criticism of the AFP raids may be behind a similar calculation in dropping the investigations against Dan Oakes and Annika Smethurst. Nonetheless, the prosecution against McBride continues despite public interest concerns being raised by former NSW Director of Public Prosecutions Nicholas Cowdery and the Senate Environment and Communications References Committee.[143]

This raises the question of whether the protection of intelligence whistleblowers should rest with the Attorney-General alone or be regulated more closely through legislation. The apparent inconsistency and lack of transparency which characterises the case-by-case determinations of successive Attorneys-General suggest that the introduction of an avenue for external disclosures of intelligence information *in the public interest* would be appropriate. Any such disclosures would need to adhere to a high threshold of public interest and be subject to a rigorous process.

7 Is Law Enforcement Information Intelligence Information?

Wilkie's actions highlight the tension between the democratic accountability that disclosing information to journalists can provide and the secrecy that the intelligence agencies require in order to function effectively. Applying a blanket exclusion to intelligence information from the scope of protected external disclosures significantly erodes accountability by exposing legitimate whistleblowers to serious reprisals and criminal penalties. The scope of any exclusions must, therefore, be narrowly constrained and justified. Information relating to operatives and operations generally falls within the central ambit of this exclusion.

The same cannot be said of information 'reasonably likely to prejudice Australia's law enforcement interests'.[144] Accountability and integrity in Australia's law enforcement agencies has long been controversial, giving rise to some of the most infamous cases of whistleblowing. Those cases have in turn triggered inquiries and, often, urgently needed reforms. A prominent example can be found in the ABC's reporting, by Chris Masters and Phil Dickie from *The Courier Mail*, on corruption in the Queensland Police Force. As a result of their work (which relied heavily on anonymous sources), the government set up the Fitzgerald Inquiry that ultimately led to the imprisonment of the Police Commissioner Terry Lewis and recommended a series of far-reaching reforms, from disbanding the Police Special Branch to establishing critical new systems of oversight.

---

142 Greste (n 21) 232–3.

143 Christopher Knaus, 'Commonwealth Prosecutors Wrong on Witness K Case, Former NSW DPP Says', *The Guardian* (online, 1 April 2021) <https://www.theguardian.com/australia-news/2021/apr/01/commonwealth-prosecutors-wrong-on-witness-k-case-former-nsw-dpp-says>; *Inquiry into Press Freedom Report* (n 1) xii.

144 *PIDA 2013* (Cth) s 41(2).

In 2013, one of the whistleblowers/sources, former police officer Nigel Powell, explained why he had been deterred from pursing internal channels and had instead chosen to speak to the media:

> You will have an official body saying, 'you better be pretty sure of what you got, because if we find you are vexatious and you don't have a firm basis for what you are saying, then you could be prosecuted' …
>
> Now, what was I saying then – had I actually seen corruption take place? No.
>
> Had I had actual evidence of money crossing hands? No. I had my suspicions, which no longer sounds like it would be enough to make a complaint.
>
> So I would be in exactly the same position, I wouldn't be going to the official body I should be going to, I would be going to the media.[145]

The inclusion of law enforcement information in the definition of intelligence information reflects a troubling creep in the scope of information excluded from one of the most important and demonstrably effective methods of external oversight. It therefore compounds the secrecy inherent in the sector and attendant accountability deficits.[146] In light of these issues, Brown has argued that the statutory definition of intelligence information should be revised 'to actually make sense'.[147] Such an amendment would not need to open *all* intelligence information to the possibility of external disclosure. Rather, it would revise the existing definition to ensure that only the core of intelligence information was subject to a blanket exclusion, with other information subject to the usual rigorous requirements for protected disclosures, including a public interest test.

IV SOURCE PROTECTION

Once a whistleblower discloses information to a journalist, they become that journalist's 'source'. In this Part, we examine the ethical and legal protections that exist for confidential journalistic sources, and how they overlap with federal whistleblower protections.

If a whistleblower complies with legal requirements, under either the *Corporations Act* or *PIDA,* they will enjoy the substantial protections provided under those respective schemes. This includes protection for their anonymity, from legal action, and from victimisation (under the *Corporations Act*) or reprisals (under *PIDA*).

