THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Press Freedom

Senate Standing Committees on Environment and Communications

30 August 2019

Coordinating Author
Dr Rebecca Ananian-Welsh

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Table of Contents

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Introduction

For more than a century, The University of Queensland (UQ) has maintained a global reputation for delivering knowledge leadership for a better world.

The most prestigious and widely recognised rankings of world universities consistently place UQ among the world's top universities.

UQ has won more national teaching awards than any other Australian university. This commitment to quality teaching empowers our 52,000 current students, who study across UQ's three campuses, to create positive change for society.

Our research has global impact, delivered by an interdisciplinary research community of more than 1500 researchers at our six faculties, eight research institutes and more than 100 research centres.

The TC Beirne School of Law is a global centre of research excellence contributing to the understanding and development of law nationally and internationally, and the effectiveness of law as a discipline, across a broad range of legal and policy issues.

The School of Communication and Arts brings together a wealth of expertise and creativity across all facets of communication, journalism, writing, literature, art history and the arts at UQ. Under the UNESCO Chair in Journalism and Communication, the School of Communication and Arts is positioned as a leader in press freedom research.

The School of Political Science and International Studies is recognised nationally and internationally as a leading school that translates complex ideas and problems into transformative research. In particular, its staff conduct cutting edge research in freedom of speech, national security laws and security policy.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Summary and recommendations

Thank you for the opportunity to make a submission to this Inquiry.

We welcome this Inquiry's focus on the protection of press freedom and note our earlier submission to the Parliamentary Joint Committee on Intelligence and Security's Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press (the **PJCIS Inquiry**), which overlaps in some respects. Our submission is based on multidisciplinary research on the impact of national security laws on press freedom, combining detailed legal analysis with empirical research and interviews.

The importance of a free press cannot be overstated. However, it has often been overlooked in the development and expansion of Australian security laws. As the United Nations Human Rights Committee recognised in respect of the International Covenant on Civil and Political Rights:

> A free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other Covenant rights. It constitutes one of the cornerstones of a democratic society. The Covenant embraces a right whereby the media may receive information on the basis of which it can carry out its function. The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion. The public also has a corresponding right to receive media output.[i]

Press freedom thus extends not only to the protection of journalists and media organisations in the conduct of their work, but to the protection of confidential sources and the public's right to know.

A healthy democracy requires that government operates with the greatest possible degree of openness and transparency. We recognise, however, that government requires a degree of secrecy in order to operate effectively and to protect national security. Thus, both secrecy and openness are required in order for Australian society and democracy to thrive.

Our core submission is that transparency and accountability must be defining characteristics of the Australian government, and that exceptions to this must be narrowly tailored to suit the national interest. A combination of legislative complexity and overreach have fostered a culture of secrecy in the public sector and undermined press freedom in Australia.

Importantly, unlike other Western liberal democracies, Australia lacks codified national protection for freedom of speech or the associated freedom of the press. Thus, our Five Eyes partners operate within a human rights legal framework fundamentally different to our own. In addition, those nations grant significant legislative protections to journalists not seen in Australia. Press freedom is at particular risk here and that deficit calls for urgent redress. Our international standing, reputation and relations rely on our capacities to ensure security and the rule of law, just as they do on our capacities to ensure press freedom. These points are expanded in the below submission.

Recommendations outlined in this document are:

1. Amend the General Secrecy Offence to protect press freedom.
2. Provide exemptions from prosecution to protect press freedom.
3. Clarify when a foreign media organisation will qualify as a foreign principal.
4. Require that media warrants be issued by a judge in contested proceedings.
5. Consider extending a form of privilege to journalistic materials.
6. Extend whistleblower protection to intelligence officers and operations.
7. Review public sector culture and practices with respect to media inquiries.
8. Amend and clarify legal definitions of national security.
9. Introduce a Media Freedom Act.

Terms of reference

a. Disclosure and public reporting of sensitive and classified information, including the appropriate regime for warrants regarding journalists and media organisations and adequacy of existing legislation

1. Disclosure and secrecy offences

1.1. The chilling effect

Australia's disclosure and secrecy regimes have expanded significantly in recent years, including through the introduction of new criminal offences. Most prominently, the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (***Espionage Act***) amended the *Criminal Code* to introduce broadly framed foreign interference and secrecy offences, as well as 27 new espionage offences. These schemes sit alongside other secrecy and disclosure offences, including 'gag' style offences relating to Special Intelligence Operations by ASIO, preventative detention orders and ASIO questioning and detention warrants.

In our research into the impact of the new layers of legislation on the media, journalists routinely described it as having a 'chilling effect', causing them and their sources to shut down stories they would otherwise have done.

> J: The big changes? It's the chilling effect, the fear that's inculcated by employees of corporations, employees of private organisations, bureaucrats, public servants, contractors. It's the fear of backlash (from) government… It's an increasing realisation that there will be investigations about leaks. There will be retribution for those things, when you're talking about the bureaucracy and other sort of people in government.

According to Manager of Editorial Policy for the ABC Mark Maley,

> In relation to the Espionage Bill, we are potentially facing criminal charges over researching the story and broadcasting material - visual, electronic material, videos, audio - which was routine in the past. In the past, there has been freedom around those sorts of activities. It has now been criminalised. Although it's yet to happen in relation to either of those bills, the potential clearly exists for a government to criminalise journalism because a media organisation has gone too far or the government is vindictive or excessively authoritarian and secretive. I'm not saying that's the government that we have, I don't think it is. I don't think that's the intention of this government. But, nonetheless, the powers in the Espionage Bill and in the Abhorrent Materials Bill have the potential for journalists to be charged with criminal offences which we would then have to go to court to defend… The movement of everyday journalism into the criminal realm has had a huge impact. It ups the ante enormously.

Maley said the risk of falling foul of the laws and facing criminal prosecution is sufficient to deter journalists from their work:

> Even if you think you've got a good defence, you might have to put somebody through a criminal trial. There have been instances within the last couple of years, where journalists have been the target of criminal investigations and been interviewed by the police. There has been the prospect of serious criminal charges, and it freaks people out. I mean, being interviewed by the Federal Police because you're being investigated for a serious criminal offence which occurred in the normal act of journalism is unsettling to say the least.

At the same time, he said the laws have critically undermined journalists' capacity to fulfil one of their most fundamental ethical responsibilities: protecting their sources.

> [The laws] make stories too risky to do because you're exposing people to criminal sanctions, whether your own journalists or whether your sources. I think you'll find that most experienced investigative journalists now will tell you that they've been contacted by sources in a way which has been insecure with stories and they've gone back to the source and said, 'Forget it, if we run this story on the basis of your information, you will be caught and you will, at the very least, lose your job and find yourself in jail.

1.2. The General Secrecy Offence

The General Secrecy Offence is particularly concerning for its **potential to criminalise journalism**.

