Submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the impact of law enforcement and intelligence powers on the freedom of the press

The submitters

This submission is made by Associate Professor Johan Lidberg and Dr Denis Muller. Associate Professor Lidberg is the deputy head of journalism and the director of the Master of Journalism program at Monash University. Dr Muller is a senior research fellow at the Centre for Advancing Journalism at the University of Melbourne. They are the editors of In the Name of Security – Secrecy, Surveillance and Journalism, published in 2018 by Anthem Press (ISBN-13: 978-1-78308-769-3). The book predicted the situation for media freedom and civil liberties in Australia that prompted this inquiry. They would be willing to appear at the inquiry if required.

Introduction

Since the September 11, 2001 attacks on the United States, Australia has passed more than 70 pieces of legislation under the rubric of national security. These laws have been of unprecedented reach (Williams 2011, 1137) and the parts impacting adversely on journalism have come about somewhat randomly (Pearson & Fernandez 2018, 64). Random or not, the effect has been to create a highly repressive interlocking web of laws which seriously impedes the ability of the media to perform its democratic function of carrying out public-interest journalism, and to protect its sources of information.

This submission should be read in conjunction with submission six from the Journalism Education and Research Association Australia and submission 19 from Associate Professor Joseph Fernandez. These submissions complement ours in raising points tangential to the principal issues we raise.

The key question that needs to be posed is why Australia is the only country among the Five Eyes intelligence-sharing community, and indeed among mature liberal democratic countries, that see a need to equip its security and intelligence agencies with powers that extend to issuing and executing search warrants against individual journalists and media organisations justified by hunting down public interest whistleblowers in the name of national security? In no other mature liberal democracy do we observe a public discourse or parliamentary inquiries into media freedom and civil liberates driven by the passing or amendments of national security laws to the extent that we see in Australia (Lidberg and Muller, 2018). This makes Australia an outlier. We put it to the inquiry – is that what we want to be? An outlier when it comes to media freedom and civil liberties in the liberal democratic world? These questions are especially pertinent given the rise of autocratic leaders in the world, such as Donald Trump (USA), Victor Orban (Hungary), and Jair Bolsonaro (Brazil) who vehemently question liberal democracy as manifested by free speech and media freedom and the independent rule of law. Here it is important to point out that although this inquiry focuses on media freedom, this problem extends well beyond media, covering all civil liberties that make up the fabric of liberal democratic systems.

To make matters worse, Australia alone among the Five Eyes countries has no constitutional or quasi-constitutional protection for freedom of the media or indeed civil liberties generally. Thus, the Australian media is caught in a pincer between laws that criminalise journalism and the absence of a robust specific legal framework against which the enactment and use of those laws can be challenged and moderated.

There has been inadequate resolve to protect the public interest by ensuring that journalists and journalism are able to properly perform their professional duties and obligations (Pearson & Fernandez 2018, 51).

As the distinguished media lawyer Peter Bartlett recently put it in *The Australian* (22 July 2019), while freedom of the press is not enshrined in Australia's Constitution, it serves as a fundamental aspect of our democracy. He argued that this required recognition of the principle that journalists should be allowed to communicate and

publish effectively without governmental interference, threats of retribution, and onerous legal or economic pressures, subject to reasonable legal limitations.

Bartlett's argument pinpoints the central problem: how to balance the need to keep the nation safe and the rights of citizens to know what government is doing in their name.

As the interlocking web of laws enacted under the rubric of national security has grown since 2001, the powers of government to interfere in the work of the media, the threats of retribution and the consequent legal and economic pressure have grown accordingly. As a result, we argue, the balance has tilted too far towards national security considerations at the cost of the right of the population to know what government is doing.

In this submission, we specify aspects of the national security laws which we say have created this imbalance and propose an approach to remedying the situation. The overall point to make is that the Australian lawmakers have, since September 11, 2001, created a web of national security and anti-terror laws so extensive and punitive that covering national security in that any meaningful way holds power to account has become very hard and at times borders on the impossible. This means that a number of journalists and media outlets back away from covering national security to minimise legal risks to reporters and their organisations. This is not good for a healthy liberal democracy where scrutiny of power by independent media is an important democratic property.