It may be, however, that the whistleblower does not comply with legal requirements; or their compliance is uncertain. A source may be confident that their disclosure meets the public interest test, but their employer disagrees. An

145 Amy Remeikis, 'Moonlight Rising: Fitzgerald Whistleblower Questions Reforms', *Brisbane Times* (online, 5 July 2013) <https://www.brisbanetimes.com.au/national/queensland/moonlight-rising-fitzgerald-whistleblower-questions-reforms-20130704-2pf0w.html>.

146 See generally Keiran Hardy and George Williams, 'Terrorist, Traitor, or Whistleblower: Offences and Protections in Australia for Disclosing National Security Legislation' (2014) 37(2) *University of New South Wales Law Journal* 784.

147 Brown (n 2) 16.

organisation may suspect a whistleblower has disclosed more information than is strictly necessary and, in the process, voided their legal protection. There may be a similar dispute over whether exceptional circumstances existed to support an emergency disclosure. Or, a source may simply be afraid that making an internal complaint would expose them to danger, because they do not trust the mechanisms for protecting their identity. Certainly, where the disclosure concerns information that is security classified, commercial in confidence, trade secrets, or relates to national security or law enforcement, questions are likely to be raised over whether it could possibly be the subject of a protected external disclosure.

In light of this uncertainty, a whistleblower speaking to a journalist may be strongly concerned for their future. They may be risking not only reprisal or victimisation, but criminal conviction. They are therefore likely to insist on confidentiality. What assurances or protections is a journalist in a position to offer?

A Ethical Obligations and the Free Press

The US newspaper magnate, William Randolph Hearst, famously said, '[n]ews is something somebody doesn't want printed; all else is advertising'.[148] Hearst was underlining the essential watchdog role that journalism plays, by exposing information that the powerful, in particular, would rather keep hidden. In those circumstances, journalists typically rely on sources who may be unwilling to come forward if they believed their identity would be exposed.

The ethical obligation to protect sources is a central principle in almost every media code of conduct around the world. Australia's media industry union, the Media Entertainment and Arts Alliance, says that journalists should

> [a]im to attribute information to its source. Where a source seeks anonymity, do not agree without first considering the source's motives and any alternative attributable source. Where confidences are accepted, respect them in all circumstances.[149]

The BBC's Editorial Guidelines state:

> We must ensure when we promise anonymity that we are in a position to honour it, taking account of the implications of any possible court order demanding the disclosure of our unbroadcast material. When anonymity is essential, no document, computer file, or other record should identify a contributor or source.[150]

The AFP raids of June 2019 took direct aim at these principles of journalistic confidentiality. In their aftermath, representatives from Australian media united in affirming their commitment to source protection: they would not give up their confidential sources, even if it meant facing legal consequences themselves.[151] This

148 Dana Magill, 'Hearst, William Randolph (1863–1951)' in Rodney P Carlisle (ed), *The Encyclopedia of Politics: The Left and the Right* (Sage Publications, 2005) vol 1, 679, 680.

149 'MEAA Journalist Code of Ethics', *Media, Entertainment and Arts Alliance* (Web Page) <https://www.meaa.org/meaa-media/code-of-ethics/>.

150 'Section 6: Fairness to Contributors and Consent – Guidelines', *British Broadcasting Corporation* (Web Page) <https://www.bbc.com/editorialguidelines/guidelines/fairness/guidelines#anonymity>. See also 'Code of Conduct', *National Union of Journalists* (Web Page) <https://www.nuj.org.uk/about/nuj-code/>.

151 See, eg, National Press Club, 'NPC Statement on the AFP Raids' (Media Release, 5 June 2019); Ben Fordham, 'Ben Fordham Faces AFP Raids After Source Reveals Confidential Information', *2GB* (online,

statement boldly recognised the very real prospect of severe fines or imprisonment for a journalist seeking to protect a source.