The General Secrecy Offence criminalises intentional 'communication' or 'dealing with' information made or obtained by a current or former Commonwealth officer by reason of their position as a Commonwealth officer,[ii] and the person is reckless as to whether:

- the information has a security classification of 'secret' or 'top secret';[iii]
- the communication or dealing damages the security or defence of Australia;[iv]
- the communication or dealing interferes with or prejudices the application of a Commonwealth criminal offence;[v] or
- the communication or dealing harms or prejudices the health or safety of the Australian public.[vi]

The penalty for communicating information is imprisonment for 5 years,[vii] while the penalty for dealing with information is imprisonment for 2 years.[viii]

'Deal' is defined broadly to include: receiving, obtaining, collecting, possessing, recording, copying, communicating or publishing all or part of the information, including the effect or description of the information.[ix] The offence therefore captures a range of conduct which journalists carry out. For example, a journalist who receives a 'secret' classified document from a Commonwealth officer and publishes the document, or an opinion or description of the document's contents, or who describes the contents of the documents to their employer, would be guilty of the General Secrecy Offence. The offence would also capture an administrative staff member who a journalist has asked to make copies of 'secret' documents. 'Deal' also includes dealing with the effect or description of information, meaning that the offence may criminalise a journalist making a note of a conversation with a source who described the effect of a 'secret' document. The General Secrecy Offence has the potential to criminalise **passive receipt** as well as **mere possession** of documents, though the offence requires that a person be reckless as to the security classification of the material.[x]

By broadly criminalising all dealings with a broad set of classified and unclassified government information, the General Secrecy Offence places media organisations and journalists at serious risk of prosecution and, moreover, risks law enforcement or intelligence action aimed at the investigation of leaks well-before publication has occurred or is even considered.

The legislation attempts to protect press freedom by providing a defence for persons communicating information in the business of reporting news (**Journalism Defence**).[xi] For that defence to apply, the person must have:

- dealt with the information in their capacity as a 'person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media.'[xii]
- have reasonably believed that engaging in the conduct was in the public interest.

Alternatively, the defence is available to administrative staff members of an entity engaged in the business of reporting news who have acted under the direction of a journalist, editor or lawyer who reasonably believed the conduct was in the public interest.[xiii]

A person will not have reasonably believed that dealing with the information was in the public interest if the conduct was for the purpose of directly or indirectly assisting a foreign intelligence agency or military organisation.[xiv]

The defence recognises the potential impact of the General Secrecy Offence and, we submit, appropriately focuses on the 'business of reporting news' generally rather than attempting to define 'journalist'. However, the framing of this protection as a defence, rather than as an exemption, negatively impacts press freedom by:

- Conveying that the journalist engaged in criminal wrongdoing.
- Placing the onus on the journalist or media organisation to prove that the defence is applicable.
- Compounding the chilling effect on press freedom by threatening journalists with criminal prosecution. This adds stress, time and the financial cost of defending their actions in court, and many journalists and editors are choosing to cancel otherwise legitimate stories rather than risk prosecution.

Recommendation 1: Amend the General Secrecy Offence to protect press freedom

- The General Secrecy Offence should be amended to clearly exclude mere passive receipt from the scope of criminalized conduct.
- The secrecy offence provisions of the *Criminal Code* should be amended to reframe the Journalism Defence as an exemption.

1.3 Espionage and foreign interference

The *Espionage Act* also introduced 27 new espionage offences consisting of 11 underlying offences and 16 aggravated offences with penalties ranging from 15 years to life imprisonment. 'Espionage' essentially concerns dealing with information to be communicated to a foreign principal where that information is security classified or concerns national security. Where the person dealing with information intends to prejudice Australia's national security, or advantage the national security of a foreign country, the penalty is imprisonment for life. If a person is merely reckless, the penalty is 25 years imprisonment. **National security is defined broadly** to include Australia's political, military and economic relations.[xv] This definition widens the scope of the meaning of 'national security information' and 'national security interests' in the espionage offence, to potentially capture a wide range of conduct within the realm of standard journalistic activities. We address the issues arising from legal definitions of national security below in respect of Term of Reference (f).

The foreign interference laws introduced a further suite of offences and a registration scheme for certain activities undertaken on behalf of a foreign principal.

'**Foreign principal**' is a term fundamental to both the espionage and foreign interference schemes. It is defined to include a foreign government principal or political organisation,[xvi] public international organisation, terrorist organisation or entity owned, directed or controlled by any of these foreign principals.[xvii] 'Foreign government principal' includes: foreign governments (including local governments) or their authorities, foreign public enterprises,[xviii] or entities owned, directed or controlled

by a foreign government principal.[xix] A literal reading of the law implies that legitimate foreign news organizations such as the BBC could be classified as foreign principals for the purposes of the Espionage Act. If this were the case, the impact on media freedom would be considerable.

Unlike the secrecy offence there is no journalism defence available under the espionage or foreign interference frameworks. Three defences are available to a charged espionage offence, however these defences fail to address the potential impact of the laws on press freedom.[xx]

Recommendation 2: Provide exemptions from prosecution to protect press freedom

- Exemptions from criminality should apply across Australia's secrecy and disclosure offences, including those relating to: espionage, foreign interference, and Special Intelligence Operations by ASIO.
- Exemptions should apply to persons:
  - Who dealt with the information in their capacity as a 'person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media.'
  - And reasonably believed that engaging in the conduct was in the public interest.
  - When the conduct was not for the purpose of directly or indirectly assisting a foreign intelligence agency or military organisation.
- These exemptions should give clarity to the meaning of 'public interest' by defining that term by reference to a non-exhaustive list of criteria, including the public interest in press freedom and government accountability.
- The public interest test should also clearly ensure that the exemption does not apply in cases where there is a clear and imminent threat to national security.

Recommendation 3: Clarify when a media organisation will qualify as a foreign principal

Clear parameters and a high-threshold should be set down in legislation, defining the circumstances in which a media organisation could be considered a 'foreign principal' for the purposes of the espionage and foreign interference laws.

2. Warrants

The exercise of powers by law enforcement and intelligence agencies is usually premised on the agency's capacity to obtain a warrant. There are a wide range of warrants available under Commonwealth law, including but not limited to:

- Surveillance device warrants;[xxi]
- Search warrants;[xxii]
- Warrants to inspect postal articles;[xxiii]
- Computer access warrants;[xxiv]
- Telecommunications interception warrants;[xxv]
- Stored communications warrants;[xxvi] and
- Arrest warrants.[xxvii]

Generally speaking, warrants are issued in respect of ASIO by the Attorney-General on request of the Director-General of ASIO. Warrants are issued to law enforcement agencies variously under different

provisions by senior officers, eligible judges, Magistrates or other legally qualified issuing authorities. The grounds of issue tend to focus on the necessity of the warrant in furthering an investigation.[xxviii]

Present warrant processes risk press freedom in three respects:

- The public interest – and particularly the public interest in press freedom – is not articulated as a relevant consideration in the warrant issuing process.
- The issuing authority may not be sufficiently independent or qualified to appropriately consider and give weight to the public interest in press freedom when deciding whether to issue the warrant.
- The issuing authority is not assisted by submissions or arguments concerning the public interest in press freedom, seriously hampering the role that this factor can play in the issuing authority's determination.

