Committee Secretary

Senate Standing Committees on Environment and Communications

PO Box 6100

Parliament House

Canberra ACT 2600

1 August 2019

To the Committee,

Thank you for the opportunity to make a submission to this inquiry. We do so jointly as members of the Griffith Criminology Institute (Dr Hardy) and the Gilbert + Tobin Centre of Public Law at the University of New South Wales (Professor Williams). We are solely responsible for the views and content in this submission.

The federal Parliament has enacted 75 separate pieces of counter-terrorism legislation since 2001. A disturbing number of these have the potential to affect press freedom, particularly those enacted since the problem of foreign fighters arose in 2014. When concerns about these laws have been raised, ministers have assured journalists they will not be 'prosecuted for doing their job'.[1]

Despite such assurances, it is clear that these laws can be used to prosecute journalists and to otherwise prevent them from reporting on matters of public interest. Indeed, the recent police raids on the ABC headquarters in Sydney, as well as repeated access to metadata without proper

[1] Lenore Taylor, 'George Brandis: Attorney-General must approve prosecution of journalists under security laws', *The Guardian*, 30 October 2014.

authorisation,[2] including journalists' metadata,[3] confirm that Australia's counter-terrorism and national security laws raise very real concerns about their impact on press freedom.

This submission draws on research published in the following articles and chapters:

- Keiran Hardy and George Williams, 'Free Speech and Counter-Terrorism in Australia', in Ian Cram (ed) *Extremism, Free Speech and Counter-Terrorism Law and Policy: International and Comparative Perspectives* (Routledge, 2018); (*Annex A*)
- Keiran Hardy and George Williams, 'Special Intelligence Operations and Freedom of the Press' (2016) 41 *Alternative Law Journal* 160; (*Annex B*)
- Keiran Hardy and George Williams, 'Terrorist, Traitor or Whistleblower? Offences and protections in Australia for Disclosing National Security Information' (2014) 37 *University of New South Wales Law Journal* 784 (*Annex C)*

Below we outline the main findings of this research. After discussing press freedom and what it should require, we focus our comments in three areas: access to journalists' metadata, disclosure offences, and the broad statutory definition of national security.

In summary, we recommend that:

1. The federal Parliament enact clear, positive protection for freedom of speech and freedom of the press that operates to ensure specific national security or other laws are interpreted and applied in a way that respects these freedoms;
2. Journalist information warrants allowing access to metadata be available only in relation to serious crimes;

[2] Paul Karp and Josh Taylor, 'Police made illegal metadata searches and obtained invalid warrants targeting journalists', *The Guardian*, 23 July 2019.
[3] Luke Royes, 'AFP officer accessed journalist's call records in metadata breach', *ABC News*, 29 April 2017.

3. Journalists should be notified of the existence of such warrants, and be given an opportunity to contest them in a judicial hearing;
4. Offences for disclosing information, including s 35P and s 34ZS of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), should include an exemption for information disclosed in the public interest;
5. Intelligence disclosure offences should include a similar exemption, with an additional requirement that the employee reasonably believes other avenues for disclosing the information (i.e. internally and to the IGIS) have proved inadequate;
6. The penalties for copying, recording or receiving information should be significantly less than those for disclosing it. The definition of 'dealing' with information in the espionage and foreign interference laws should be amended accordingly;
7. Statutory definitions of national security should not extend to all matters relating to economics and foreign affairs. Accordingly, s 90.4(1)(e) of the *Criminal Code Act 1995* (Cth) (Criminal Code) should be repealed.

1. Freedom of the press

Freedom of the press is closely related to the freedom of expression in Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR). Article 19(2) requires that:

> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[4]

[4] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 19(2).

The United Nations Human Rights Committee believes a 'free, uncensored and unhindered press' is 'one of the cornerstones of a democratic society'.[5] The ability of media organisations to report freely on matters of public interest is essential not only for freedom of expression, but also to ensure transparency, accountability and the enjoyment of other human rights.[6] A properly functioning democracy requires the free flow of information between citizens and their elected representatives.[7] We might therefore describe press freedom as **a democratic right that is essential for achieving human rights, transparency and accountability of government, and the proper election of the people's representatives to Parliament.**

Press freedom should entail that media organisations are 'able to comment on public issues without censorship or restraint', and that they maintain their 'independence and editorial freedom'.[8] It also means that **members of the public have a corresponding right to access information freely from a diversity of sources**.[9] In other words, press freedom is not simply about the right of journalists to publish information; it implies that all members of the public have a right to access information that is important to making democratic decisions.