B Shield Laws and Warrants

Whilst journalistic ethics offers robust protection for sources, the law does not. The clearest protection arises in the form of 'shield laws', which operate in every Australian jurisdiction except Queensland.[152] Shield laws aim to ensure that a journalist or their employer is not compellable to disclose the identity of a confidential source in court. The existence of shield laws is a form of legislative acknowledgement of the importance of source protection for journalists. They reassure journalists that the courts are cognisant of the importance of source confidentiality. If Smethurst, for example, was prosecuted for publishing classified government material, shield laws would help her keep her sources secret. However, the shield is thin.[153] A court may order that shield protection does not apply if it is satisfied that 'the public interest in the disclosure of evidence of the identity of the informant' outweighs two countervailing considerations. First, any likely adverse effect of the disclosure on the source (or any other person). Second, 'the public interest in the communication of facts and opinion to the public by the news media and, accordingly also, in the ability of the news media to access sources of facts'.[154] Together these provisions identify the competing 'public interests' at stake, namely, the administration of justice and press freedom.

Federal shield laws protect journalists' sources in the courtroom, as well as in the pre-trial (curial) stages of a civil or criminal proceeding.[155] But they do not

---

4 June 2019) <https://www.2gb.com/ben-fordham-faces-police-raids-after-source-reveals-confidential-government-information/>.

152 See, eg, *Evidence Act 1995* (Cth) s 126K; *Evidence Act 2011* (ACT) s 126K; *Evidence Act 1995* (NSW) s 126K; *Evidence Act 2008* (Vic) s 126K; *Evidence Act 1906* (WA) s 20I. Journalist is defined variously across Australian evidence law. In the Commonwealth and ACT legislation, a 'journalist' is a person who is 'engaged and active in the publication of news and who may be given information by an informant in the expectation the information may be published in a news medium': *Evidence Act 1995* (Cth) s 126J; *Evidence Act 2011* (ACT) s 126J. In the NSW and WA legislation, a journalist is defined to be a 'person engaged in the profession or occupation of journalism in connection with the publication of information in a news medium': *Evidence Act 1995* (NSW) s 126J; *Evidence Act 1906* (WA) s 20G. The Victorian definition adds that the person may be engaged in connection with the publication of 'information, comment, opinion or analysis in a news medium': *Evidence Act 2008* (Vic) s 126J(1). However, it provides much more guidance in determining whether a person is engaged in the profession or occupation of journalism: at s 126J(2). At the time of writing, consultations are underway in Queensland with respect to the introduction of shield laws: see Marty Silk, 'Qld Govt Begins Talks on Media Shield Law', *The West Australian* (online, 24 February 2021) <https://thewest.com.au/business/media/qld-govt-begins-talks-on-media-shield-law-ng-s-2050860>. In addition, the Parliamentary Joint committee on Intelligence and Security called on the Australian government to 'promote consideration of harmonisation of State and Territory shield laws through National Cabinet', which undoubtedly would include the introduction of such a scheme in Queensland: *Inquiry into the Impact of the Exercise of Law Enforcement Report* (n 1) xxii.

153 For critique, see, eg, Hannah Ryan, 'The Half-Hearted Protection of Journalists' Sources: Judicial Interpretation of Australia's Shield Laws' (2014) 19(4) *Media and Arts Law Review* 325.

154 *Evidence Act 1995* (Cth) s 126K.

155 Ibid s 131A.

extend to investigatory or non-curial processes.[156] As a result, federal agencies are able to circumvent the main objective of the shield laws by using search powers to investigate the journalist's own records and identify their confidential sources, before legal proceedings have been commenced or even considered. Indeed, this was a clear purpose of the AFP raid on Smethurst. Protecting source confidentiality in federal police investigations would therefore require statutory reform.[157]

One model for potential reform is presented by the *Evidence Act 2008* (Vic). In contrast to the federal position, uniform evidence laws in Victoria, NSW, the ACT and the Northern Territory ('NT') extend shield protection to 'disclosure requirements' beyond the trial context.[158] The Victorian Act expressly includes search warrants within the scope of 'disclosure requirements', thereby giving critical protection to source confidentiality in police investigations.[159] Stephen Odgers says it is 'possible' that shield protections in the NSW, ACT and NT evidence Acts may also extend to search warrants, though this remains untested.[160]

The *Police and Criminal Evidence Act 1984* (UK) offers another, more detailed, model for reform. This scheme excludes all journalistic materials from the scope of search warrants.[161] Confidential journalistic materials may not be accessed. Where such materials are not held in confidence, investigators may apply to a judge, in a contested hearing, for a 'production order'.[162] Regular search warrants may be sought for non-confidential journalistic materials only where a production order has not been complied with or where there is good reason to think it would not be effective.[163]

C Covert Data Surveillance

A source may be identified when a journalist's private materials are accessed under a search warrant. But the same end may also be achieved with covert data surveillance – an option available to a wide range of government agencies, which may not even require a warrant.