Moreover, Australia is lagging behind other nations – including our Five Eyes partners – in the protection of press freedom. Not only do we lack an entrenched constitutional protection for press freedom as in the US or a Charter right to free speech that extends to press freedom as in the UK, Canada and New Zealand, but we fail to recognise journalistic materials or source communications as privileged in any way.[xxix] In the warrant context, McNamara and McIntosh observe that "it is immediately clear that UK journalists are better protected than their Australian counterparts".[xxx]

We draw the Committee's attention to Australia's Journalist Information Warrant (**JIW**) scheme and UK contested warrant processes. These warrant schemes are specifically designed to protect press freedom from incursion and should inform the adoption of similar processes across Australian law enforcement and intelligence powers.

2.1. The Journalist Information Warrant Model

The JIW is the only warrant under Australian law designed to balance investigative powers against press freedom. A JIW is required for an agency to gain access to a journalist or their employers' retained metadata for the purpose of identifying a confidential source.[xxxi] Otherwise, retained metadata may be accessed by a wide range of government agencies without a warrant and, therefore, with scant oversight.

The introduction of a JIW was a unique, positive recognition of the threat these laws pose to press freedom and, specifically, source confidentiality.

Some disturbing weaknesses in this warrant process were demonstrated in the recently tabled Report of the Commonwealth Ombudsman which documented widespread misconduct. This included one instance of a police officer accessing a journalist's metadata without a JIW and two further instances of police officers applying for and obtaining a JIW from a person not authorised to provide it.[xxxii] Thus whilst we submit that the JIW process provides a model for a broader Media Warrant scheme, it requires clear improvements.

Agencies may seek a JIW from an 'issuing authority': **a judicial officer**, member of the Administrative Appeals Tribunal or a lawyer of five years' standing who has been consensually appointed to the role by the Attorney-General.[xxxiii] ASIO may apply directly to the Attorney-General for a JIW,[xxxiv] although in some circumstances the Director-General of ASIO may issue a JIW directly.[xxxv]

A JIW is subject to **both purpose and public interest tests** (though where ASIO has applied for a JIW, only the public interest test, not the purpose test, applies).[xxxvi] Applying the purpose test, the issuing authority must only issue a JIW if satisfied that it is reasonably necessary for either: (a) the

enforcement of the criminal law, finding a missing person or enforcing laws that impose financial penalties or protect the public revenue, or (b) the investigation of a serious offence punishable by imprisonment for at least three years.[xxxvii]

The issuing authority in respect of a JIW must also be satisfied that issuing the warrant is in the public interest, specifically that: "**the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source**."[xxxviii] In weighing these competing interests, the issuing authority will have regard to matters such as privacy and whether reasonable attempts have been made to obtain the information otherwise.[xxxix]

The issuing authority in respect of a JIW is assisted by submissions made by the '**Public Interest Advocate.**'[xl] This security-cleared lawyer who has been appointed to the position by the Prime Minister[xli] makes submissions to assist the application of the public interest test. The presence of the Public Interest Advocate reflects the need for a contested warrant process to protect press freedom. In the absence of this Advocate, the issuing authority only receives submissions from the relevant government agency and is unassisted in their consideration of countervailing public interest factors which may be beyond their expertise. However, the position of Public Interest Advocate has attracted criticism for being insufficiently directed towards the protection of press freedom as opposed to other public interests, such as national security. Specifically, the Public Interest Advocate does not stand in the shoes of the journalist or their employer; nor do they represent the interests of media or open justice more broadly; nor does the Advocate liaise with the potential subject of the warrant. Writing in 2017, Sal Humphreys and Melissa de Zwart reported that two former judges had been appointed to the role of Public Interest Advocate, and that these advocates were 'under no obligation to champion the journalist's position and may never take the point of view of the journalist or advocate on their behalf.'[xlii]

2.2. The UK Model

Press freedom enjoys significantly greater protection in the context of warrant proceedings in the UK. Under the *Police and Criminal Evidence Act 1984* (UK) (***PACE***), **a search warrant cannot be issued** for 'excluded material' or 'special procedure material', which includes journalistic material.[xliii] In order to obtain a search warrant with respect to journalistic material that is not held in confidence, police must seek a production order from a judge and notify the person who would be subject to the order, paving the way for a fully contested warrant proceeding before the judge.[xliv] In issuing the warrant, the **judge** will have regard to the standard conditions for issuing the warrant, whether other methods of obtaining the information have been tried, and whether certain public interest criteria are met.[xlv] The judge retains an **overarching discretion** whether to issue the warrant, which case analysis by McNamara and McIntosh revealed to be an important inclusion.[xlvi] **Production orders may not be sought** in respect of journalistic material held in confidence.[xlvii] Regular search warrants may be sought in respect of journalistic material that is not held in confidence only where a production order has not been complied with or where there is good reason to think it would not be effective.[xlviii]

Even in terrorism investigations a similar process applies. However, the scheme under the *Terrorism Act 2000* (UK) applies to all journalistic material whether or not it is held in confidence, and police are not required to notify the person that they are seeking an order against them.[xlix] The issuing of an access order under the *Terrorism Act* also includes a public interest threshold: there must be reasonable grounds for believing the procurement of the material is in the public interest, having regard to the likely benefit to the investigation and the circumstances under which the person concerned possesses the material.[l] Again, these orders are issued by a judge who maintains an important overarching discretion.

The more recent *Investigatory Powers Act 2016* (UK) provides for a wide suite of investigatory powers including the interception of communications. Even within that framework there are substantive and procedural protections where journalistic materials are concerned. These kinds of protections have heightened importance in Australia where, unlike the UK, intercepted communications may be adduced as evidence in a criminal prosecution.[li]

As McNamara and McIntosh argued, "Remarkably, there are arguably greater media protections in UK terrorism investigations than there are in investigations into ordinary offences in Australia".[lii] Aspects of the UK system remain controversial. For example, during the passage of the Investigatory Powers Bill there was (and remains) considerable debate in the UK about the adequacy of these protections. However, the three schemes outlined above provide an important point of reference against which the Australian Parliament might consider the laws in this country.

We are not aware of any evidence to suggest that the protections for press freedom enshrined in the above UK laws have in any way compromised national security, or the ability of the security services to perform their duties.

2.3. An Enhanced Media Warrant Process

In recognition of the threat that police and intelligence powers pose to the preservation of source confidentiality and press freedom more broadly – both in their direct operation and by facilitating a broader chilling effect on journalists and sources – we recommend that an enhanced, contested issuing process applies to all law enforcement and intelligence warrants that:

- Aim to identify a journalist's confidential source, or
- Relate to the investigation of conduct undertaken in the course of the practice of journalism, or
- Pertain to journalistic material.

The introduction of Media Warrants may also be appropriate in some contexts in which law enforcement and intelligence agencies exercise powers in the absence of a warrant. For instance, the JIW serves an important role within the context of a broader scheme that provides for warrantless access to retained metadata.[liii] We submit that an added layer of protection should also exist to preserve press freedom and source confidentiality in respect of, at least: optical surveillance and the use of tracking devices by ASIO[liv] and warrantless powers to obtain documents related to serious offences and serious terrorism offences by the AFP.[lv] This does not preclude legislative allowance for emergency situations, as is common across warrant procedures.

In the Media Warrant context, **'source', 'journalism' and 'journalist' should be broadly defined**. As the United Nations Human Rights Committee has recognised: "Journalism is a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self- publication in print, on the internet or elsewhere".[lvi] The narrow application of Media Warrant processes to 'professional' journalists and their sources would fail to reflect the reality of contemporary journalism and undercut the process's potential to adequately protect press freedom in modern Australia.[lvii] The nature and form of the journalism undertaken by the potential subject of a Media Warrant could be taken into account by the issuing authority.

The independence and integrity of the warrant process and, it follows, of the agency seeking the warrant, is dependent on the independence and integrity of the issuing authority. A warrant with respect to journalists, their sources, or journalistic material should be subject to robust independent oversight and in-built safeguards at the issuing stage and subsequently. All such warrants should be issued by a **serving superior court judge** when sought by a law enforcement agency. It would be

consistent with existing warrant procedures if Media Warrants with respect to ASIO were issued by the Attorney-General on the request of the Director-General of ASIO, though we acknowledge that issuing by a sitting or retired superior court judge would maintain a higher and more desirable level of independence and integrity. Annual Reports of the relevant agencies should detail the numbers of Media Warrants sought and obtained to enable ongoing public oversight, including by Parliament.

In addition to existing legislative considerations and thresholds, a Media Warrant should be issued on the basis of a **public interest test**. Specifically, the issuing authority must consider the impact of the Media Warrant on press freedom and source confidentiality, and should only issue the Warrant if its investigative value substantially outweighs those impacts. In this context the issuing authority may also have regard to other matters, including the impact of the warrant on privacy and the availability of less intrusive alternative methods of investigation, and must retain an overarching discretion whether or not to issue the warrant. We note that the express consideration of press freedom and the examination of the necessity and proportionality of the measure would bring Australia more closely into line with nations (such as the UK, Canada and New Zealand) operating under a Charter of Rights framework.

Media Warrant proceedings should be **contested**. Wherever possible and appropriate (including in the context of search warrants as in the UK) the person or organisation against whom the warrant is sought should be notified and given an opportunity to contest the application before a judge. Where this is not appropriate, as is usually the case for intelligence agencies, the issuing authority should be assisted by a **Media Freedom Advocate** whose role is to represent the interests of the media and press freedom. The independence of the Media Freedom Advocate is of fundamental importance, as is their suitability and qualification for the position. Media Freedom Advocates should be appointed in consultation not only with peak legal bodies but also with key representatives from the media industry.

Finally, consideration should be given to adopting the position reflected under *PACE* (UK), whereby journalistic materials held in confidence may not be subject to certain warrants, including search warrants and data access powers. We support a broad recognition of **journalistic materials as attracting a form of privilege**.

Recommendation 4: Require that media warrants be issued by a judge in contested proceedings

All warrants that:

- Aim to identify a journalist's confidential source, or
- Relate to the investigation of conduct undertaken in the course of the practice of journalism, or
- Pertain to journalistic material.

Should:

- Be issued by a superior court judge.
- Be subject to a public interest test that includes express consideration of the public interest in press freedom.
- Be contested. Where it is clearly inappropriate to inform the potential subject of the warrant of the application, they may be contested by an independent Media Freedom Advocate.
- Define 'source', 'journalism' and 'journalist' broadly.

Recommendation 5: Consider extending a form of privilege to journalistic materials

Consideration should to be given to adopting the position reflected under *PACE* (UK), whereby journalistic materials held in confidence may not be subject to certain warrants, including search warrants and data access powers and, particularly, to adopting the approach of a number of comparable jurisdictions whereby journalistic materials attract a form of privilege.

b. The whistleblower protection regime and protections for public sector employees

1. The public-sector whistleblower protection regime

Public-sector whistleblowing is governed by the *Public Interest Disclosure Act 2013* (Cth) (***PIDA***). Disclosures by public officials may be made internally, externally, in an emergency, or to a legal practitioner.[lviii] 'Disclosable conduct' includes conduct engaged in by an agency, public official, or contracted services provider for a Commonwealth contract,[lix] that either:

- Contravenes Australian or applicable foreign law;
- Perverts or attempts to pervert the course of justice;
- Is engaged in for corrupt purposes;
- Constitutes maladministration or an abuse of public trust;
- Involves falsification, deception, plagiarism or misconduct in relation to scientific research, analysis, evaluation or advice;
- Results in the wastage of public money or property;
- Unreasonably results in or increases a risk of danger to the health and safety of persons; or
- Results in or increases danger to the environment.[lx]

2. Intelligence agencies and whistleblower protections

The principles of accountability which inform the *PIDA* whistleblower protection regime are equally relevant to intelligence organisations. However, information that relates to an intelligence agency, or the conduct of an intelligence agency officer, is excluded from disclosable conduct under *PIDA*.[lxi] We acknowledge that particular difficulties may arise in connection with sensitive information relevant to, or originating from, intelligence officers and operations. However, a blanket ban on whistleblower protections in this arena is inappropriate. In determining whether a disclosure is contrary to the public interest, any potential damage to Commonwealth security, defence, international relations or relations with a State or Territory are relevant considerations.[lxii] These considerations should provide a starting point for the development of an intelligence organisation whistleblowing regime that allows for the disclosure of information, showing misconduct or illegal activity, that does not pose any immediate risk to national security.

Recommendation 6: Extend whistleblower protection to intelligence officers and operations

Consider extending whistleblower protection to public sector intelligence agency whistleblowers and whistleblowers who disclosure intelligence agency related misconduct and illegal activity.

d. Appropriate culture, practice and leadership for Government and senior public employees

Our research shows the relationship between journalists and government has deteriorated in recent years. The trust that underpinned the relationship has been replaced by a culture of secrecy. This has made it difficult for journalists to access sources at all levels of the government and the bureaucracy, making reporting in the public interest increasingly challenging.

> L: The fact that now you can never, ever speak to a media officer at a department or get an answer verbally, everything has to be in writing, so you have to put questions in writing, and then they answer whatever they want in writing that doesn't actually answer the questions and you're not having a conversation so you can't pull them up on it. The fact that it's very hard to get background briefings, so if you want to understand the policy or you want to understand something, they don't do that anymore.
>
> C: It just feeds into this overarching narrative around government secrecy. Everywhere you look in terms of transparency and government, things are either not improving, or getting worse. In terms of whistleblowers, they are clearly getting worse, because of all the national security legislation, because of the raids, the AFP raids, because of the government's punitive approach to whistleblowers, things are getting worse. In terms of FOI, things are getting worse because FOI teams are being under-resourced, there's been some incredibly dodgy decisions, the information regulator is being under-resourced. In terms of other areas of transparency in government around lobbying, around donations, things have just stayed the same for 10-15 years with no inclination to make it more transparent at all.

At the same time, Freedom of Information (**FOI**) – a formal mechanism intended to maintain openness and transparency – appears to be dysfunctional. Journalists described over-worked staff, and increasingly narrow interpretations of what can be released, at odds with the underlying principles of FOI. For news media, where timeliness is crucial, the months it now regularly takes to process even routine requests under FOI and Right to Information (**RTI**) legislation can have the same effect as denying the information in the first place.

> S: [FOI has] a real, direct effect on what gets into the public domain, and for anybody doing any kind of investigative work, it's bread and butter… What I've found is that government agencies have become increasingly adept at finding ways to avoid giving up information through FOI and RTI. I've seen this at a federal level, I've seen it at local government level dealing with councils, I've seen it less so at state level. But, at the federal level, I've been given the most incredible run-around by Treasury for example. I was once asked to participate in a 7-way teleconference with Treasury bureaucrats to discuss an FOI application that I had put in and I had absolutely no idea who I was talking to, it was like something out of Kafka. At the other end of the scale, the local council I am currently dealing with are clearly expecting me to send everything that they provide me with to the Information Commissioner for an external review because they have redacted pretty much 90% of what they have provided me with.
>
> S: Even a good [application], even an efficient one, takes months. I've had them drag out for well over 12 months, by which time the news value is severely diminished, if it's there at all… it's a mechanism that is supposed to increase governance and transparency, but government agencies have become increasingly adept at gaming the system.
>
> C: I think rejection rates last year, of the last financial year, were at record highs, the delays in 2016-2017 were way, way above any other year in the past, and on a practical level, trying to get a record that you know exists, the department knows exists, should be accessible under FOI, it's just impossible. It's so difficult. If they don't want it released, it will be delayed and delayed and delayed. It will be heavily redacted and then you have to go through the process of appealing that decision or having a review of that decision, and then taking it to the Information Commissioner, who itself is extremely under-resourced.

While there is an understandable scepticism from law enforcement and security agencies about the motives of journalists, particularly with regard to handling classified documents, news organisations pointed out that in the past the relationship has been far more co-operative. Journalists may be inclined to publish, but few if any wish to reveal information that is genuinely damaging to national security or likely to put lives at risk. Journalists also recognise that their capacity to work with whistleblowers and receive sensitive information depends on their reputations as responsible custodians of that information.

One senior journalist spoke of an incident in which they received a classified PowerPoint presentation that revealed Australian agents had been spying on the Indonesian president and his wife.

> L: I didn't understand half of the slides, I didn't know what they were talking about. And so, it was kind of a risk that we might be inadvertently revealing something that really was against the national interest, so we went to the security agencies and said, 'This is what we've got, we intend to publish, but if there is something that we might not understand about this document, please tell us now, we don't want to publish something irresponsibly', and their initial response was, you know, 'Don't publish this', 'Why?', 'Because it's embarrassing', 'Sorry, that's not a good enough reason.' That has always been normal practice to have that sort of backroom conversation, and it's not collusion, it's doing the right thing, you know, so you're not inadvertently putting something you don't know.
>
> L: "I guess there was always an element of risk… we could have been prosecuted under the old Crimes Act… but governments traditionally accepted that the media had a right to publish stories and that it was in everybody's interests for them to recognise that and for there to be a trusted negotiation over the bits that might really put someone in danger or might really endanger the national interest. I think that trust relationship, because of all the new legislation, the new penalties, and because of the attitude, that's in question, and I think that actually is potentially detrimental both ways."

Journalists acknowledged that the long-standing *Crimes Act* also technically criminalised much of their previous dealings with government sources, but they argued that the more recent tranches of national security legislation have contributed to an overall atmosphere of hostility and distrust which undermines the ability of both the media and government to function effectively.

> J: I think it's much broader than national security legislation itself. One of the things, going back to the AFP stuff, if you look at the underlying charges against both (ABC Journalists) Dan and McBride, they're not national security. They're not new laws. They're actually old laws: an old defence act, receipt of stolen goods. There was at one point an old Crimes Act charge that they decided to do away with because it would never stick. I don't even know whether these would ever stick. What's interesting is, new legislation is troubling and the metadata stuff is troubling, but if there is a will to pursue something like this, they seem to find a way.

By definition, the relationship between media and government is often likely to be fraught, particularly when the media is reporting on things the government would rather not be aired in public. However, it is important for the government to recognise that when the media's watchdog role is unnecessarily limited, its own functioning becomes less robust and efficient.

Recommendation 7: Review public sector culture and practices with respect to media inquiries

The government introduce a review of public service and departmental culture, with a view to restoring principles of openness and accessibility, particularly in relation to media inquiries.

e. Mechanisms to ensure that the Australian Federal Police have sufficient independence to effectively and impartially carry out their investigatory and law enforcement responsibilities in relation to politically sensitive matters

The clearest way to ensure the actual and perceived independence of the AFP is to rest the exercise of its powers (particularly intrusive powers) on the existence of a valid warrant issued by an independent, impartial and appropriately qualified decision-maker, preferably in contested proceedings. See our submission to Term of Reference (a) above, specifically part 2 in respect of media warrants.

f. Related Matters

1. The definition of national security

The scope of Australia's national security laws rests upon the legal definition of 'national security'. At its core, national security involves the protection of the state and its people, at least from foreign forces.[lxiii] Today, however, this term is subject to various legal definitions, leading to **confusion**, **complexity** and in many instances **overbreadth**.[lxiv] A complex definition of national security has the potential to create uncertainty as to the scope and potential impact of national security laws, facilitating a chilling effect on public interest journalism. An overly broad definition has a far-reaching impact on the scope of offences and, relevantly, the potential criminalisation of legitimate journalism.

We recommend that the definition of 'national security' across Commonwealth legislation be clarified and narrowed. It is possible to gain some guidance from international developments in this respect.

1.1. *Australian law*

Several statutes – including the *Intelligence Services Act 2001* (Cth)[lxv] – refer to 'Australia's national security' but stop short of providing any definition. In other statutes a host of definitions must be read in conjunction in order ascertain the scope of the provisions.

For example, the definition of 'activities prejudicial to security' is central to the grounds of issue for a number of interception warrants, including surveillance device warrants issued under the *Australian Security Intelligence Organisation Act 1979* (Cth) (***ASIO Act***) and warrants allowing the interception of telecommunications, and access to stored telecommunications, under the *Telecommunications (Interception and Access) Act 1979* (Cth) (***TIA Act***).[lxvi] 'Activities prejudicial to security' is defined in the *ASIO Act* to include any activities concerning which Australia has responsibilities to a foreign country, as referred to in the definition of 'security'.[lxvii] 'Security' is defined as:

- The protection of, and of the people of, the Commonwealth and the several States and Territories from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference – whether directed from, or committed within, Australia or not;
- The protection of Australia's territorial and border integrity from serious threats; and
- The carrying out of Australia's responsibilities to any foreign country in relation to the above matters.[lxviii]

The references to certain acts, including 'sabotage' and 'espionage', widen the scope of this definition. For example, the offence of espionage can be found in Part 5.2 of the *Criminal Code*. It entails a person dealing with information, subject to security classification or concerning Australia's national security, intending to or recklessly prejudicing Australia's national security, or advantaging the national security of a foreign country, with the result that the information or article being is communicated or made available to a foreign principal.[lxix] 'National security', in Part 5.2 of the *Criminal Code,* is defined to include:

- The defence of the country;
- The protection of the country or any part of it, or the people of the country or any part of it, from:
    - Espionage, sabotage, terrorism, political violence and foreign interference; and

  - Activities intended and likely to obstruct, hinder or interfere with the performance by the country's defence force of its functions or with the carrying out of other activities by or for the country for the purposes of its defence or safety.
- The protection of the integrity of the country's territory and borders from serious threats.
- The carrying out of the country's responsibilities to any other country in relation to:
  - Espionage, sabotage, terrorism, political violence and foreign interference;
  - Activities intended and likely to obstruct, hinder or interfere with the performance by the country's defence force of its functions or with the carrying out of other activities by or for the country for the purposes of its defence or safety; and
  - The protection of the integrity of the country's territory and borders from serious threats.
- The country's **political**, **military** or **economic relations** with another country or other countries.[lxx]

To summarise this example: in order to understand the basis for issuing an interception warrant one must look to the warrant grounds in the *TIA Act*, then to the definition of 'activities prejudicial to security' in the *ASIO Act*, which refers to the definition of 'security' in the *ASIO Act*, which in turn refers to espionage which is defined (at length) in the *Criminal Code*. The meaning of espionage hinges on the term 'national security' which is defined in the *Criminal Code*. That definition includes complex and further-defined phrases such as espionage, terrorism and foreign interference, as well as broad notions such as politically motivated violence and all political, military and economic relations between countries.

