Source Confidentiality Under Siege: How Law Enforcement Powers Threaten Journalists' Ethical Obligations

Adam Lukacs, University of Queensland, in his CAMLA Essay Competition winning piece, comments on the legislative framework protecting the confidentiality of journalists' sources.

I Introduction

The media are regarded as the 'eyes and ears' of the public.[1] In the course of acting as a public watchdog and gathering news, journalists occasionally guarantee anonymity to sources to preclude them from being subject to retribution for exposing matters of public interest to the media.[2] However, journalists enjoy limited protections for their sources under Australian law, and such protections face unique challenges in the context of metadata retention and national security regimes.[3] Relevantly, the vulnerability of source confidentiality was highlighted by the Australian Federal Police's raids on the home of Annika Smethurst and the Australian Broadcasting Corporation's Sydney headquarters in June 2019, which arose out of Smethurst's reporting on a proposal to expand federal surveillance powers.[4] One aim of the raid had been to identify the anonymous source who had provided Smethurst with classified information concerning the proposal. This essay will argue that police powers of search and seizure pose a significant threat to journalistic source confidentiality, specifically with respect to laws that provide a framework for data surveillance. The protections afforded to journalists and their sources under these regimes are weak, and such laws therefore represent a grave intrusion on journalists' ethical obligations when less intrusive alternatives are available. In this respect, the journalists' ethical obligations with respect to source confidentiality will first be discussed, followed by an assessment of the legal regimes which threaten source confidentiality.

Metadata retention laws, Journalist Information Warrants and the industry assistance scheme will be encompassed in this discussion. Finally, how these regimes undermine shield laws and how shield laws could potentially be reformed to better protect journalists and their sources in this context will also be explained.

II Journalistic Ethical Obligations

Source confidentiality is a core ethical obligation for journalists and a central tenet of press freedom.[5] Failure to provide source confidentiality would risk deterring sources from assisting the press in informing the public on matters of public interest.[6] A journalist's obligation to preserve the confidentiality of a source where they have agreed to do so is found, *inter alia*, in Clause 3 of the Media, Entertainment & Arts Alliance Journalist Code of Ethics.[7] Clause 3 relevantly provides that "where confidences are accepted, respect them in all circumstances".[8] Despite the ethical breach that revealing a source's identity would entail and the negative repercussions that would follow from this,[9] such as exposing the source to danger and eroding the trust between journalists and their sources,[10] Australian law provides minimal protection for journalists who face such a demand.[11] Journalists' ethical codes have no legal status and courts have consistently refused to recognise the existence of any 'journalists' privilege' protecting a journalist from disclosing their sources.[12] A journalist will be required to reveal a source in court proceedings if it is "necessary in the interests of justice"[13]

1 *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 183 (Sir Donaldson MR).

2 Sanette Nel, 'Journalistic Privilege: Does it Merit Legal Protection?' (2005) 38(1) *Comparative and International Law Journal of South Africa* 99, 100.

3 Sal Humphreys and Melissa de Zwart, 'Data Retention, Journalist Freedoms and Whistleblowers' (2007) 165(1) *Media International Australia* 103, 103.

4 Rebecca Ananian-Welsh, '*Smethurst v Commissioner of Police* and the Unlawful Seizure of Journalists' Private Information' (2020) 25 *Media & Arts Law Review* 60, 60, 61. See *Smethurst v Commissioner of Police* (2020) 376 ALR 575; *Australian Broadcasting Corporation v Kane* (2020) 377 ALR 711 ('*Kane*').

5 Rebecca Ananian-Welsh, 'Journalistic Confidentiality in an Age of Data Surveillance' (2019) 41(2) *Australian Journalism Review* 225, 225 ('Journalistic Confidentiality'); *Mahon Tribunal v Keena and Kennedy* [2009] IESC 64 [23] (Fennelly J). See also 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) [13], [19], [45].

6 *Goodwin v United Kingdom* (1996) 22 EHRR 123 [39]; Joseph Fernandez, 'Pass the Source – Journalism's Confidentiality Bane in the Face of Legislative Onslaughts' (2017) 27(2) *Asia Pacific Media Educator* 202, 203.