---

156 Stephen Odgers, *Uniform Evidence Law* (Thomson Reuters, 16th ed, 2021) 21. For discussion of the somewhat complex role that section 131A plays in the Commonwealth uniform evidence framework, see at 1261–2.

157 Statutory reform of this nature occurred in New Zealand in 2012. As Sanette Nel observed:

> promise of confidentiality made by a journalist to a particular source *becomes meaningless* in the face of a police officer armed with a search warrant that entitles him or her to look through the entire contents of the newsroom without prior warning. Sources of information will also dry up due to fears that journalists' files will be readily available to the police.

Sanette Nel, 'Journalistic Privilege: Does It Merit Legal Protection?' 38(1) *The Comparative and International Law Journal of Southern Africa* 99, 111 (emphasis added).

158 *Evidence Act 2008* (Vic) s 131A(2); *Evidence Act 1995* (NSW) s 131A(2); *Evidence Act 2011* (ACT) s 131A(2); *Evidence Act (National Uniform Legislation) 2011* (NT) s 131A(2).

159 *Evidence Act 2008* (Vic) s 131A(2)(g).

160 Odgers (n 156) 21. See also discussion of arguments for and against this position: at 1262–4.

161 *Police and Criminal Evidence Act 1984* (UK) ss 11(2)–(3) (definition of 'excluded material'). The *Terrorism Act 2000* (UK) sets up a framework by which such materials may be obtained under a search warrant in a terrorism investigation.

162 *Police and Criminal Evidence Act 1984* (UK) ss 8(1)(d), 9, 11 (definition of 'excluded material'), 13 (definition of 'journalistic material'), 14 (definition of 'special procedure materials'), sch 1 cl 8.

163 Ibid sch 1 cls 12–14.

Introduced in 2015, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) ('*Data Retention Act*')[164] obliges all telecommunications service providers in Australia to retain customer metadata for at least two years. A range of government agencies are authorised to access the retained metadata without a warrant.[165] By late 2018, telecommunications service providers reported receiving some 350,000 requests to access metadata each year.[166]

In the telecommunications context, retained metadata does not include the content or substance of a communication. Rather, it includes information about the communication, such as telephone numbers, locations and times associated with a communication.[167] The prevalence of GPS tracking on devices also means that metadata is likely to reveal a person's locations throughout the day, giving rise to 'an enormously rich trail of information'.[168]

A journalist's metadata could easily be capable of revealing the identity of their sources, as well as details of when, where, and how they communicated. Indeed, by triangulating the information, one former director of both the Central Intelligence Agency and the National Security Agency, General Michael Hayden, told a symposium in 2014 that the information is so rich that '[w]e kill people based on metadata'.[169]

Threats to journalistic confidentiality prompted the introduction of the Journalist Information Warrant ('JIW'), which is required to authorise agency access to journalists', or their employers', metadata for the purpose of identifying a confidential source.[170] As the definition of 'source' only refers to journalists 'working in a professional capacity', a JIW will not be required to access metadata

164 On the legislative history of this Act, see Rick Sarre, 'Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia' (2017) 12(3) *Asian Criminology* 167, 170–1.

165 The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) ('*Data Retention Act*') specifies 14 agencies capable of gaining access to retained metadata, including police and intelligence agencies: *Telecommunications (Interception and Access) Act 1979* (Cth) s 110A ('*TIA Act*'). This does not include agencies declared by the Minister to be a 'criminal law-enforcement agency': s 110A(3). Reports from 2018 suggested that, at that time, an extensive range of other agencies (including, for example, local councils) had relied on state-based powers to gain access to retained metadata: Commonwealth, *Parliamentary Debates*, House of Representatives, 6 December 2018, 12777–9 (Adam Bandt). See also Communications Alliance Ltd, Submission No 87 to Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation (Assistance and Access) Bill 2018* (December 2018). This submission concerned specific agencies (including state agencies and local councils) that had made requests for metadata.

166 Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 19 October 2018, 41 (John Stanton, Chief Executive Officer of Communications Alliance Ltd).