A further example of overlapping definitions can be found in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ('*NSI Act')*, designed to prevent the disclosure of information likely to prejudice national security in federal criminal and civil proceedings.[lxxi] 'National security' is defined broadly in the *NSI Act* to include Australia's defence, security, international relations or law enforcement interests.[lxxii] In *Thomas v Mowbray* – a case concerning the constitutional validity of anti-terrorism control order legislation – the High Court queried whether in this provision 'the Parliament has sought to over-reach the bounds of the understanding of "national security"'.[lxxiii] 'International relations', referred to in the *NSI Act* definition of 'national security', is said to include political, military and economic relations with foreign governments and international organisations.[lxxiv] 'Security' is defined by reference to the *ASIO Act* definition, as outlined above.[lxxv]

1.2. *International law*

The international community has sought to give meaning to national security in the context of setting boundaries on the extent to which nation-states may have recourse to national security as a ground for derogating from fundamental human rights.[lxxvi]

Both the *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*[lxxvii] and the *Johannesberg Principles on National Security, Freedom of Expression and Access to Information*[lxxviii] focus their definitions of national security on the core aim of protecting the existence of the state. The former, for example, provides that

> National security may be invoked to justify measures limiting certain rights only when they are taken to **protect the existence of the nation or its territorial integrity or political independence against force or threat of force**.[lxxix]

This is **contrasted with 'merely local or relatively isolated threats to law and order'**.[lxxx] The *Johannesberg Principles* define national security as:

> to protect a **country's existence or its territorial integrity** against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an international source, such as incitement to violent overthrow of the government.[lxxxi]

Recommendation 8: Amend and clarify legal definitions of national security

- A single definition of 'national security', 'security' and 'national interests' apply across Commonwealth legislation.
- Consideration be given to simplifying these definitions and removing circularity.
- Consideration should be given to ensuring that the legal definition of national security is not so broad as to encompass 'isolated or merely local threats to law and order'.
- The definition of 'national security' be amended to remove broad references to Australia's political or economic relations.
- Further and alternatively, the definition be constrained to focus on the prevention of harm or prejudice to Australia's national security.

2. Data surveillance and source confidentiality

Source confidentiality is one of journalists' most central ethical considerations and is essential to a functioning democracy and a free and independent media. The fundamental importance of journalistic confidentiality was recognised by the United Nations Human Rights Committee in 2011 when it said that nations 'should recognise and respect that element of the right to freedom of expression that embraces the limited journalistic privilege not to disclose information sources.'[lxxxii]

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)* and *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (***TOLAA***) create and facilitate frameworks of covert surveillance which make it extremely difficult for journalists to fulfill their ethical obligation to ensure source confidentiality. Warrantless access to metadata means that journalists should assume that a wide range of state and federal government agencies have access to their metadata. Anyone engaged in journalism or public interest writing who is not a 'professional journalist' must be aware that government agencies may access their metadata without a warrant even for the direct purpose of identifying a confidential source. The only obstacle to full metadata access by government is the JIW, discussed above in respect of Term of Reference (a).

The *TOLAA* compounds source vulnerability by presenting a way for government to circumvent encryption and other protection technologies and by extending and easing government surveillance of the content of communications. The *TOLAA* creates a complex framework by which agencies have been given tools to enable them to request and even compel Providers – defined with extravagant breadth – to embed weaknesses and decryption technologies into target devices, among a vast range of other 'acts and things.'

The breadth of powers created under the *TOLAA* is coupled with slim independent oversight or accountability mechanisms. *TOLAA* Requests and Notices are limited to certain law enforcement and national security purposes, so that agencies may only seek (or compel) Provider assistance in furtherance of legitimate agency objectives. Importantly, a traditional warrant or authorisation is required in order to support access to information or documents. Thus, the improvement of warrant

processes (discussed above under Term of Reference (a) part 2) would positively impact the scope of data surveillance powers under the *TOLAA*.

Under present laws there is every chance that journalists investigating national security matters, serious crimes, or who interact with government sources who have access to classified information (and who therefore may be subject to an investigation under federal espionage or foreign interference laws) may be subject to surveillance, and may be targeted under the *TOLAA*. Indeed, journalists engaged in this kind of reporting may be subject to: general metadata access, targeted metadata access to identify their sources under a JIW, orders under the *TOLAA* to cause weaknesses to be built into their attempts to encrypt or protect their data, and warrant-based access to their (now decrypted) communications. All of this could take place without the journalist or their employer ever knowing, or the interests of the journalist or the media industry being represented to decision-makers at any stage. In this context of widespread covert data surveillance, slim protections for journalistic confidentiality, far-reaching government powers and an absence of public information or effective oversight, journalists are not in a position to protect source confidentiality.

One journalist said killing off significant parts of stories out of fear of source identification is now commonplace. Highlighting the particular impact of uncertainty around metadata retention laws.

> C: Metadata laws break up all of the avenues you have to communicate with sources and puts them in jeopardy. Sources don't have a detailed complex knowledge about how metadata laws work and how journalist information warrants might work and some of the protections or lack of protections or whatever. They're not fully across it but they have this general sense that their communications with journalists are subject to warrantless monitoring. It just puts everything into this state of uncertainty and jeopardy in which you have to be so careful around every little communication you have with a source. They know that. It puts them off. As soon as there's some sort of hiccup in terms of your communication going through an unencrypted channel, they freak out, get cold feet, get nervous, and routinely pull out of stories.

Recognising journalists' ethical obligation to protect sources, the same journalist said the onus is on journalists to ensure source confidentiality but that fulfilling this obligation is made more difficult by data-retention laws. This brings a layer of complexity to doing the kinds of journalism that until recently have been considered pedestrian, and calls for a high level of technological competency on the part of both journalists and their sources.

> C: There is definitely a trend that people who come forward seem to be only doing so if they are aware of the ways to safely communicate. The onus is on the journalist to understand their source's level of savviness with encrypted communications. If you don't understand the laws and the tech, you're putting your source in danger because sources often have no understanding of the laws. You need to understand the laws to be able to protect your sources. That is one thing that has happened as a result of all the legislation that's coming through. I have to ask everyone who comes forward, 'Can you download this? Can you download Signal? Can you put everything in an encrypted email? Can you use secure drop to transfer files instead of just sending them to me?' You have to actively go through those procedures.

Telling someone something like that heightens the danger or risk associated with what they are doing, which, of course, you have a duty to tell them as a journalist. It makes it much more real for sources, and it can be very discouraging.

Our research has revealed the extensive use of encryption technologies in protecting sources. It follows that the introduction of the complex industry assistance scheme and decryption laws in 2018 added further layers of uncertainty, complexity and risk to the journalist-source relationship.

> J: Part of our obligation is to educate our sources on how to communicate with us. A lot of people don't understand this stuff. People will say, 'I'll email you a document', and you have to say, 'Don't do that. Stop. What's the document? How many people have this document? Is it just you? Is it five people? Where is it sitting right now? Is it on a computer?', 'Oh, I can print it off and send it to you', 'You know that will be recorded. Let's talk about another way of doing that. Why don't you turn off your cloud service on your phone and take pictures of it, and then let's think about how you then get it to us'. And, so, that's part of the training as well because it's our responsibility to protect them. Our responsibility is also to educate them.

By undermining journalists' capacity to ensure source confidentiality the current security landscape is recalibrating and hampering interactions between journalists and their sources. In particular, the vast, complex, covert and intimidating data access and surveillance powers available to law enforcement and intelligence agencies deter sources from coming forward and place considerable pressure on journalists attempting to protect their sources. For those sources who do approach a journalist, their communications are fraught with risk to the point that the journalist may be the one to kill the story or refuse a source whose identity may be discoverable through, for example, metadata access.

It is worth noting that this is true even of stories that might not directly relate to security issues. The confusion over what can and can't be legally investigated makes all such journalism vulnerable.

3. Protecting press freedom

Australia's national security laws are uniquely broad and complex. The imperative to protect press freedom is, however, fundamental and deserving of general recognition and protection. In light of these concerns, our international obligations,[lxxxiii] and the interests of legal clarity, consistency and proportionality, we support calls for a Media Freedom Act. This Act is not a panacea; it would not avoid the need for detailed review of Australia's legal frameworks for their impact on press freedom. However, a Media Freedom Act would serve three important purposes.

First, it would **recognise and affirm** the importance of press freedom in Australia. This recognition would support the fourth estate role of Australian media and evidence Australia's commitment to the rule of law. The Act would also recognise that press freedom is not an absolute principle but may be subject necessary and proportionate limitations.

Second, it would support the development of an appropriate **culture of disclosure** and open government within the public sector. This role would be served by requiring the public sector (including law enforcement and intelligence officers) to consider the impact of their decisions on press freedom and government accountability, and to adopt the least intrusive option that is reasonably available in the circumstances.

Third, it would **protect** press freedom by ensuring that legitimate public interest journalism was excluded from the scope of criminal offences. This form of protection would ensure legal consistency and clarity, and avoid the need for technical amendments across countless statutory schemes.

Recommendation 9: Introduce a Media Freedom Act

Enact a Media Freedom Act, recognising the importance of press freedom to Australian democracy, giving press freedom a clear place in public decision-making and excluding legitimate public interest journalism from the scope of criminal offences.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Contributing authors

This submission has been written by the following authors.

Dr Rebecca Ananian-Welsh
Senior Lecturer
TC Beirne School of Law

Rose Cronin
Research Assistant
TC Beirne School of Law

Professor Kath Gelber
Head of School
School of Political Science and International Studies

Professor Peter Greste
UNESCO Chair in Journalism and Communications
School of Communication and Arts

Richard Murray
Research Fellow
School of Communication and Arts

Zoe Winder
Research Assistant
School of Communication and Arts

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Endnotes

[i] Human R ghts Comm ttee, *General Comment No 34: Article 19 Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [13].
[ii] *Criminal Code Act 1995* (Cth) ss 122.4A(1)(c), (2)(c).
[iii] Ib d s 122.4A(1)(d)( ), (2)(d)( ).
[iv] Ib d s 122.4A(1)(d)( ), (2)(d)( ).
[v] Ib d s 122.4A(1)(d)( ), (2)(d)( ).
[vi] Ib d s 122.4A(1)(d)(v), (2)(d)(v).
[vii] Ib d s 122.4A(1).
[viii] Ib d s 122.4A(2).
[ix] Ib d s 90.1(1)–(2).
[x] Ib d s 122.4A(1)–(2).
[xi] Ib d s 122.5(6)–(7).
[xii] Ib d s 122.5(6).
[xiii] Ib d s 122.5(6).
[xiv] Ib d s 122.5(7).
[xv] Ib d (Cth) s 90.4.
[xvi] Ib d (Cth) s 90.1(1) (def n t on of fore gn po t ca organ sat on).
[xvii] Ib d s 90.2.
[xviii] Ib d s 70.1 (def n t on of fore gn pub c enterpr se).
[xix] Ib d s 90.3.
[xx] See Austra an Lawyers for Human R ghts, Subm ss on No 7 to PJCIS, Par ament of Austra a, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*, 22 January 2018, 6; Wh st eb owers Austra a, Subm ss on No 51 to PJCIS, Par ament of Austra a, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*, 26 March 2018, 3-4, 7; Human R ghts Watch, Subm ss on No 10 to PJCIS, Par ament of Austra a, *Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*, 22 January 2018; Par amentary Jo nt Comm ttee on Human R ghts, Par ament of Austra a, *Human Rights Scrutiny Report* (2018) 246-254.
[xxi] *Australian Security Intelligence Organisation Act 1979* (Cth) s 26; *Surveillance Devices Act 2004* (Cth) s 14.
[xxii] *Australian Security Intelligence Organisation Act 1979* (Cth) s 25; *Crimes Act 1914* (Cth) s 3E.
[xxiii] *Australian Security Intelligence Organisation Act 1979* (Cth) s 27.
[xxiv] *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A; *Surveillance Devices Act 2004* (Cth) s 27A.
[xxv] *Telecommunications (Interception and Access) Act 1979* (Cth) s 9 (te ecommun cat ons serv ce warrant – ASIO), s 9A (named person warrant – ASIO), s 46 (te ecommun cat ons serv ce warrant – agenc es), s 46A (named person warrant – agenc es).
[xxvi] Ib d s 109 (stored commun cat ons warrant – ASIO), s 110 (stored commun cat ons warrant – cr m na aw-enforcement agenc es).
[xxvii] *Crimes Act 1914* (Cth) s 3ZA.
[xxviii] See eg: *Australian Security Intelligence Organisation Act 1979* (Cth) s 25(1) (search warrant), s 25A(1) (computer access warrant), s 26(3)(a)( ) and (b)( ) (surve ance dev ce warrant); *Surveillance Devices Act 2004* (Cth) s14(1) (surve ance dev ce warrant), s 27A(1)(c) (computer access warrant); *Crimes Act 1914* (Cth) s 3E (search warrants), ss 3F-3K; *Telecommunications (Interception and Access) Act 1979* (Cth) s 110 (stored commun cat ons warrant), s 116.
[xxix] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 180J, 180Q.
[xxx] Lawrence McNamara and Sam McIntosh, Conf dent a Sources and the Lega R ghts of Journa sts: Re-th nk ng Austra an Approaches to Law Reform (2010) 32(1) *Australian Journalism Review* 81 89.
[xxxi] Bendetta Brev n Metadata Laws, Journa sm and Res stance n Austra a (2017) 5(1) *Media and Communication* 76, 78.
[xxxii] Commonwea th Ombudsman, Par ament of Austra a, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979 for the period 1 July 2016 to 30 June 2017* (2018); Pau Karp and Josh Tay or, Po ce made ega metadata searches and obta ned nva d warrants target ng journa sts , *The Guardian* (on ne at 23 Ju y 2019) <https://www.theguard an.com/austra a-news/2019/ju /23/po ce-made- ega -metadata-searches-and-obta ned- nva d-warrants-target ng-journa sts?CMP=Share_ OSApp_Other>.
[xxxiii] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5(1) (def n t on of ssu ng author ty), 6DB-6DC.
[xxxiv] Ib d ss 180J-180L.
[xxxv] Ib d s 180M.
[xxxvi] Ib d s 180L(2)(b).
[xxxvii] Ib d s 180T(2)(a), referr ng to ss 178-180(4).