7 Mark Pearson, *The Journalist's Guide to Media Law: A Handbook for Communicators in a Digital World* (Taylor & Francis Group, 6th ed, 2019) 318.

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

9 Lawrence McNamara and Sam McIntosh, 'Confidential Sources and the Legal Rights of Journalists: Re-Thinking Australian Approaches to Law Reform' (2010) 32(1) *Australian Journalism Review* 81, 81–82.

10 Media, Entertainment & Arts Alliance (MEAA), Submission No 90 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications (Interception and Access Amendment (Data Retention) Bill 2014* (19 January 2015) 4 ('MEAA Submission'); *Kane* (n 4) 720 [36]–[37], 723 [46] (Abraham J); Pearson (n 7) 318.

11 McNamara and McIntosh (n 9) 81.

12 *McGuinness v Attorney-General (Vic)* (1940) 63 CLR 73, 87 (Rich J); *Harvey and McManus v County Court of Victoria* (2006) 164 A Crim R 62, 79–80 [90] (Hollingworth J); *R v McManus and Harvey* [2007] VCC 619 [34]–[35] (Chief Judge Rozenes); *Kane* (n 4) 755 [197] (Abraham J); *Liu v The Age Company Ltd & Ors* (2016) 92 NSWLR 679, 706 [123] (McColl JA); *Re Evening News* (1880) 1 LR (NSW) 211, 240 (Martin CJ). See Joseph Fernandez, 'Journalists' Confidential Sources: Reform Lessons from Recent Australian Shield Law Cases' (2014) 20(1) *Pacific Journalism Review* 117, 129.

as there is a paramount public interest in securing the administration of justice which no undertaking of confidentiality can override.[14] Despite the potential consequences for refusing to disclose sources, journalists have stalwartly adhered to this ethical principle,[15] even with the prospect of severe fines or imprisonment.[16] Indeed, this is unsurprising as sources remain the "wellspring of journalists' work" — source confidentiality encourages the free flow of information in a democratic society because confidential disclosures provide vital information that supports public interest journalism.[17] However, despite widespread recognition of the crucial link between press freedom and source confidentiality,[18] and journalists' ardent commitment to source protection, the capacity of journalists to protect their sources is fragile in light of technological developments and national security laws that now pose a threat to guaranteeing source anonymity.[19]

III Vulnerability of Source Confidentiality

A Law Enforcement Powers

Government search, seizure and surveillance powers vastly expanded in the aftermath of 9/11,[20] with 75 pieces of counter-terrorism legislation being enacted since 2001.[21] While police raids such as the one on Smethurst's home and the ABC present a clear threat to source confidentiality, federal covert data surveillance schemes represent a far more insidious danger.[22]

1. *Data Retention*

As amended in 2015, the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA**) implements a national scheme for mandatory data retention, obligating all telecommunications providers in Australia to retain customer metadata for at least two years.[23] There is no definition of 'metadata' in the legislation, but such providers are required to retain, among other things, information relating to the time, date and location of communications passing over their services.[24] Such data consists of information about a communication or parties to a communication, as distinct from the content or substance of that communication, which is inaccessible except under a warrant.[25] This data can nevertheless reveal significant identifying and personal information about one's contacts, communications, activities and whereabouts,[26] and is accessible without a warrant by ASIO if disclosure would be in connection with the performance by ASIO of its functions[27] and by other law enforcement agencies if it is 'reasonably necessary for the enforcement of the criminal law'.[28] Such data not only captures the communications between a journalist and a source but also the fact that information has passed between them and the details of when, where and how they communicated.[29] Law enforcement agencies can triangulate this information in such a way to reveal the identity of a journalist's sources,[30] demonstrating the threat that these law enforcement powers pose to source confidentiality as such powers potentially allow law enforcement to frustrate journalists' efforts to maintain source confidentiality by examining their metadata.

2. *Journalist Information Warrants*

However, because accessing journalists' metadata may reveal their confidential sources, the TIA includes a Journalist Information Warrant (**JIW**) scheme.[31] This allows a journalist's metadata to be accessed for the purpose of identifying a confidential source if the public interest

13 *John Fairfax & Sons Ltd v Cojuangco* (1988) 165 CLR 346, 354–355 (Mason CJ, Wilson, Deane, Toohey and Gaudron JJ).