167 Sarre (n 164) 168. See also *TIA Act 1979* (Cth) s 187AA which sets out a table of information which must be retained.

168 Sarre (n 164) 168.

169 John Naughton, 'Death by Drone Strike, Dished Out by Algorithm', *The Guardian* (online, 21 February 2016) <https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan>.

170 Benedetta Brevini 'Metadata Laws, Journalism and Resistance in Australia' (2017) 5(1) *Media and Communication* 76, 78.

to identify a source who provided information to a non-professional journalist.[171] In evidence before the Parliamentary Joint Committee on Intelligence and Security in 2019, the AFP revealed that in the 2017–18 financial year it had gained two JIWs which allowed it to access journalists' metadata 58 times.[172]

An issuing authority[173] may only issue a JIW if satisfied that it is for a specified law enforcement purpose.[174] In light of Australia's considerable suite of secrecy-based offences, this requirement could be easily fulfilled in an investigation concerning the disclosure of sensitive government information to a journalist,[175] as well as the disclosure of information regarding alleged criminal conduct or involving trade secrets by a private sector whistleblower. In addition, investigations into serious criminal conduct, such as organised crime, might support a successful application for a JIW even though the source is peripheral, though potentially useful, to that investigation. Indeed, the investigation may even relate to the wrongdoing which led to the source's decision to blow the whistle in the first place. Moreover, it would be expected that a JIW could be obtained in order to investigate the actual or potential leaking of classified material *before* determining whether the source was covered by whistleblower protections.[176] In all, there is every likelihood that a whistleblower (even a protected whistleblower) could be identified by a government agency under a JIW, undermining the emphasis placed on protecting anonymity under whistleblower laws.

The issuing authority must also be satisfied that issuing the warrant is in the public interest. Here the interests at stake are articulated as 'the public interest in issuing the warrant' and 'the public interest in protecting the confidentiality of the identity of the source.'[177] In weighing these competing interests, the issuing authority will have regard to matters such as privacy and whether reasonable attempts have been made to obtain the information by any other means.[178]

---

171 *TIA Act 1979* (Cth) s 5(1) (definition of 'source'). 'Source' is defined in section 5(1) as

> a person who provides information: (a) to another person who is working in a professional capacity as a journalist; and (b) in the normal course of the other person's work in such a capacity; and (c) in the expectation that the information may be disseminated in the form of: (i) news, current affairs or a documentary; or (ii) commentary or opinion on, or analysis of, news, current affairs or a documentary.

172 Josh Taylor, 'Australian Federal Police Accessed Journalists' Metadata 58 Times in a Year', *The Guardian* (online, 9 July 2019) <https://www.theguardian.com/world/2019/jul/09/australian-federal-police-accessed-journalists-metadata-58-times-in-a-year>.

173 An issuing authority is a judicial officer or a person who is a member of the Administrative Appeals Tribunal and a lawyer of five years' standing who has been consensually appointed to the role by the Attorney-General: *TIA Act 1979* (Cth) ss 5(1) (definition of 'issuing authority' and definition of 'Part 4-1 issuing authority'), 6DB–6DC.

174 The warrant must be reasonably necessary for either: (a) the enforcement of the criminal law, finding a missing person or enforcing laws that impose financial penalties or protect the public revenue, or (b) the investigation of a serious offence punishable by imprisonment for at least three years: *TIA Act 1979* (Cth) s 180T(2)(a), referring to ss 178–180(4).

175 See, eg, *Criminal Code Act 1995* (Cth) div 122.

176 For example, as provided for under *PIDA 2013* (Cth).

177 *TIA Act 1979* (Cth) s 180T(2)(b).

178 Ibid s 180T(2)(b). This limited avenue of oversight does not apply to ASIO, who can apply directly to the Attorney-General for a Journalist Information Warrant ('JIW'): at ss 180J–180L; although in some circumstances the Director-General of ASIO can even issue a JIW directly: at s 180M. Where ASIO has applied for a JIW, only the public interest test, not the purpose test, applies: at s 180L(2)(b).