[xxxviii] Ib d s 180T(2)(b).
[xxxix] Ib d s 180T(2)(b).
[xl] Ib d s 180T(2)(b)(v).
[xli] Ib d s 180X(1).
[xlii] Sa Humphreys and Me ssa de Zwart, Data Retent on, Journa st Freedoms and Wh st eb owers (2017) 165 *Media International Australia* 103, 106.
[xliii] *Police and Criminal Evidence Act 1984* (UK) ss 8(1)(d), 11 (mean ng of exc uded mater a), 13 (mean ng of journa st c mater a), 14 (mean ng of spec a procedure mater a s).
[xliv] Ib d s 9, Sch 1 [8].
[xlv] Ib d Sch 1 [2](b).
[xlvi] McNamara and McIntosh (n xxx).
[xlvii] *Police and Criminal Evidence Act 1984* (UK) s 11(2)-(3) (mean ng of exc uded mater a).
[xlviii] Ib d Sch 1 [12]-[14].
[xlix] McNamara and McIntosh (n xxx) 89.
[l] *Terrorism Act 2000* (UK) Sch 5 [6](3).
[li] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 74; 75A.
[lii] McNamara and McIntosh (n xxx) 90.
[liii] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 175 (ASIO te ecommun cat ons data access), 178 (Enforcement agency access to te ecommun cat ons data).
[liv] *Australian Security Intelligence Organisation Act 1979* (Cth) ss 26D, 26E.
[lv] *Crimes Act 1914* (Cth) ss 3ZQN, 3ZQO.
[lvi] Human R ghts Comm ttee (n 1) [44].
[lvii] Edward L. Carter, Not to D sc ose Informat on Sources : Journa st c Pr v ege Under Art c e 19 of ICCPR (2017) 22(4) *Communication Law and Policy* 399, 423; Jan Oster, Theory and doctr ne of med a freedom as ega concept (2013) 5(1) *Journal of Media Law* 57, 58.
[lviii] *Public Interest Disclosure Act 2013* (Cth) ss 25; 26(1).
[lix] Ib d s 29(1)(a)-(c).
[lx] Ib d s 29(1).
[lxi] Ib d ss 29(1) [Tab e Item 2]; 33, 41.
[lxii] Ib d s 26(3).
[lxiii] Rebecca Anan an-We sh and N co a McGarr ty-Wh te, Nat ona Secur ty: A Hegemon c Const tut ona Va ue n Rosa nd D xon (ed), *Australian Constitutional Values* (Hart-B oomsbury, 2018), 267-271.
[lxiv] For academ c attent on and cr t que, see eg: Ke ran Hardy and George W ams, Terror st, tra tor, or wh st eb ower? Offences and protect ons n Austra a for d sc os ng nat ona secur ty nformat on (2014) 37(2) *University of New South Wales Law Journal* 784, 787-788; Dav d Brooks, Jeffery Cork , and M chae Coo e, The Austra an Secur ty Cont nuum: Nat ona and Corporate Secur ty Gaps from a Surve ance Language Perspect ve n Randy K. L ppert, Kev n Wa by, Ian Warren and Darren Pa mer (eds), *National Security Surveillance and Terror: Canada and Australia in Comparative Perspective* (Spr nger Internat ona Pub sh ng, 2016), 133-134; Kev n Wa by, Randy K. L ppert, Ian Warren and Darren Pa mer, Interrogat ng Nat ona Secur ty, Surve ance, and Terror n Canada and Austra a n Randy K. L ppert, Kev n Wa by, Ian Warren and Darren Pa mer (eds), *National Security Surveillance and Terror: Canada and Australia in Comparative Perspective* (Spr nger Internat ona Pub sh ng, 2016), 7; Rebecca Anan an-We sh and N co a McGarr ty-Wh te, Nat ona Secur ty: A Hegemon c Const tut ona Va ue n Rosa nd D xon (ed), *Australian Constitutional Values* (Hart-B oomsbury, 2018), 267-271.
[lxv] *Intelligence Services Act 2001* (Cth) s 11.
[lxvi] *Australian Security Intelligence Organisation Act 1979* (Cth) s 26(3)(a)( ); *Telecommunications (Interception and Access) Act 1979* (Cth) ss 9(1)(a)( ), 9A(1).
[lxvii] *Australian Security Intelligence Organisation Act 1979* s 4 (def n t on of act v t es prejud c a to secur ty).
[lxviii] Ib d s 4 (def n t on of secur ty).
[lxix] *Criminal Code Act 1995* (Cth) s 91.1.
[lxx] Ib d s 90.4.
[lxxi] *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) s 3.
[lxxii] Ib d s 8.
[lxxiii] (2007) 233 CLR 307, 358 [124] (Gummow and Crennan JJ).
[lxxiv] *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) s 10.
[lxxv] Ib d s 9.
[lxxvi] *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1984/4 (28 September 1984); *Johannesburg Principles on National Security Freedom of Expression and Access to Information Freedom of Expression and Access to Information*, UN Doc E/CN.4/1996/39 (1 October 1995).
[lxxvii] *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Doc E/CN.4/1984/4 (28 September 1984) annex [29]–[30].
[lxxviii] *Johannesburg Principles on National Security Freedom of Expression and Access to Information Freedom of Expression and Access to Information*, UN Doc E/CN.4/1996/39 (1 October 1995), pr nc p e 2.
[lxxix] *Siracusa Principles*, UN Doc E/CN.4/1984/4, [30].
[lxxx] Ib d.

[lxxxi] *Johannesburg Principles on National Security Freedom of Expression and Access to Information Freedom of Expression and Access to Information*, UN Doc E/CN.4/1996/39 (1 October 1995), pr nc p e 2.
[lxxxii] Human R ghts Comm ttee (n 1) [45]. D scussed n Edward Carter, "Not to D sc ose Informat on Sources": Journa st c Pr v ege Under Art c e 19 of the ICCPR (2017) 17 *Communication Law and Policy* 399.
[lxxxiii] See eg: Art c e 19 of the *International Covenant on Civil and Political Rights*, opened for s gnature 16 December 1966, 999 UNTS 171 (entered nto force 23 March 1976); Human R ghts Comm ttee (n 1).