In addition to the national security laws, there are a number of other laws that create offences inimical to press freedom, in particular the secrecy of information law contained in Part 5.6 of the Commonwealth Criminal Code, 1995, and the Public Interest Disclosure Act 2013. The obstructive way in which government agencies administer the Freedom of Information Act 1982 is a further barrier to media freedom.

We will deal with each of these in turn. But first, it is useful to summarise our recommendations.

- Review the sections of our criminal codes that make it a crime for public servants to disclose corruption and maladministration to third parties, including journalists. Whistleblowers should be properly protected and not pursued if their disclosures are in the public interest.

- Our national security and anti-terror laws should be reviewed annually asking the question: "Do we really need this level of power for the intelligence and security agencies?" If the answer is no, we need to roll back their powers by amending and changing the laws.

We need to amend the federal Freedom of Information (FOI) law to include our intelligence and security agencies. This sends a signal of accountability and transparency. Case in point: the US Central Intelligence Agency is **not** exempt from US FOI law, which is similar to the FOI systems in close to all liberal democratic countries.

We need a bill or charter of rights explicitly protecting our civil liberties such as freedom of speech and media freedom. If we can't get a constitutional bill of rights through Parliament, the second-best option is a Media Freedom and Civil Liberties Act. Either of these options would be a way to get the national security and democratic freedom seesaw back in balance.

The national security laws

The problems

The oppressiveness of these laws begins with the scope of the term "national security". It has become a Humpty Dumpty term: that is to say, it can mean anything the Government wants it to mean. For instance, the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 – which was enacted as part of the panoply of national security laws already mentioned -- can be used for any of the following purposes:

- to enforce the criminal law;
- to find a missing person;
- to enforce a fine or protect the public revenue, or
- to investigate offences against the criminal law of a foreign country.

While it is possible to imagine circumstances in which any of these might conceivably impinge on national security considerations, this provision is so broad as to unreasonably burden the freedom of the media. It is a concrete example of how the imbalance between national security and freedom of the press has come about.

For free-media purposes, the term national security should be narrowly defined as matters concerning the sovereignty and safety of the nation and its people. If legal action is brought against the media on national-security grounds, the onus should be on the prosecution or plaintiff to prove any connection between the media activity complained of and risk to the sovereignty and security of the nation and its people.

This principle should apply throughout all the national security laws. It should be one of two standard tests applied before any legal action is taken against the media on national-security grounds. The other is a public-interest test. We argue, then, that in order to get an action against the media off the ground, two elements should be proved beyond reasonable doubt in criminal proceedings and on the balance of probabilities in civil proceedings. The first element is that the matter complained of did in fact concern national security as defined above. The second element is that there was no public interest in the publication of the material. Failure to prove either of these should render the proceedings invalid.

The law has defined the public interest in many ways but none of these definitions has been accepted as universally satisfactory or authoritative. For present purposes, we propose that the concept of the public interest should encompass the performance of parliament, executive government, the judiciary and public institutions, as well as considerations of public health and safety and matters on which the citizen needs to be informed in order to participate in political, economic and social life.

Beyond these definitional questions lie a wide range of specific oppressions contained in the national security laws. We do not pretend to identify all of them in this submission but we do identify what we regard as the most egregious of them.

In 2003, Parliament enacted *The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act*, giving ASIO power to seek warrants to question and detain people for up to seven days, without telling the detained person the grounds on which the warrant was issued.

The Media Entertainment and Arts Alliance published a report in 2005 that set out its concerns about the implications of these amendments for the practice of journalism. The MEAA's main concern was that the amendments prevented any media scrutiny of the current operations of ASIO, including any scrutiny of these extra-judicial detentions, even where they violated international human rights conventions.

There is no public-interest test by which journalistic scrutiny might be permitted, and no media exemptions from the operation of the amendments. Concretely, a journalist who may reveal by his or her writings to have good information about matters of national security could be detained under these provisions, and any person detained, or knowing about the detention, is prohibited from speaking to anyone about it. It is a gag accompanied by serious infringements on civil liberties, being detention in secret without charge or judicial review.

Looked at from a media-freedom and human rights perspective, this law is an abomination and an affront to democracy. Not only does it contravene the doctrine of habeas corpus but it completely shuts out any press scrutiny of the use by the security services of these extraordinary powers. It invites the conclusion that if a democratic government is prepared to abandon such fundamental rights as part of a so-called war on terror, it has handed the terrorists a win.

In 2005, Parliament enacted *The Anti-Terrorism Act (No. 2)*, which defined what constituted a terrorist organization, created new offences and gave federal agencies

new powers, including the power to impose "control orders" on people. These control orders have the effect of restricting their freedom of communication and association.

The Act makes it an offence to disclose the fact that the federal police have given notice to someone to produce documents relating to a serious terrorism offence. A journalist who writes that such a notice has been issued could face up to two years' imprisonment for doing so.

In 2014, Parliament enacted the *National Security Legislation Amendment ACT (No 1)*. Section 35P of that Act makes it an offence to disclose information relating to a "special intelligence operation" or SIO. Because of other national security laws, it is impossible to know what SIOs are on foot, and so it is possible for a journalist to write unwittingly about one and so fall foul of this law. For a prosecution to succeed, it is sufficient for the Crown to prove that the publication was reckless. The Crown does not need to prove that the journalist intended to damage national security or did actual damage.

The penalty for mere disclosure is imprisonment for up to five years. If it does do actual damage or places at risk the health or safety of anyone or prejudices the success of an intelligence operation, the penalty is up to ten years' imprisonment.

In May 2015, Parliament enacted the *Telecommunications (Interception and Access) Amendment (Data Retention) Act*. This is the "metadata" law already mentioned. It has serious implications for the press because it provides a powerful tool to help government to track down journalists' sources.

The Act requires internet service providers to retain metadata for two years and contains a schedule setting out what this consists of:

- information that identifies the subscriber to a telecommunications service – their name, address or any other identifying information;
- details of the contract they have with the service provider, including the type of devices they have and the billing and contact information;

- information that identifies the source of a communication, including details of the device, type of service and the account used;
- information that details the destination of a communication;
- the date, time and duration of a communication;
- the type of communication used – voice, SMS, email, social media etc;
- the type of service used – ADSL, Wi-Fi, VoIP, cable etc;
- the features of the service – call waiting, call forwarding, data volume usage;
- the location of the equipment or line used – cell towers, Wi-Fi hotspots

The Act empowers the Minister for Communications to modify this list by use of a legislative instrument such as a new law or an amendment to an existing law, making it relatively easy for the Minister to add to it.

The Act contains some limited protection for journalism.

If an agency – including the intelligence agencies and the federal police -- wants metadata that would identify a journalist's source, the agency must obtain a warrant to do so. However, the warrant system is weak. The agency can get a warrant from a judge, a magistrate, or a lawyer-member of the Administrative Appeals Tribunal.

In addition, the Director-General of National Security can ask the Minister for Communications for a warrant, specifying the grounds for the request. In deciding whether to issue a warrant, the Minister must apply a public-interest test: Does the public interest in issuing the warrant outweigh the public interest in protecting the confidentiality of the identity of the journalistic source?

In applying this test, the Minister must have regard to:

- the privacy of any person affected by the warrant;
- the gravity of the matter;
- the extent to which the information obtained under the warrant would assist the intelligence agency's work;
- whether reasonable efforts have been made to get the information by other means;

- any submissions by the Public Interest Advocate (an office created under the legislation to put public-interest-related arguments).

In circumstances of urgency, the Prime Minister, the Defence Minister or the Foreign Affairs Minister may give oral consent to the issuing of a warrant, and the Director-General of Security is himself empowered to issue a warrant if the situation is urgent, no minister is available and security will be, or is likely to be, seriously prejudiced if the warrant is not issued.