The issuing authority will be assisted by submissions made by a 'Public Interest Advocate'.[179] This security-cleared lawyer, appointed to the position by the Prime Minister,[180] makes submissions to assist the application of the public interest test. However, they do not stand in the shoes of the journalist or their employer; nor do they represent the interests of media or open justice more broadly; nor do they liaise with the potential subject of the warrant. Thus, a journalist will have no way of knowing whether they are subject to a JIW.

In practice, it is impossible to assess the effectiveness of the JIW regime. The entire process is secret, with no transparency about the number of applications, the arguments used, the successful applications, or any other aspect of the proceedings.

Whilst the JIW is a positive recognition of the threat these laws pose to journalistic confidentiality, it only applies to professional journalists and provides a relatively minor obstacle to agencies accessing information for the direct purpose of identifying a journalist's confidential source.[181]

In light of the *Data Retention Act*'s intrusion on journalistic confidentiality, journalists were widely encouraged to make use of encryption technologies in their interactions with sources.[182] Then, on the evening of the final parliamentary sitting day of 2018 and over strong concerns of opposition parties, government departments, industry and the public,[183] the federal government passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) ('*TOLAA*').

The *TOLAA* creates a complex set of processes giving agencies the power to ask and even force telecommunications 'providers' (defined with extravagant breadth to include everyone from major internet service providers to phone repair workers)[184] to undertake 'acts or things' to assist the agency in its law enforcement

179 Ibid s 180T(2)(b)(v).

180 Ibid s 180X(1).

181 Oversight and accountability are serious issues with the data retention scheme. The Report of the Commonwealth Ombudsman, tabled in July 2019, reported widespread misconduct under the metadata retention and access scheme. This included one instance of an AFP officer accessing a journalist's metadata without a JIW and two further instances of officers applying for and obtaining a JIW from a person not authorised to provide it: Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979: For the Period 1 July 2016 to 30 June 2017* (Annual Report, November 2018); Paul Karp and Josh Taylor, 'Police Made Illegal Metadata Searches and Obtained Invalid Warrants Targeting Journalists', *The Guardian* (online, 23 July 2019) <https://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists?CMP=Share_iOSApp_Other>.

182 See, eg, Richard Ackland, 'Data Retention: "Journalist Information Warrants" Are Warrants in Name Only', *The Guardian* (online, 23 March 2015) <https://www.theguardian.com/commentisfree/2015/mar/23/data-retention-journalist-information-warrants-are-warrants-in-name-only>; Mike Dobbie, 'Data Retention and Your Journalism', *Media, Entertainment and Arts Alliance* (Blog Post, 7 December 2015) <https://www.meaa.org/news/data-retention-and-your-journalism/>; Sally Humphreys and Melissa de Zwart, 'Data Retention, Journalist Freedoms and Whistleblowers' (2017) 165(1) *Media International Australia* 103, 106.

183 Commonwealth, *Parliamentary Debates*, House of Representatives, 6 December 2018, 12777–9 (Mike Kelly and Adam Bandt), 12792–4 (Julian Hill and Andrew Wilkie).

184 *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) s 317C.

or intelligence-related work.[185] 'Acts or things' is as broad as it sounds. It can include embedding backdoor weaknesses and decryption technologies into target devices – an extraordinary power that undercuts the very concept of private, secure communications. While agencies do not require a warrant to force a 'provider' to build a weakness into a target device, they do need a traditional warrant to gain access to the actual content of the information, documents, or communications.[186]

Under these laws, there is every chance that journalists who investigate national security matters or serious crimes, or who work with government sources with access to classified information, will be subject to a legally-sanctioned digital assault. They risk: general warrantless metadata access by a wide range of government agencies; targeted metadata access to identify their sources under a JIW; orders under the *TOLAA* to place backdoors in their encrypted or protected data; and warrant-based access to their (now decrypted) communications. These forms of data surveillance are all covert, so each could take place without the journalist or their employer ever being aware of them and at no stage are their interests, or those of the industry, ever represented.

In all, a whistleblower may be confident that a journalist will adhere to their ethical obligation for source protection, but should be aware that the journalist can do very little to protect their source from identification (including covert identification) by government agencies, especially in the context of a police investigation. A 'non-professional' journalist should be doubly concerned. Their metadata is vulnerable to access by a wide range of agencies without a warrant, including for the express purpose of identifying their confidential source. This is troubling for journalists, may expose whistleblowers, and, in creating a significant deterrent for potential whistleblowers who may also feel unable to make an internal disclosure, it severely and dangerously degrades the media's watchdog role.