14 *Nicholls v Director of Public Prosecutions (SA)* (1993) 61 SASR 31, 41 (Legoe ACJ), 51 (Perry J); *Independent Commission Against Crime and Corruption v Cornwall* (1993) 38 NSWLR 207, 234 (Abadee J); *Von Doussa v Owens (No 3)* (1982) 31 SASR 116, 117 (King CJ); *Re Buchanan* (1964) 65 SR (NSW) 9. See also *X Ltd v Morgan-Grampian Publishers* [1991] 1 AC 1, 48 (Lord Bridge).

15 National Press Club, 'NPC Statement on the AFP Raids', *National Press Club of Australia* (Web Page, 5 June 2019) <https://www.npc.org.au/article/freedom-of-the-press/2019/75-npc-statement-on-the-afp-raids>; MEAA Submission (n 10) 4. See Wendy Bacon and Chris Nash, 'Confidential Sources and the Public Right to Know' (1999) 21(2) *Australian Journalism Review* 1, 1–2.

16 See, eg, *R v Kessing* (2008) 73 NSWLR 22, 35 [57] (Bell JA); *R v Barrass* (unreported, District Court of Western Australia, Judge Kennedy, 7 August 1990); *R v Budd* (unreported, Supreme Court of Queensland, Dowsett J, 20 March 1993).

17 Des Butler and Sharon Rodrick, *Australian Media Law* (5th ed, Thomson Reuters, 2015) 689; *Ashby v Commonwealth of Australia (No 2)* [2012] FCA 766 [18] (Rares J) ('*Ashby*'); *McKenzie and Baker v Magistrates' Court of Victoria and Leckenby* [2013] VSCA 81 [3] (Harper JA).

18 Human Rights Committee (n 5) [2]–[3].

19 Moira Paterson, 'The Public Privacy Conundrum – Anonymity and the Law in an Era of Mass Surveillance' in Johan Lindberg and Denis Muller (eds), *In the Name of Security – Secrecy, Surveillance and Journalism* (Anthem Press, 2018) 15, 15.

20 Ananian-Welsh, Journalistic Confidentiality (n 5) 226.

21 George Williams and Kieran Hardy, Submission No 11 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (26 July 2019) 1 ('Williams and Hardy Submission').

22 Ananian-Welsh, Journalistic Confidentiality (n 5) 226.

23 Ibid; *Telecommunications (Interception and Access) Act 1979* (Cth) ss 187A, 187AA, 187C ('TIA').

24 TIA (n 23) s 187AA; Williams and Hardy Submission (n 21) 7.

25 TIA (n 23) ss 7, 108, 172; Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Report, 27 February 2015) 12 [2.17].

26 Williams and Hardy Submission (n 21) 7. See also *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung* (Court of Justice of the European Union, C-293/12 and C-594/12, 8 April 2014) [27].

27 TIA (n 23) ss 174–175.

28 Ibid ss 110A, 177–180. See also Centre for Media Transition, Submission No 31 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (31 July 2019) 4 ('Media Transition Submission').

29 MEAA Submission (n 10) 6; Ananian-Welsh, Journalistic Confidentiality (n 5) 227; Paterson (n 19) 17.

30 See, eg, *F v Crime and Corruption Commission* [2021] QCA 244 [4] (Mullins JA).

31 Mark Pearson and Joseph M. Fernandez, 'Surveillance and National Security 'Hyper Legislation' – Calibrating Restraints on Rights with a Freedom of Expression Threshold' in Johan Lidberg and Denis Muller (eds), *In the Name of Security – Secrecy, Surveillance and Journalism* (Anthem Press, 2018) 51, 66.

in issuing the warrant outweighs the public interest in protecting the journalist's sources.[32] The public interest requirement involves considerations of privacy and whether reasonable attempts have been made to obtain the information otherwise.[33]

'Source' is defined narrowly in the TIA to only capture journalists 'working in a professional capacity'.[34] A JIW is therefore not required to access metadata to identify a source who provides information to a non-professional journalist, meaning that the JIW scheme only applies to some journalist-source interactions and confers no protection to journalistic confidentiality outside of 'professional' journalism.[35] This represents a problematic intrusion on journalists' ethical obligations, as the definition of 'source' allows law enforcement to access the metadata of an individual engaged in legitimate and good faith journalism, who may otherwise not be a 'professional journalist', to uncover their sources without a JIW.[36]