It is obvious that obtaining a warrant is a relatively easy task. If the application comes before a judge, there is some chance that the grounds for the application will be carefully scrutinised. Otherwise, it is likely to be rubber-stamped. For that reason it is likely that an agency will apply instead to a lesser official – a magistrate, a lawyer-member of the AAT, or try to route it through the political processes by getting an application before a Minister, or declare it to be urgent and get it through the Director-General of Security or orally by a senior Minister.

It is only human for law-enforcement officials to take the easiest route to getting a warrant. This was vividly illustrated by the way the Australian Federal Police obtained the warrant to raid the headquarters of the ABC in June 2019 over the story which has become known as the Afghan Files. The police obtained their warrant from a local court registrar in Queanbeyan. That can hardly be seriously considered as judicial review of the warrant application.

In 2017, Parliament enacted the *National Security Legislation Amendment (Espionage and Foreign Interference) Act.*

This law makes it an offence punishable by anything from two to fifteen years' jail for a person who does any of the following in relation to national security information:

(a) receives or obtains it;

(b) collects it;

(c) possesses it;

(d) makes a record of it;

(e) copies it;

(f) alters it;

(g) conceals it;

(h) communicates it;

(i) publishes it;

(j) makes it available.

Dealing with information includes:

(a) dealing with all or part of it; or

(b) dealing only with the substance, effect or description of it.

It is a defence that the person dealt with or held the information:

(a) in the public interest, and

(b) in the person's capacity as a journalist engaged in fair and accurate reporting.

However, the defendant bears the evidential burden in relation to this. And the criterion of "fair and accurate reporting" is so subjective as to seriously weaken the defence. Who decides what is fair, for instance? A government embarrassed by a disclosure is likely to argue strenuously that the reporting was unfair, regardless of the objective merits of the story.

Schedule 2 of this Act incorporated Part 5.6 of the Criminal Code Act 1995. That part is headed "Secrecy of Information". It defines two general categories of information:

- Inherently harmful information (Section 122.1).
- Information likely to harm Australia's interests (Section 122.2).

Inherently harmful information means any information that:

- Has a security classification attached to it, or
- Belongs to one of the intelligence services, or
- Relates to the operations of an intelligence service or a law-enforcement agency.

A public servant or a former public servant who leaks inherently harmful information either intentionally or recklessly faces a maximum term of imprisonment of seven years. A public servant or former public servant who leaks information likely to harm Australia's interests either intentionally or recklessly also faces a maximum seven-year jail sentence.

There is nothing in the legislation to say what general classes of information might fall within the definition of information "likely to harm Australia's interests". As a one-time investigative reporter, Ross Coulthart, once said, it could be the office Christmas card.

There is a further section, 122.3, which is headed "aggravated offence". Under this section, it is an aggravated offence for a public servant or a former public servant to leak:

- Any document marked "for Australian eyes only", or
- Five or more records that have a security classification.

This carries a maximum prison term of between five and ten years, depending on certain technical details.

Material leaked to the ABC about alleged war crimes committed by Australian soldiers in Afghanistan – the Afghan Files story for which the ABC was raided in June 2019 -- would be an aggravated offence because it was marked "for Australian eyes only" and it consisted of more than five records with a security classification.

The effect of Sections 122.1 and 122.2 is to leave it open for the Government to decide what information can be used to form the basis of charges under these laws. Thus the law is open to abuse through arbitrary enforcement of the kind that we have seen with the raids by the Australian Federal Police on the ABC and the News Corp journalist Annika Smethurst in early June 2019.

And just to be sure that no information at all can escape the reach of this law, Section 122.4 makes it an offence for a public servant or former public servant to disclose any

Government information at all that they received in the course of their work and had a duty to keep secret.

It is a defence to a prosecution that the person communicated, removed, held or otherwise dealt with the relevant information in the person's capacity as someone engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media, and:

- at that time, the person reasonably believed that engaging in that conduct was in the public interest, or
- was, at that time, a member of the administrative staff of news organisation, and
- acted under the direction of a journalist, editor or lawyer in the organisation who reasonably believed that engaging in that conduct was in the public interest.

The defendant once more bears the burden of proving their innocence.

The remedy

The entire body of national security legislation should be comprehensively reviewed against a set of principles concerning freedom of the media. These principles should include, as a minimum:

- That the media is entitled to a public-interest defence in every case.
- That the laws are enforceable against the media only in circumstances where their conduct creates a clear and present danger to the health and safety of the public or to the security of Australia.
- That for the purposes of press freedom the term national security is defined narrowly so that it refers to the sovereignty and safety of the nation and its people.
- That the performance of the security services should be just as much an object of public scrutiny as that of any other part of government.
- That judicial supervision of any warrant system used for pursuing journalists or their sources should be in the hands of a judge of a superior court.
- That *intention* to harm national security should be the fault standard for any prosecution of the press, not mere accident or inadvertence.

- That the onus of proof in all cases rests on the prosecution.

The secrecy of information laws

These laws have been dealt with above as part of our argument about the national security laws. However, the secrecy of information laws as embodied in Part 5.6 of the Criminal Code Act, 1995 requires review and amendment to reflect the arguments made about them in the section above.

Information "likely to harm Australia's interests" is not defined. It is an open-ended catch-all that is used to go after public servants who leak and the journalists who publish those leaks.

Apart from their inherently oppressive nature, these laws leave it open for the Government to decide what information can be used to form the basis of prosecutions. Thus the law is vulnerable to abuse through arbitrary enforcement. There have been three recent cases to illustrate this arbitrariness.

In two cases, the Australian Federal Police embarked on criminal investigations against journalists under these laws, and in the third case the police did not embark on an investigation.

The two cases that became the subject of the police investigations were deeply embarrassing to the Government. One was the story by Annika Smethurst of the *Sunday Herald Sun* that the Government was contemplating allowing the Australian Signals Directorate to spy on Australian citizens in Australia. The second was the Afghan Files story already referred to. It contained allegations that Australian troops fighting in Afghanistan may have committed war crimes.

The third case arose from a leak of information concerning the security implications arising from the passage of what has become known as the medevac legislation. This provides for asylum-seekers on Manus Island and Nauru to be brought to Australia for

medical treatment. The passage of this law represented a defeat for the Federal Government, which then staged a public relations stunt to highlight what it claimed were the risks to national security caused by the new law. The stunt involved the Prime Minister making a one-day trip to Christmas Island where the detention centre was momentarily re-opened and a press conference held there.

Coincidentally, *The Australian* newspaper published a substantial leak about the stated security implications of the medevac law. The leak was of such magnitude that Duncan Lewis, the Director-General of ASIO, made a public statement strongly protesting against it because, as *The Age* reported (31 July 2019, P5) it represented a "seriously damaging" breach of security. The secretary of the Home Affairs Department, Mike Pezzullo, said the impact on his agency had been "critical" – the highest possible level.

Yet the AFP did not investigate this leak, saying that an internal IT audit done by Home Affairs showed that more than 200 people had been on the email address list for the information and that to try to track down the leaker "would not be an efficient or effective use of AFP resources".

These three cases tell us that enforcement of the secrecy laws is hostage to political considerations. This places the AFP in an untenable position because it gives the appearance of a police force making decisions about prosecutions based on political factors, when in fact it is more likely that the question of whether there is a reference to them from the Government is decided by other agencies or by ministerial offices on political grounds. Indeed in the medevac case, the Labor Party has stated its belief that the AFP did not investigate because to do so risked embarrassing the Government. We argue that this situation undermines public confidence in the operational independence of the AFP.

A threshold question that we say the Committee should address is this: should leaks of government information to the media that do not concern national security, defined narrowly, be subject to the criminal law? We argue that they should not be. This is one more way in which the imbalance between government secrecy and the public right to know what the government is doing could be redressed.

Beyond these overarching issues of scope and arbitrary enforcement, the secrecy-of-information laws contain serious attacks on press freedom.

Journalists' liability is set out in the same part of the Criminal Code as public servants' liability.

It states that anyone who receives, deals with or publishes the classes of information described in the law are also liable to be prosecuted, along with the leaker.

That is a clear attack on the freedom of the media.

There is a public-interest defence, but how it works is very uncertain.

The law says it is a defence if:

- The defendant was acting in the capacity of a journalist reporting news, presenting current affairs or expressing editorial or other content in news media, and
- Reasonably believed that receiving and publishing the information was in the public interest.

This looks all right on the surface but there are several pitfalls in it.

First, who is a journalist? Everyone engaged in doing news journalism, including bloggers and citizen journalists? Or only those employed by big media organisations?

Second, what is in the public interest?

Third, what constitutes a "reasonable belief"?

Finally, the onus is on the journalist to prove his or her innocence beyond reasonable doubt. That is the reverse of the usual practice in criminal law where the onus is on the prosecution to prove guilt.

The entire Part 5.6 of the Criminal Code Act needs to be rewritten, narrowing its scope to information which, if leaked, would present a clear and present danger to public health or safety or national security narrowly defined.

The public interest needs to be defined; the Act needs to make it clear that anyone doing journalism is presumed to be entitled to the public-interest defence, "reasonable belief" needs to be dropped, and the onus of proof should be laid on the prosecution.

Whistleblower laws

At Commonwealth level, these are contained in the Public Interest Disclosure Act 2013. Professor A. J. Brown, who helped to try to make something workable out of an exceptionally flawed first draft, has called it a dog, and he is right. Fortunately, it is about to be reviewed. In principle, the findings from this inquiry need to harmonise with the findings from that review, but without knowing the outcome of either exercise, it is impossible to mount an argument based on events that have yet to unfold.

However, as matters stand, the Act states that its purpose is to:

- promote the integrity and accountability of the Commonwealth public sector;
- encourage and facilitate the making of public interest disclosures by public officials;
- ensure that public officials who make public interest disclosures are supported and are protected from adverse consequences relating to the disclosures, and
- to ensure that disclosures by public officials are properly investigated and dealt with.

Fine words. But they have severe limitations, especially where journalism is concerned.

Broadly speaking, a public interest disclosure is a disclosure of information, by a public official, that is:

- a disclosure within the government, to an authorised internal recipient or a supervisor, concerning suspected or probable illegal conduct or other wrongdoing (referred to as "disclosable conduct"); or
- a disclosure to anybody, if an internal disclosure of the information has not been adequately dealt with, and if wider disclosure satisfies public interest requirements; or
- a disclosure to anybody if there is substantial and imminent danger to health or safety; or
- a disclosure to an Australian legal practitioner for purposes connected with the above matters.

There are questions about the meaning of "anybody". There is no explicit mention of journalists as being among those to whom a protected disclosure can be made. It might reasonably be supposed that "anybody" would include the media, but it is far from clear whether it does. After a couple of general references to "anybody", the Act falls silent, leaving it completely unclear as to who "anybody" might be.

In June 2019, a whistleblower from the Australian Tax Office, Robert Boyle, was indicted on charges of breaching laws on handling public documents and recording phone calls when he blew the whistle on the Tax Office's mistreatment of taxpayers. This mistreatment involved aggressively pursuing tax debts, including by taking money directly out of a taxpayer's bank account without their knowledge or consent.

Boyle seemed to have followed the whistleblower rules as set out in the Public Interest Disclosure Act. He had raised his concerns inside the Tax Office. The Tax Office conducted an investigation but it was a whitewash. Boyle then went to the ABC and the Fairfax newspapers. As a result he was charged with 66 offences of breaching public service regulations. Altogether these carried a maximum cumulative prison term of more than 160 years.

Before laying charges, the Tax Office offered Boyle a settlement consisting of a monetary payout and a statement of service, but he would have to sign a gag order preventing him from going public. Hush money, in other words. He refused to sign and was then charged.

The fact that the Tax Office offered him a settlement indicates it knew his complaint was justified and its only interest was in hushing up the bad behaviour of its debt-collectors. In fact, the Tax Office did make some changes to its debt-collecting methods after his complaint.