V A CHAIN OF DISCLOSURE AND ACCOUNTABILITY: DISCUSSION AND RECOMMENDATIONS

The events of 2019 revealed the fragile state of press freedom in Australia and provided fresh examples of the fundamental importance of whistleblowing to public accountability and institutional integrity. While press freedom and whistleblowing are often thought of as separate issues, this article makes evident that the two should be considered as part of the same system. There will always be circumstances in which the formal, internal mechanisms for whistleblowers break down, leaving those who feel compelled to expose misbehaviour turning to the media as a whistle-of-last-resort. Similarly, there is little point protecting press freedom if the authorities are able to identify and pursue sources who are legitimately exposing wrongdoing, using official investigative tools. Accountability and integrity across the public and private sectors rely on the creation of safe pathways for protected

185 Ibid s 317A.

186 For discussion see, eg, Rebecca Ananian-Welsh, 'Journalistic Confidentiality in an Age of Data Surveillance' (2019) 41(2) *Australian Journalism Review* 225.

disclosures, from an initial complaint through to the (far rarer) scenario of 'going public'. In this Part, we draw together the foregoing analysis and summarise our recommendations for reform.

A Enhancing Whistleblower Protections

The driving force behind whistleblower and source protections is the achievement of accountability and integrity. These aims do not always require public disclosure of information. Most complaints have the potential to be effectively managed internally or through an independent authority such as an Ombudsman. Thus, the best protection from inappropriate or risky public disclosures is a robust and effective system for internal disclosures. This article has identified key weaknesses in these systems. First, inconsistency between *PIDA* and the *Corporations Act* – particularly with respect to the public interest test and definitions of disclosable conduct/matters – has the potential to create confusion and undermine the system overall. Second, *PIDA* fails to create a safe pathway for intelligence disclosures, even where a disclosure might be critical for integrity and in the public interest. Also, the scope of 'intelligence information' is unnecessarily broad, which has the capacity to undermine accountability in the law enforcement (as well as intelligence) context, and drive whistleblowers to silence or, feeling they have no better option, publicity.

The enhancement of whistleblower protections for internal intelligence disclosures would support both national security and accountability and should be a reform priority for *PIDA*. The creation of an avenue for external intelligence disclosures must be approached with great caution but, as the case studies explored have demonstrated, ought not be dismissed out of hand.

B Press Legitimacy and Freedom

A journalist may not be the ideal first contact for a whistleblower, but disclosures to the media have an important and legitimate role to play in maintaining the accountability and integrity of Australian institutions. This fact might be overlooked in the system created by *PIDA*.

PIDA would be enhanced by expressly identifying journalists as potential recipients of a protected external disclosure.

Similarly, the failure to extend shield law-style protections to law enforcement and investigation contexts has created a backdoor by which confidential sources (including whistleblowers whose anonymity may be protected) may be identified by police and a range of other government agencies. Victoria leads the way in addressing this gap in source protection and provides a possible model for reform.

At present, a journalist's ethical obligations have no legal support, potentially leaving journalists in the position of having to defy the police and courts in order to honour their code of ethics. Given the scope and sophistication of modern investigative techniques, including extensive covert search and surveillance powers, it may be impossible for journalists to guarantee their sources anonymity (and certainly not without applying sophisticated counter-surveillance techniques). Although the number of stories *not* told cannot be measured, empirical research

supports the claim that many sources have decided that the risks and costs of exposure are simply too great to speak to journalists, and democratic accountability is suffering as a result.[187]

C The Public Interest

Central to this entire discussion is the concept of the public interest. Ultimately, the government is empowered to serve the public it represents. While commercial media has an obligation to generate a profit for their owners, they nonetheless have an additional and arguably higher obligation to serve the public. The concept of the public interest appears throughout the law, but it is differently framed and interpreted, depending on statutory context.[188] Thus, all public interest tests are not created equal; any such test will serve a different purpose and emphasise distinct aims and concerns. It is, in all, a notoriously vague and slippery area that, nonetheless, forms the basis of the external disclosure, shield law, and JIW schemes. For present purposes, it is important to note that a core objective of the whistleblower regime is to serve the public interest in *public*, *democratic* accountability – of which press freedom and source confidentiality are integral parts. Thus, these considerations deserve express articulation in public interest tests at each stage in the chain of disclosure – from internal complaint through to the warrant applications and shield laws that become relevant once information has been published.