Agencies may seek a JIW from an 'issuing authority',[37] which must only issue a JIW if it is satisfied that the warrant is for a specified law enforcement purpose.[38] These purposes include enforcing the criminal law, finding a missing person, enforcing laws that impose financial penalties, protecting the public revenue or for the investigation of a serious offence punishable by at least three years' imprisonment.[39] While this 'purpose test' provides some limit on the scope of JIWs, this requirement may be easily fulfilled in the context of Australia's secrecy-based offences.[40] Under these laws, specifically espionage offences that criminalise a wide range of conduct pertaining to the handling and communication of classified and national security information,[41] a JIW could be obtained to investigate the potential leaking of classified information before determining whether the source was covered by whistleblower protections.[42]

The JIW regime is therefore a minor obstacle to law enforcement agencies accessing information for the direct purpose of identifying a journalist's confidential source. Further, journalists may be subject to criminal penalties under these laws for merely receiving or possessing sensitive information, even prior to publication.[43] This gives rise to the risk that the JIW regime may be employed to access a journalist's metadata to prevent the disclosure of information leaked to journalists or to discover the source of a leak.[44] A promise of confidentiality made by a journalist to a particular source therefore becomes meaningless where a relatively easily-obtained JIW entitles law enforcement to identify that source,[45] thus demonstrating the intrusion on journalists' ethical obligations that these law enforcement powers represent.

Further, journalists cannot contest JIWs because of secrecy provisions that render the revelation of the existence of a JIW application or an application's result a crime,[46] meaning that a journalist whose metadata is being targeted will not be informed of this.[47] While a targeted media organisation can have no input into the application for a JIW, an issuing authority will be assisted by submissions made by the 'Public Interest Advocate' (**PIA**) with respect to the public interest test.[48] However, the PIA does not represent the interests of journalists and is insufficiently directed towards protecting the freedom of the press as opposed to other public interests, such as national security.[49] The coalescence of the perceived inadequacy of the public interest and purpose tests, the PIA's lack of representing journalists' interests, scant oversight and there being no independent assessment of a JIW application by a superior court judge[50] has prompted calls for media organisations to be notified of the existence of JIWs in relation to them and for JIWs to be issued by judges in contested hearings.[51] There is a significant threat to source confidentiality posed by the capacity for law enforcement agencies to covertly access journalists' data for the express purpose of source identification, which

32 TIA (n 23) ss 180J, 180L, 180T; Williams and Hardy Submission (n 21) 7; Rebecca Ananian-Welsh et al, Submission No 17 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (26 July 2019) 10 ('Ananian-Welsh Submission').

33 TIA (n 23) s 180T(2)(b); Paterson (n 19) 20.

34 TIA (n 23) s 5(1) (definition of 'source').

35 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

36 Ibid 235.

37 TIA (n 23) ss 5(1), 6DB–6DC.

38 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

39 TIA (n 23) ss 178–180(4), 180T(2)(a); Ibid.

40 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

41 See, eg, *Criminal Code Act 1995* (Cth) ss 91.1–92A; *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18(2), 18A(1), 18B(1), 35P, 92(1); *Defence Act 1903* (Cth) s 73A; *Office of National Intelligence Act 2018* (Cth) ss 42, 45; *Crimes Act 1914* (Cth) ss 3ZZHA, 15HK; *Intelligence Services Act 2001* (Cth) ss 39–40M.

42 Ananian-Welsh, Journalistic Confidentiality (n 5) 228.

43 Williams and Hardy Submission (n 21) 9.

44 Ibid 9–10.

45 Nel (n 3) 111.

46 TIA (n 23) s 182A; Williams and Hardy Submission (n 21) 7; Ananian-Welsh, Journalistic Confidentiality (n 5) 229.

47 Media Transition Submission (n 26) 5.

48 Ibid; TIA (n 28) s 180T(2)(b)(v).

49 Ananian-Welsh Submission (n 32) 11.

50 Media Transition Submission (n 28) 7.

51 Ibid 3; Williams and Hardy Submission (n 21) 7; Ananian-Welsh, Journalistic Confidentiality (n 5) 235.

means that journalists may no longer be able to confidently fulfil their ethical obligations when they have guaranteed a source confidentiality.[52] The excessive secrecy of the JIW process, ineffective protections available under the JIW regime and onerous penalties for secrecy offences suggests that the law has disproportionately moved in favour of competing public interests such as national security,[53] representing an unjustified intrusion on journalists' ethical obligations in the process.

3. *'Acts and Things'*

The introduction of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLAA**) compounds the threat posed to journalistic confidentiality presented by mandatory data retention.[54] The TOLAA created industry assistance and computer access schemes and expanded the scope of search and seizure warrants, allowing law enforcement agencies to access the content of communications and overcome the use of encryption.[55]

Under the industry assistance scheme, policing and intelligence agencies can request or compel communications providers[56] to do a broad range of 'acts and things' to: assist an agency in their objectives;[57] enforce the criminal law as it relates to a serious criminal offence punishable by three or more years' imprisonment; safeguard national security; and, matters ancillary to those objectives.[58] 'Acts and things' importantly encompasses agencies being able to request or compel providers to remove electronic protections applied to telecommunications, including encryption, meaning such providers can be required to decrypt encrypted communications.[59] Accessing the content of a communication requires a valid warrant[60] and any such requests under this scheme are approved on the basis that they are 'reasonable, proportionate, practicable and technically feasible'.[61] While agencies are prohibited from requiring providers to build a 'systemic weakness' or 'systemic vulnerability' into their carriage services or devices,[62] this does not prevent an agency from requiring a provider to target a *specific* service or device.[63] For example, the AFP could require a provider to break past the passcode on a journalist's smartphone or insert an eavesdropping capability into a journalist's Google Home device.[64] Accessing the retrieved data would require a warrant but would allow agencies to uncover confidential sources without engaging the JIW provisions, as they do not extend to requests to access information under the TOLAA.[65] The lack of acknowledgment of or protection for source confidentiality under the TOLAA raises serious concerns for the potential of a wide range of telecommunications actors to 'assist' government agencies in data surveillance, making it extremely difficult for journalists to ensure source confidentiality.[66]

This framework does not in and of itself operate as a data surveillance scheme, but presents a way for law enforcement agencies to circumvent encryption and other protection technologies used by journalists and their sources when communicating.[67] While access to journalists' data is not as simple under this scheme as under the TIA, journalists investigating national security matters or who interact with government sources may nevertheless be targeted under the TOLAA.[68] They may covertly be subject to orders to cause weaknesses to be built into their attempts to encrypt or protect their data and warrant-based access to their now decrypted communications,[69] exposing confidential communications between journalists and their sources.[70] The inclusion of maintaining the public interest in journalistic confidentiality as a necessary condition for the issuance of a TOLAA-related warrant authorising access to data would provide some degree of protection that does not currently exist, and thus make the TOLAA framework a somewhat more proportionate intrusion on journalists' ethical obligations.[71] However, in their present form, these laws pose a significant threat to source confidentiality because, to the extent that journalists use electronic devices or web-based accounts, they can offer no assurances of confidentiality to their

52 Ananian-Welsh, Journalistic Confidentiality (n 5) 226.

53 Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement Powers on the Freedom of the Press* (Report, August 2020) 129 [3.306] ('PJCIS Report'); Media Transition Submission (n 28) 3.

54 Ananian-Welsh, Journalistic Confidentiality (n 5) 230.

55 Ibid.

56 *Telecommunications Act 1997* (Cth) s 317C.

57 Ibid ss 317A, 317B, 317G; Ananian-Welsh, Journalistic Confidentiality (n 5) 231.

58 *Telecommunications Act 1997* (Cth) ss 317(1)–(2), 317B.

59 Ibid ss 317E(1)(a), 317B; Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 38 [54]; Ananian-Welsh, Journalistic Confidentiality (n 5) 231.

60 *Telecommunications Act 1997* (Cth) s 317ZH.

61 Ibid ss 317JAA, 317JC, 317P, 317RA, 317V, 317ZAA.

62 Ibid s 317ZG.

63 Ibid s 317B.

64 Ibid ss 317E(1)(c), 317L(1), 317T(1); Ananian-Welsh, Journalistic Confidentiality (n 5) 232.

65 Ananian-Welsh, Journalistic Confidentiality (n 5) 232.

66 Ibid 231, 233, 236.

67 Ibid 234.

68 Ibid.

69 Ibid.

70 Alliance for Journalists' Freedom, Submission No 13 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (2019) 4.

71 Ananian-Welsh, Journalistic Confidentiality (n 5) 236.

sources.[72] This breadth of powers is coupled with minimal independent oversight or accountability mechanisms, further undermining the already scarce protections afforded to journalists and their sources,[73] demonstrating the disproportionate nature of this intrusion on journalists' ethical obligations.

B Shield Laws

The clearest protection for source confidentiality is found in 'shield laws', which operate in every Australian jurisdiction except Queensland.[74] Shield laws aim to ensure that a journalist or their employer are not compellable to disclose the identity of a confidential source in court.[75] Such laws aim to foster freedom of the press not by protecting journalists themselves, but their anonymous sources, and thereby are a legislative acknowledgement of the public interest in source confidentiality.[76] Despite this acknowledgment, the protection offered by shield laws is precarious.[77] A court may order that the laws' protections do not apply if it is satisfied that 'the public interest in the disclosure of evidence of the identity of the informant' outweighs any likely adverse effect of the disclosure on the source and outweighs the public interest in the communication of facts and opinion by the media and the ability of the media to access sources.[78]

Relevantly, federal shield laws do not extend to investigatory or non-curial processes.[79] As a consequence, most Australian law enforcement agencies are easily able to circumvent the object of shield laws by using search powers to investigate journalists' records and identify their confidential sources before legal proceedings have even commenced.[80] This is in contrast to the Victorian position where shield law protections apply to police investigations, preventing a document that would identify a journalist's confidential source from being accessed under a regular warrant.[81] The Victorian position is aligned with the legislative shield law framework of other countries such as the United Kingdom and New Zealand, with these frameworks recognising that source confidentiality is just as important in police investigations as curial proceedings.[82]

Because law enforcement in weaker shield law jurisdictions can coercively obtain documentary evidence during the investigatory stage of criminal proceedings, the need to seek disclosure in court proceedings is obviated, consequently eroding the utility of shield laws.[83] This was especially highlighted by the Smethurst raids, as the AFP had access to all material on Smethurst's phone – confidential or otherwise – with shield laws offering no protection due to their exclusive applicability to court proceedings. The rise of metadata interception also necessitates that journalists must assume their conversations with their sources could be intercepted, thus negating the intent of shield laws that recognise and protect journalist privilege because such laws are easily circumvented.[84] These weaknesses in shield laws risk 'chilling' public interest journalism because if journalists operate knowing that they can become the subject of an invasive search warrant and potential sources understand that confidences cannot be assured because of this, neither party will be willing to engage in such journalism.[85]

Insofar as they can be used to bypass the protection offered by shield laws, these law enforcement powers represent a significant threat to source confidentiality, and the effective protection of source confidentiality would require statutory reform.[86] Were shield laws to be extended to police investigations and brought in line with the position of Victoria and other jurisdictions that offer strong protections for source confidentiality like New Zealand and the UK (and if Queensland enacted shield laws of this nature), sources would not be left vulnerable to identification at early, often crucial, stages of an investigation.[87] This framework would offer a more robust and complete protection, ensuring shield laws fulfil their operative purpose: to encourage the free flow of information, which risks being undermined if journalists and their sources are inadequately protected.[88]

---

72 Alliance for Journalists' Freedom, *Press Freedom in Australia* (White Paper, May 2019) 13; Australian Lawyers Alliance, Submission No 5 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (24 July 2019) 7 [9].

73 Ananian-Welsh, Journalistic Confidentiality (n 5) 234.

74 See, eg, *Evidence Act 1995* (Cth) s 126K; *Evidence Act 1995* (NSW) s 126K; *Evidence Act 2008* (Vic) s 126K; *Evidence Act 2011* (ACT) s 126K; *Evidence Act 1906* (WA) s 201.

75 Ibid.

76 *Hancock Prospecting Pty Ltd v Hancock* [2013] WASC 290 [174] (Pritchard J); Explanatory Memorandum, Evidence Amendment (Journalists' Privilege) Bill 2011 (Cth) [1]; Pearson and Fernandez (n 31) 67–68.

77 See Hannah Ryan, 'The Half-Hearted Protection of Journalists' Sources: Judicial Interpretation of Australia's Shield Laws' (2014) 19 *Media and Arts Law Review* 325.

78 See, eg, *Evidence Act 1995* (Cth) ss 126K, 131A. PJCIS Report (n 53) 130 [3.305]; Joseph M. Fernandez and Mark Pearson, 'Shield Laws in Australia: Legal and Ethical Implications for Journalists and their Confidential Sources' (2015) 21(1) *Pacific Journalism Review* 61, 67; Patrick George, 'Free Speech and Protecting Journalists' Sources: Preliminary Discovery, the Newspaper Rule and the Evidence Act' (2017) 36(2) *Communications Law Bulletin* 24, 30.

79 *Kane* (n 4) 757 [204]–[205]; Stephen Odgers, *Uniform Evidence Law* (Thomson Reuters, 15th ed, 2020) 20.

80 Rebecca Ananian-Welsh and Joseph Orange, 'The Confidentiality of Journalists' Sources in Police Investigations: Privacy, Privilege and the Freedom of Political Communication' (2020) 94 *Australian Law Journal* 777, 789.

81 *Evidence Act 2008* (Vic) s 131A.

82 *Contempt of Court Act 1981* (UK) s 10; *Evidence Act 2006* (NZ) s 68.

83 McNamara and McIntosh (n 9) 89.

84 Media, Entertainment and Arts Alliance, Submission No 98 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of National Security Legislation* (2012) 7.

85 Anna Kretowicz, 'Reforming Australian Shield Laws' (Reform Briefing 2/2021, Press Freedom Policy Papers, The University of Queensland, 2021) 5.

86 Ananian-Welsh and Orange (n 80) 789. See, eg, New Zealand Law Commission, *Review of the Search and Surveillance Act 2012* (Report No 141, June 2017).

87 Kretowicz (n 85) 7.

88 *Ashby* (n 17) [18] (Rares J).

III Conclusion

It is uncontroversial that law enforcement and intelligence agencies require significant powers to undertake overt and covert investigations to uphold public safety.[89] However, the TIA and TOLAA create and facilitate frameworks of covert surveillance which encumber journalists in ensuring source confidentiality, thus undercutting their ethical obligations in the name of security.[90] The TIA, TOLAA and the JIW schemes all place considerable pressure on journalists attempting to protect their sources and undermine the object of shield laws. In that regard, the present state of law enforcement powers poses a significant threat to journalistic confidentiality and represent an unjustified intrusion on journalists' ethical obligations. Journalists' ethical obligations have no legal support, leaving journalists in the position of having to defy police and the courts in order to honour their ethical obligations. The abovementioned covert search and surveillance powers may mean that journalists cannot guarantee their sources anonymity from law enforcement.[91] While Australia has a strong tradition of public interest journalism, the effect of these law enforcement powers undermines the ability of the 'fourth estate' to scrutinise and hold accountable government institutions through public interest journalism which is indispensable to facilitating this scrutiny.[92] The fact that these powers allow law enforcement to clandestinely uncover sources or effectively coerce journalists into disclosing them demonstrates that such powers place source confidentiality under siege, when authorities would prefer the public to remain in the dark.[93]

89 Ananian-Welsh Submission (n 32) 2.
90 Ibid; Ananian-Welsh, Journalistic Confidentiality (n 5) 233.
91 Ananian-Welsh, Journalistic Confidentiality (n 5) 236).
92 Richard Murray, Rebecca Ananian-Welsh and Peter Greste, 'Journalism On Ice: The Effect on Public Interest Reporting of National Security Legislation in Australia' in T Workneh and P. Haridakis, *Counter-Terrorism Laws and Freedom of Expression: Global Perspectives* (Lexington Books, 2021).
93 National Press Club (n 15).