This is similar to another case involving a former Customs officer called Allan Kessing. He wrote an internal report pointing out serious security breaches at Sydney Airport. Criminals and people without proper security checks were being employed as baggage-handlers. His report was ignored. In desperation he gave the report to *The Australian* newspaper. He was prosecuted and given a nine-month suspended jail sentence. The Customs service, meanwhile, did a $220 million upgrade of security at Sydney Airport.

So for all the fine words of the Public Interest Disclosure Act, the instinct of the bureaucracy is to protect itself, not the people who blow the whistle on their wrongdoing. In the interests of media freedom, this inquiry needs to address the role of the media in being the means by which the objectives of the Public Interest Disclosure Act are given effect to. Because there is a separate review of the Act on foot, it is not necessary for this inquiry to address the manifold shortcomings in the Act. But it is necessary for this inquiry to explicitly lay out and recognise some principles concerning the fourth-estate function of the press in a liberal democracy, what is generally called the watchdog function. That requires the media to act in ways that hold power to account. Reporting what whistleblowers disclose is a central aspect of that function.

Media freedom laws

Much though we would like to advocate an amendment to the Constitution to entrench press freedom, we are realistic enough to know that the chances of that happening approach zero. Instead we propose that the Government should enact a charter of basic

rights, including the right of freedom of speech and of the media, similar to the charters of rights in Victoria and the ACT and the Bill of Rights in New Zealand.

These provide a mechanism against which laws trespassing on press freedom can be publicly tested on the floor of the Parliament and in general public debate, and against which judges can interpret the meaning of such laws. The core idea is contained in section 6 of the New Zealand Bill of Rights. This provides that where an enactment can be given a meaning that is consistent with the provisions of the Bill of Rights, that meaning shall be preferred over any other meaning. This allows judges to interpret the law in ways that are consistent with the provisions and intentions of the Bill of Rights.

Specifically, New Zealand's *Intelligence and Security Act 2017* acknowledges in its objectives that the protection of the country's national security must be pursued in accordance with the country's human rights obligations and in a way that enables there to be effective transparency for the purpose of democratic accountability and as a check on abuse of power.

The present situation concerning media freedom at law in Australia is deeply unsatisfactory. The so-called free speech cases in the High Court, culminating in the creation of an implied right to freedom of speech on matters of government and politics in *Lange v the Australian Broadcasting Corporation* (1997) 189 CLR 520, have proved to be of extremely limited value in practice. The reasonableness test attached to *Lange* has been strictly applied by the courts so that in cases where *Lange* qualified privilege has been used to defend defamation actions, the defence has generally failed.

An implied freedom is a poor substitute for an explicit one, and confining it to matters of government and politics imposes boundaries on the application of the defence which are indefensible in a democratic polity. Campbell and Crilly (2011, 61), surveyed the position in some detail, and concluded that "the constitutional protection of political communication provides a false assurance that courts are protecting and nourishing the public interest in open and free communication".

For these reasons, we say this inquiry should recommend a media freedom law similar to that contained in the New Zealand Bill of Rights. Rightly designed, such a law would go a long way towards addressing the current gross imbalance between national security powers and media freedom and civil liberties. Something similar was proposed by the Australian Human Rights Commission as long ago as 2008. It is time it was done so that Australia may join the fold of liberal democracies using best practice in this field.

References

Campbell, T. and Crilly, S. 2011. 'The implied freedom of political communication twenty years on'. University of Queensland Law Journal, 30(1): 59-78.

Lidberg, J. and Muller, D. 2018. *In the name of security – secrecy, surveillance and journalism*. Anthem Press

Pearson, M. and Fernandez, J. 2018 'Surveillance and Nation and National Security "Hyperlegislation" – Calibrating Restraints and Rights with a Freedom of Expression Threshold'. In *In the name of security – secrecy, surveillance and journalism.* Eds Lidberg, J. and Muller, D. pp. 51-73. Anthem Press.

Williams, G. 2011. 'A decade of Australian Anti-Terror Laws'. *Melbourne University Law Review,* 35: 1136-1176.