VI CONCLUSION

Barely a week goes by without an important news story making global headlines based on leaked documents that reveal inappropriate, immoral, or illegal conduct by those in positions of power. These stories are unlikely to be volunteered by the impugned people or organisations. They come from individuals who choose to call out the wrongdoing they have witnessed. This decision invites reprisal, sometimes in subtle or mild ways, other times by risking more serious retaliations, unemployment, or criminal prosecution.

Whistleblower protection laws recognise and support the fundamental role that these individuals play in the liberal democratic system. Journalists' ethical obligation to protect their sources and, in most states, evidentiary shield laws complement these protections, creating an all-important chain of disclosure that enhances accountability and the rule of law. This article has examined and critiqued the legal protections for private and public sector whistleblowers and, relatedly,

187 See generally Rebecca Ananian-Welsh, Sarah Kendall and Richard Murray, 'Risk and Uncertainty in Public Interest Journalism: The Impact of Espionage Law on Press Freedom' (2021) 44(3) *Melbourne University Law Review* 764; Richard Murray, Rebecca Ananian-Welsh and Peter Greste, 'Journalism on Ice: National Security Laws and the Chilling Effect in Australian Journalism' in Téwodros Workneh and Paul Haridakis (eds), *Counter-Terrorism Laws and Freedom of Expression: Global Perspectives* (Lexington Books, 2021) 173.

188 *Hogan v Hinch* (2011) 243 CLR 506, 536–7 [31]–[32] (French CJ).

journalists' confidential sources under federal law. In doing so, it has revealed the intersection between whistleblowing and press freedom as well as gaps and weaknesses in existing legal frameworks.

While whistleblowing is protected by highly complex sets of legal provisions, press freedom and even free expression are barely mentioned, let alone recognised or protected, under law. For the Senate Environment and Communications References Committee, this was 'not acceptable', and

> [i]n order to better protect a free press in Australia, the committee considers that federal legislation should be introduced to protect the right to freedom of expression and in so doing also guide Parliament in its consideration of intersecting criminal and national security laws.[189]

Despite this divergence in protection, whistleblowers and press freedom are interconnected – as demonstrated in, for instance, the AFP raids on Smethurst and the ABC, and the Kessing and Wilkie affairs. Close examination of private and public sector whistleblower protections as well as protections for journalists' sources reveals a number of weaknesses and inconsistencies. As Brown articulates, a failure to address these problems can have serious consequences. An effective whistleblowing regime makes it easier and safer for whistleblowers to make their concerns known without fear of reprisal, as well as having a deterrent effect on those considering breaking the rules. Conversely, when the system is ineffective or subject to gaps and loopholes, the likelihood of misbehaviour rises.

This is the case even in the national security context, where security agencies have expressed their concerns about the potential for the media to do great harm by either deliberately or inadvertently exposing secret information.[190] History suggests, however, that journalists have generally shown restraint in the way they have handled sensitive details.[191] This is not to say that the media and the public should have unfettered rights to sensitive information. Rather, any weakening or limitation of the scope of protected disclosures should be subject to close scrutiny. Not only can disclosures to the media be a legitimate, appropriate, and important part of the democratic system, but when journalists have dealt with sensitive information, it has often triggered much needed reforms. This supports a need to formally recognise, describe, and protect the chain of accountability created by public disclosures through the media in the *Corporations Act*, *PIDA*, government agencies' powers of surveillance and investigation, and the courts.

---

189 *Inquiry into Press Freedom Report* (n 1) 130 [7.73].

190 Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 20 September 2019, 20–1 (Michael Pezzullo, Secretary of the Department of Home Affairs).

191 See, eg, Brian Toohey, *Secret: The Making of Australia's Security State* (Melbourne University Press, 2019) ch 37, discussing the investigation of 'significant intelligence leaks' to over 40 journalists between 1972 and 1975, and Toohey's observation that: 'Australian media reporting has never resulted in the death of an intelligence operative or undercover police officer – far more people have been wrongly killed as a result of intelligence operations being kept secret': at 20.