Press freedom is not an absolute right. It can be limited for reasons of national security. Article 19(3) of the ICCPR states that freedom of expression may be subject to restrictions, if those restrictions are provided by law and necessary 'for the protection of national security or of public order (*ordre public*), or of public health or morals'.[10] However, while the UN Committee recognises national security as a legitimate reason for restricting freedom of expression, it warns that criminal offences should not unduly restrict the publication of information in the

[5] United Nations Human Rights Committee, *General Comment No. 34, Article 19: Freedom of opinion and expression*, 12 September 2011 (CCPR/C/GC/34) 3.
[6] Ibid.
[7] Ibid 4.
[8] Ibid.
[9] Ibid.
[10] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 19(3).

'legitimate public interest'.[11] In particular, the UN Committee has stated explicitly that **prosecuting journalists for disclosing information in the public interest**, **where that information does not harm national security, will not comply with Article 19**.[12]

In other words, the question is not whether national security trumps press freedom, or vice versa. Rather, the question is twofold: (1) **whether specific laws, in their words or effect, burden freedom of expression by media organisations**, and (2) **whether those laws adopt means that are proportionate to achieving the legitimate end of national security**. This proportionality approach is consistent with the implied freedom of political communication recognised by the High Court.[13] That right derives from sections 7 and 24 of the *Constitution,* which require that members of both Houses of Parliament be 'directly chosen by the people'.

Unfortunately, Australian law does not currently provide clear and unambiguous protection for freedom of speech and freedom of the press in accordance with Article 19 of the ICCPR. This means that Parliament can enact laws in national security and other contexts without Parliament giving due weight to these freedoms. The result has been a disturbing number of laws that are inconsistent with basic democratic values. **This should be remedied by the federal Parliament enacting positive protection for freedom of speech and freedom of the press** that operates to ensure national security or other laws are interpreted and applied in a way that respects these freedoms.

In addition, existing laws should be amended where they disproportionately impact on freedom of speech and of the press.

---

[11] United Nations Human Rights Committee, above n 5, 7.
[12] Ibid.
[13] *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1; *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; *Coleman v Power* (2004) 220 CLR 1.

2. Access to journalists' metadata

As amended in 2015, the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) requires communications service providers (CSPs) to retain metadata for two years.[14] There is no definition of metadata in the legislation, but CSPs are required to retain information relating (amongst other things) to the time, date and location of communications passing over their services.[15] This is not trivial data, as it can reveal significant identifying and personal information about a person's contacts, communications, activities, and whereabouts.[16] This information can be accessed by ASIO and enforcement agencies without a warrant.[17]

Because accessing journalists' metadata may reveal their confidential sources, the legislation includes a journalist information warrant (JIW) scheme. A JIW allows a journalist's metadata to be accessed on application to a judicial authority, if the public interest in issuing the warrant outweighs the public interest in protecting the journalist's sources.[18] A JIW can be sought for any of the normal purposes for accessing metadata – namely, to further ASIO's activities, enforce the criminal law, find a missing person, or enforce a law that imposes a pecuniary penalty or protects the public revenue.[19] Journalists cannot contest these warrants, in part because they need not be notified of their existence. The first time a journalist is likely to suspect their metadata has been accessed by ASIO or law enforcement is when they become aware of an ongoing criminal investigation (for example, through a raid on their offices).

---

[14] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 187A, 187C.
[15] *Telecommunications (Interception and Access) Act 1979* (Cth), s 187AA.
[16] Will Ockenden, 'What reporter Will Ockenden's metadata reveals about his life', *ABC News*, 24 August 2015.
[17] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 177-180.
[18] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 180L, 180T.
[19] *Telecommunications (Interception and Access) Act 1979* (Cth), ss 180L, 180T.

Recently, the Ombudsman reported that metadata has been accessed repeatedly under the TIA Act without proper authorisation (including 116 times by ACT police).[20] Earlier revelations related to the unauthorised access of a journalist's metadata,[21] and the wide range of organisations accessing metadata beyond ASIO and law enforcement.[22] These reports confirm many of the issues raised in consultation on the metadata laws before their enactment.

Accessing journalists' metadata should be available only in the most serious cases (for example, where a journalist intends to harm national security by publishing security classified information). The laws themselves cannot prevent all human error or misuse, but the terms of the legislation need to be drafted in a way to minimise such possibilities. Currently, journalists' metadata can be accessed for a wide range of reasons, beyond prosecuting serious criminal offences, and by any organisation declared to be an enforcement agency.[23] The fact that journalists are not notified of a JIW means that an investigation with little basis could progress substantially and reveal confidential sources, even if the charges are ultimately dropped.

We recommend that journalists' metadata be available only for the purposes of investigating a serious criminal offence. This is currently the standard for accessing prospective metadata under the TIA Act.[24] Access should also be restricted to ASIO and criminal law enforcement agencies. The editor-in-chief (or equivalent) of a media organisation should be notified of the existence of a JIW in relation to their staff, so they can seek proper legal advice. The media organisation should then be permitted to contest the warrant by making submissions in court.

---

[20] 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 (November 2018).
[21] Royes, above n 3.
[22] Stephanie Anderson, 'List of agencies applying for metadata without warrant released by government', *ABC News*, 18 January 2016.
[23] *Telecommunications (Interception and Access) Act 1979* (Cth), s 176A.
[24] *Telecommunications (Interception and Access) Act 1979* (Cth), s 180.

These amendments would ensure procedural fairness for journalists, and strike a more appropriate balance between the needs to protect national security and freedom of the press.

3. Disclosure offences

In recent years there has been a significant legislative crackdown on the disclosure of classified information, including through strengthened offences for intelligence disclosures and espionage. Many other offences are designed to maintain operational secrecy, for example in relation to ASIO's special warrant powers and Preventative Detention Orders (PDOs).[25]

A number of these offences pose a direct risk to journalists. Section 35P of the ASIO Act applies a penalty of five years' imprisonment where a person discloses any information relating to a special intelligence operation (SIO) and the disclosure 'will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation'.[26] The person need only be reckless as to whether the disclosure will cause such harm, and the penalty is doubled to 10 years if the person intends or knows that such harm will result.[27]

This is a significant improvement on the original wording of the offence, which did not include any requirement as to the harm caused by disclosing the information. However, the offence is still likely to have a chilling effect on media reporting. In 2018, the UN Special Rapporteur on the Situation of Human Rights Defenders reported that Australian journalists may engage in self-censorship due to uncertainties over whether information relates to an SIO:

[25] *Australian Security Intelligence Organisation Act 1979* (Cth), s 34ZS; *Criminal Code Act 1995* (Cth), s 105.41.
[26] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35P(1).
[27] *Australian Security Intelligence Organisation Act 1979* (Cth), s 35P(1B).

> Given the overall secrecy of intelligence operations and without confirmation from ASIO, it is challenging for journalists to determine if an activity of interest would be a special intelligence operation. Due to high sanctions, the provision may lead to self-censorship by the media, which may take a more cautious approach to reporting on ASIO's activities.[28]

Another area of concern is the recently amended espionage offences. Under section 91.1(2) of the Criminal Code, a person faces 25 years imprisonment if they 'deal' with information that 'concerns Australia's national security' and they are reckless as to whether they will prejudice national security as a result.[29] The definition of 'dealing' with information includes not only communicating or publishing information but also receiving, possessing, copying, or making a record of it.[30] A penalty of up to 20 years' imprisonment is available even if the information itself does not have a security classification or relate to national security.[31]

Under these laws, journalists and other people are subject to criminal penalty for merely receiving or possessing sensitive information (not necessarily relating to national security), even before they decide to publish it. This raises the possibility that a newsroom may be raided to prevent (rather than respond to) the disclosure of information leaked to journalists by a government employee. While the recent raids on the ABC headquarters related to the publication of information 2 years prior, it is possible under these laws that a newsroom could be raided pre-emptively to prevent publication in the first instance. Such an event would be unacceptable in a modern liberal democracy that values freedom of the press.

---

[28] Human Rights Council, *Report of the special rapporteur on the situation of human rights defenders on his mission to Australia*, 28 February 2018 (A/HRC/37/51/Add.3) 7.
[29] *Criminal Code Act 1995* (Cth), s 91.1(2).
[30] *Criminal Code Act 1995* (Cth), s 90.1.
[31] *Criminal Code Act 1995* (Cth), s 91.2(2).

Also relevant are offences for intelligence officers under the *Intelligence Services Act 2001* (Cth) (ISA). Again, these relate both to disclosures and 'unauthorised dealing with records'.[32] While journalists cannot be prosecuted under these provisions, their offices could be searched or their metadata accessed to discover the source of a leak within an intelligence agency.

These espionage and disclosure offences should be viewed in light of the lack of whistleblower protections for journalists and intelligence officers. While the *Public Interest Disclosure Act 2013* (Cth) (PID Act) creates a whistleblower scheme for public employees, the scheme does not apply to journalists and there are no adequate protections for disclosing intelligence information in the public interest.[33] Of course, intelligence officers who leak information with intent to prejudice Australia's national security or defence should certainly be punished. However, there is no legal mechanism for an intelligence officer to disclose publicly, for example, that colleagues had tortured a suspect or embezzled money during an undercover operation. Disclosures about misconduct must be made internally to the organisation in the first instance, or to the IGIS.[34] These mechanisms may be appropriate in many cases, but there is no separate protection for intelligence whistleblowers if these avenues prove inadequate.

We recommend that offences for disclosing information – including s 35P of the ASIO Act, the espionage laws, intelligence disclosure offences, and offences relating to ASIO's special warrant powers and PDOs – include a limited public interest exemption to protect freedom of the press. For intelligence officers, this should include a requirement that the officer reasonably believes other avenues, such as disclosure internally and to the IGIS, have been ineffective.

---

[32] *Intelligence Services Act 2001* (Cth), ss 39-40M.
[33] See Keiran Hardy and George Williams, 'Terrorist, Traitor or Whistleblower? Offences and protections in Australia for Disclosing National Security Information' (2014) 37 *University of New South Wales Law Journal* 784.
[34] *Public Interest Disclosure Act 2013* (Cth), s 34.

This should be achieved by permitting the publication of information in the 'public interest'. It is important that this term be defined both so that the ambit of protection is clear, and so that it does not permit reporting in unacceptable circumstances. The definition should allow the publication of information that discloses serious wrongdoing. Section 29 of the PID Act provides a model.[35] That section, which defines 'disclosable conduct', relates to conduct by government which:

- contravenes a law;
- perverts the course of justice;
- constitutes maladministration;
- is an abuse of public trust;
- wastes public money;
- unreasonably results in a danger to health or safety; or
- increases a risk of danger to the environment

In addition, offences for receiving, possessing, copying information should receive substantially lesser penalties than those for disclosing information. This is currently the case in the ISA, but not for the amended espionage laws. The catch-all definition of 'dealing' with information should be amended to account for these differing levels of seriousness.[36]

4. Definition of national security

A final issue relates to the broad definition of national security under the recently amended espionage laws. The longstanding definition of 'security' in the ASIO Act is already very broad in extending beyond defence, border protection and national security matters to 'communal'

[35] *Public Interest Disclosure Act 2013* (Cth), s 29.
[36] *Criminal Code Act 1995* (Cth), s 90.1.

and 'politically motivated' violence.[37] Conduct satisfies that definition even if it does not relate to terrorism or otherwise have country-wide implications.

Under the new espionage and foreign interference laws, national security is defined even more broadly to include anything relating to Australia's 'political, military or economic relations' with other countries.[38] A like approach can be seen in the recently enacted encryption laws.[39] This confirms that journalists could be prosecuted under the espionage laws for receiving or possessing information that is broadly relevant to Australia's economic or foreign interests, far beyond matters relating to terrorism, military operations, or similarly serious events.

This is an unacceptable widening of the concept of national security in Australian law. Considerations of economics and foreign affairs can certainly be relevant to national security. However, it does not follow that all matters relating to economics and foreign affairs have national security implications. To limit the possible scope of the espionage offences with respect to journalists, we urge the committee to recommend that s 90.4(1)(e) of the Criminal Code (relating to political, military or economic relations with other countries) be repealed.

[37] *Australian Security Intelligence Organisation Act 1979* (Cth), s 4.
[38] *Criminal Code Act 1995* (Cth), s 90.4(1)(e).
[39] *Telecommunications Act 1997* (Cth), s 317L.

Yours sincerely,

Dr Keiran Hardy

Lecturer, School of Criminology and Criminal Justice, Griffith University; Postdoctoral Research Fellow, Griffith Criminology Institute

Professor George Williams AO

Dean, Anthony Mason Professor, Scientia Professor and Founding Director, Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales