



**Australian Government**

**Department of Home Affairs | Attorney-General's Department**

---

# **Submission to the inquiry into press freedom**

Senate Standing Environment and Communications  
References Committee

# Table of Contents

<b>Inquiry into press freedom</b>	<b>3</b>
Introduction	3
Importance of press freedom	3
Historical perspective	4
Legislative frameworks relating to lawful disclosure of sensitive information	5
Public Interest Disclosure Act 2013	5
Freedom of Information Act 1982	7
Criminal law and law enforcement powers	7
General secrecy offences	7
Journalist information warrants	9
Issue of warrants	11
Operational independence of the Australian Federal Police	12
Related matters	13
Amendments to secrecy offences	13
Classification of documents as secret	14
Defamation	14
Media Freedom Act	15
Contested warrants	15
Reporting requirements relating to Public Interest Advocates	17
Broader application of the public interest test for other types of Telecommunications (Interception and Access) warrants	17
Public reporting requirements for the Australian Security Intelligence Organisation	17
Attachment A: Five Eyes' search warrant schemes and protections for journalists	19
Canada	19
New Zealand	19
United Kingdom	20
United States	21

# Inquiry into press freedom

## Introduction

The Department of Home Affairs and the Attorney-General's Department thank the Senate Standing Environment and Communications References Committee for the opportunity to make a joint submission to the inquiry into press freedom.

This submission provides detail on:

- the importance of press freedom, including historical approaches to engagement between government and the media on press freedom in the context of the appropriate balance between reporting on matters of public interest and protecting Australia's national security
- legislative frameworks relating to lawful disclosure of sensitive information
- criminal law and law enforcement powers
- the operational independence of the Australian Federal Police, and
- related matters raised in the context of public discussion of press freedom, including in relation to the inquiry of the Parliamentary Joint Committee on Intelligence and Security into the impact of the exercise of law enforcement and intelligence powers on freedom of the press (the Parliamentary Joint Committee inquiry).

This submission is intended to complement the submission provided to the inquiry by the Australian Federal Police, which addresses a number of matters in further detail. Further, a number of related matters are dealt with through the submissions and evidence provided by the departments to the Parliamentary Joint Committee inquiry into the impact of law enforcement and intelligence powers on the freedom of the press. This submission draws on the submissions and information previously provided by the departments.

## Importance of press freedom

Australia is founded on the rule of law and has a strong tradition of respect for the rights and freedoms of every individual. The Australian Government is committed to protecting and promoting traditional rights and freedoms, including freedom of speech and opinion. These rights and freedoms are protected by the common law principle that legislation should not infringe fundamental rights and freedoms unless the legislation expresses a clear intention to do so and the infringement is reasonable.

The Australian common law provides particularly strong protections for freedom of speech related to public affairs and political matters. The courts have also recognised an implied constitutional freedom of political communication. Laws which restrict communication about government or politics are invalid if they impermissibly infringe the implied freedom. The Government believes these rights and freedoms underpin Australia's democracy, and has taken some key steps to ensure that these rights and freedoms are protected and promoted.

Press freedom is one of the fundamental pillars of Australia's democracy, and the Australian Government is committed to a free press. Press freedom plays an important role in keeping the public informed and our democratically elected officials and Government institutions accountable. However, press freedom is not absolute. Journalists, just like all Australians, are subject to the law of the land. Consistent with international human rights obligations, any limitations on press freedom should be reasonable, necessary and proportionate for the pursuit of a legitimate objective such as the protection of the rights or reputations of others or the protection of national security. Australian laws that contemplate such restriction include laws on national security and criminal justice, defamation, contempt of court and privacy.

The recent use of law enforcement powers to collect information in relation to journalists and media organisations has raised concerns regarding the appropriate balance between preserving press freedom and the imperative for law enforcement and intelligence agencies to investigate serious offending, including where media may hold evidence relevant to investigations of criminal conduct.

This submission seeks to demonstrate the appropriateness of the existing balance by providing further context around the historical approach to engagement between government and the media on matters reporting on national security, relevant legislative frameworks setting out the powers available to law enforcement and intelligence agencies in the context of investigations involving journalists or news media organisations. These investigations may not be directed at the journalist but related to the unlawful disclosure of information or other Commonwealth offences (for example, theft of Commonwealth property).

## Historical perspective

The underlying tension between freedom of the press and the need to safeguard national security information is not new and many governments have tried to find an appropriate balance.

This issue has been considered in a range of contexts including the Gibbs Review of Commonwealth Criminal Law in 1991, the Samuels and Codd Commission of Inquiry into the Australian Secret Intelligence Service in 1995, ongoing engagement with the media, the establishment of the Commonwealth Public Interest Disclosure regime in 2013, and recent reforms to Commonwealth secrecy offences in the *Criminal Code Act 1995* (Criminal Code).

Commonwealth governments have also, from time to time, undertaken engagement with the media on press freedom in the context of the appropriate balance between reporting on matters of public interest and protecting Australia's national security. Discussions of press freedom in Australia with media organisations has been occurring in various forms for many years.

For example, between 1952 and 1982, the Defence, Press and Broadcasting Committee operated the Defence Notice (D-Notice) system in Australia. The Committee, which consisted of politicians, representatives from Defence and the media, met to discuss matters of matters of national security.

A D-Notice outlined subjects relevant to significant matters of defence or national security, and requested editors to refrain from publishing certain information about those subjects. For example, matters relating to signals intelligence and communications security and capabilities of the Australian Defence Force. The D-Notice system was voluntary and non-observance of a request carried no penalties, and it was left to an editor to decide whether to publish certain information, having regard to national security requirements.

On 26 November 2010, the then Commonwealth Attorney-General, the Hon Robert McClelland MP, wrote to heads of Australian media organisations and policing agencies proposing the development of a formal, mutually agreed arrangement relating to the handling and publication of sensitive national security and law enforcement information.

At a round table convened by the former Attorney-General in April 2011, media and law enforcement representatives developed the following overarching principles regarding the publication of sensitive national security and law enforcement information:

- the overriding importance of preventing harm to the public and operational security and law enforcement personnel
- the preservation of freedom of speech and editorial independence
- the requirement for the protection of sensitive security and law enforcement information, in order for security and law enforcement agencies to effectively conduct their operation, and
- the inherent public interest in news relating to security matters

More recently, on 3 July 2019, the Attorney-General, the Hon Christian Porter MP, and the Communications Minister, the Hon Paul Fletcher MP, met with representatives from the ABC, Nine, News Corp, Free TV, SBS and Seven West Media to discuss the recent execution of search warrants by the Australian Federal Police. Attendees discussed matters relating to press freedom, including media organisations' suggestions for reform, and agreed that they would meet again in three months' time.

## Legislative frameworks relating to lawful disclosure of sensitive information

Commonwealth legislation provides for a number of avenues for the lawful disclosure of sensitive material under certain circumstances, including protections for those who disclose. These are discussed in detail below.

### Public Interest Disclosure Act 2013

The *Public Interest Disclosure Act 2013* (Public Interest Disclosure Act) provides extensive protections for whistleblowers who make disclosures in accordance with the Act, including disclosures made outside of government (external disclosures).

The Act applies to current and former public officials and has wide application to Commonwealth agencies, including Commonwealth companies, the Australian Defence Force, non-judicial staff of the federal courts, parliamentary departments, statutory office-holders and contracted service providers for Commonwealth contracts.

An independent review of the Public Interest Disclosure Act was undertaken by Mr Philip Moss AM (the Moss Review) and published in October 2016. It made 33 recommendations to improve the Public Interest Disclosure Act, which are being considered by the Government.

#### *Conduct that may be subject to a public interest disclosure*

Public interest disclosures can only be made in respect of conduct that falls within the definition of 'disclosable conduct', which includes contraventions of Commonwealth, and State or Territory laws, fraud and serious misconduct, corrupt conduct as well as minor wrongdoing. The Public Interest Disclosure Act excludes certain types of conduct from being 'disclosable conduct', such as where disclosures are made solely on the basis of disagreement with a policy or proposed policy, action or expenditure measure of the Government.

The Public Interest Disclosure Act distinguishes between disclosures that can be made internally (that is, to a government agency, an intelligence agency, the Commonwealth Ombudsman or Inspector-General of Intelligence and Security and disclosures that can be made outside of government. Each avenue has different requirements that must be met for the discloser to obtain the protections afforded by the Act, given that the information showing wrongdoing may contain sensitivities that necessitate different treatment. Further information on external disclosures is below.

#### *Protections for disclosers*

The Public Interest Disclosure Act provides a range of protections for public officials who make disclosures in accordance with the Act. If a disclosure complies with the Public Interest Disclosure Act, the Act provides the discloser with protection from any civil, criminal or administrative liability, including reprisals. The Public Interest Disclosure Act also protects information that identifies disclosers from being divulged, including in a court or tribunal, and enables disclosures to be made anonymously and without the discloser specifying that the disclosure is made under the Act.

#### *Disclosure and public reporting of sensitive and classified information*

The Public Interest Disclosure Act only permits the internal disclosure of intelligence information. This could consist of disclosure to the intelligence agency itself or to the Inspector-General of Intelligence and Security. The Act defines intelligence information as including information that has originated with, or has been received from, an intelligence agency, and sensitive law enforcement information.

The internal disclosure of intelligence information, to the intelligence agency itself or the Inspector-General of Intelligence and Security, enables the appropriate investigation of alleged Commonwealth wrongdoing. The Inspector-General of Intelligence and Security is responsible for overseeing the operation of the Public Interest Disclosure scheme as it applies to intelligence agencies, and assists intelligence agencies in meeting their obligations under the Public Interest Disclosure Act. In addition, the role of the Inspector-

General of Intelligence and Security provides an independent alternative for public officials who may not wish to report allegations of wrongdoing to the intelligence agency itself, which is the subject of the misconduct allegation. The Inspector-General of Intelligence and Security also has extensive powers that it can use in investigating allegations of wrongdoing, including requiring attendance of witnesses, taking sworn evidence, and copying and retaining documents.

External disclosure of intelligence information will not attract the Public Interest Disclosure Act's protections from criminal, civil or administrative liability. The limits on the public disclosure of intelligence information recognises the risks to national security that can arise from the disclosure of such information, including prejudice to individuals, operations and international relations. Relevantly, the Moss Review considered the treatment of intelligence information under the Public Interest Disclosure Act, but did not recommend that the existing framework for the handling of intelligence information should be changed.

#### *The public interest test*

The Public Interest Disclosure Act generally requires public officials to first raise allegations of public sector wrongdoing internally for investigation. This approach reflects the view that an agency is best placed to investigate allegations of wrongdoing within its own remit, having an understanding of existing policies and legislative frameworks, and an ability to access information for the purposes of an investigation more easily. This enables the effective and efficient investigation of disclosures. The Moss Review did not recommend any change to the general requirement for disclosures to be firstly made within government before being disclosed externally.

The Public Interest Disclosure Act enables public officials to disclose information externally if that information was disclosed in an internal disclosure, and the discloser is not satisfied with the adequacy of an investigation or a response to the investigation into that internal disclosure. Prior to making an external disclosure, the public official must also be satisfied that the disclosure 'is not, on balance, contrary to the public interest'. The discloser must consider whether the disclosure would promote the integrity and accountability of the Commonwealth public sector, the nature and seriousness of the conduct, and whether there is any risk that the disclosure could prejudice the proper administration of justice. These broad factors suggest that allegations of serious Commonwealth wrongdoing will generally be considered in the public interest to disclose.

An 'emergency disclosure' can be made without first going through an internal disclosure if the public official considers that the information concerns a substantial and imminent danger to the health or safety of one or more persons, or the environment. Disclosures can also be made to legal practitioners (without first making an internal disclosure) for the purposes of obtaining legal advice in relation to the making of a disclosure under the Public Interest Disclosure Act (a 'legal practitioner disclosure'). There is no public interest test associated with either of these types of disclosures. However, a person cannot disclose intelligence information as part of an emergency disclosure or a legal practitioner disclosure.

#### *Culture, practice and leadership for Government and senior public employees*

The Public Interest Disclosure Act aims to foster a culture that encourages and facilitates the disclosure of wrongdoing. In addition to the protections afforded to public officials who disclose wrongdoing, the Public Interest Disclosure Act also obliges various public officials to support the effective functioning of the scheme. For instance, the Commonwealth Ombudsman, heads of Commonwealth agencies and officers that are authorised to receive disclosures under the Public Interest Disclosure Act have additional obligations to ensure that disclosers are supported. These obligations are in addition to existing obligations that are provided under other public service frameworks, such as the Australian Public Service Code of Conduct and Values. The Commonwealth Ombudsman publishes standards and guidance to facilitate the appropriate investigation of disclosures made under the Public Interest Disclosure Act.

The Commonwealth Ombudsman's oversight functions under the Public Interest Disclosure Act include publishing guidance and annual reports on the operation of the Act (as part of the Ombudsman's Annual Report). The Inspector-General of Intelligence and Security has oversight functions for the intelligence agencies. Agencies must notify the Ombudsman and the Inspector-General of Intelligence and Security of certain actions relating to the handling of disclosures.

## Freedom of Information Act 1982

The *Freedom of Information Act 1982* (Freedom of Information Act) seeks to balance competing interests of access with the need to appropriately protect Government deliberations and sensitive information. It is also important to note that the vast majority of Freedom of Information requests do not relate to requests from media, but to individuals seeking their own information from government.

There have been a number of significant reviews of the Freedom of Information regime over recent years, including Dr Allan Hawke's independent Review of the Freedom of Information Act and the *Australian Information Commissioner Act 2010* in 2013 (Hawke Review), the independent Review of Whole-of-Government Internal Regulation (Belcher Red Tape Review) in 2015, and Professor Peter Shergold's independent review of government processes for the development and implementation of large public programmes and projects.

### *Intelligence and security agencies*

A comprehensive review of the Acts governing Australia's intelligence community is currently being undertaken to ensure agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians – this includes under the Freedom of Information Act.

The review will comprehensively examine the effectiveness of the legislative framework governing the National Intelligence Community and prepare findings and recommendations for reforms. The review will prepare a classified report for the Government by the end of 2019, followed by an unclassified version of that report.

## Criminal law and law enforcement powers

There are clear rules and protections in place to support freedom of the press, which are subject to ongoing review by relevant policy departments. This section provides a discussion of the criminal law and the legal frameworks governing powers available to law enforcement and intelligence agencies that are relevant to the inquiry.

There are a number of offences across Commonwealth criminal law that could potentially give rise to the exercise of law enforcement powers in the context of the activities of journalists and media organisations. These include refused classification offences, abhorrent violent material offences, as well as offences relating to unauthorised disclosure of material. Where relevant, some offences already include a specific defence for journalists, including the secrecy offences in Part 5.6 of the Criminal Code.

### General secrecy offences

The new general secrecy offence in Part 5.6 of the Criminal Code commenced in December 2018. The offences apply to two types of information. The first is information that is inherently harmful, and the second is information that causes harm to Australia's interests, or will or is likely to cause harm to Australia's interest (harm based offences).

Information is 'inherently harmful' where the information is classified 'secret' or 'top secret', was obtained or made by or for a domestic or foreign intelligence agency in connection with that agency's functions, or relates to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency. As indicated above, the secrecy offences in the Criminal Code will only apply to information that has a security classification of secret or top secret if the prosecution can prove that the information, if disclosed, could be expected to cause serious damage to the national interest or organisations or individuals, or exceptionally grave damage to the national interest (see definition of 'security classification' in section 90.5). In addition, where the information is inherently harmful on the basis of its security classification, the Attorney-General must certify that any information that is security classified has been appropriately classified at the 'secret' or 'top secret' classification level when giving his or her written consent to prosecute this offence. The prosecution would be required to prove harm or damage as a matter of fact in a prosecution.

In response to the advisory report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 of the Parliamentary Joint Committee on Intelligence and Security, the Government

agreed to the Committee's recommendation that the Attorney-General initiate a review of existing secrecy offences, taking into account the principles set out by the Australian Law Reform Commission in its report, *Secrecy Laws and Open Government in Australia* (Recommendation 24).

Specific secrecy offences that attach criminal sanctions should generally only apply where the information would cause, or is likely or intended to cause, harm to an essential public interest and this is the basis of the current secrecy offences regime. In the majority of circumstances, it is necessary to include an express proof of harm requirement in specific secrecy provisions. However, there are some circumstances where the character of the information itself points to the prospect or type of harm that may result from disclosure.

*'Public interest' defence for secrecy offences in Part 5.6 of the Criminal Code*

The accused must discharge the evidential burden pursuant to section 13.3 of the Criminal Code. This would not change were the provision reframed as an exemption.

A defendant can discharge an evidential burden by adducing or pointing to evidence that suggests a reasonable possibility that the exception has been met. If they do so, it would then be for the prosecution to disprove the matter beyond reasonable doubt. A defendant may be able to rely on evidence that forms part of the prosecution case or could lead evidence as part of the defence case, to discharge the burden. The question of whether the evidential burden has been satisfied is a question of law, to be decided by a judge. If discharged, the question of whether the prosecution has disproven the defence/exemption beyond reasonable doubt is put to a jury.

The journalist defence in Part 5.6 of the Criminal Code only requires that the person raise evidence they 'reasonably believed' that engaging in the conduct was in the public interest, i.e. they already do not need to 'prove' that their conduct was in the public interest.

Further, as per the Prosecution Policy of the Commonwealth, the prosecution will also consider whether there is a reasonable prospect of a conviction being secured prior to proceeding with a prosecution, including consideration of any lines of defence that are open to the defendant. This would include consideration of both defences and exemptions alike.

### **General powers available to agencies**

There are a range of relevant powers available to law enforcement and intelligence agencies in the investigation of the commission of possible criminal offences and for national security purposes. Such powers include, but are not limited to, those contained in the following Acts:

- *Crimes Act 1914* (Cth) (Crimes Act)
- *Telecommunications (Interception and Access) Act 1979* (Cth) (Telecommunications Interception and Access Act)
- *Surveillance Devices Act 2004* (Cth) (Surveillance Devices Act)

While these powers could be used in relation to journalists, this would be an infrequent occurrence.

*Crimes Act 1914*

Under section 3E of the Crimes Act, an issuing officer may issue a warrant to search premises if the officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises.

The occupier of the premises concerned in the warrant need not be the subject of the investigation. For the purposes of these provisions, evidential material means a thing relevant to an indictable or summary offence, including such a thing in electronic form. Also for these purposes, the issuing officer may be a magistrate, or a justice of the peace or other person employed in a court of a State or Territory who is authorised to issue search warrants or warrants for arrest.

The warrant must state:

- the offence to which the warrant relates; and
- a description of the premises to which the warrant relates or the name or description of the person to whom it relates; and
- the kinds of evidential material that are to be searched for under the warrant; and
- the name of the constable who, unless he or she inserts the name of another constable in the warrant, is to be responsible for executing the warrant; and
- the time at which the warrant expires; and
- whether the warrant may be executed at any time or only during particular hours.

If a warrant in relation to premises is being executed and the occupier of the premises or another person who apparently represents the occupier is present at the premises, the executing officer or a constable assisting must make available to that person a copy of the warrant. The executing officer must also identify themselves to the person at the premises being searched. Warrants issued under section 3E of the Crimes Act are subject to a range of safeguards, including the requirements for the independent issuing officer, the detail that must be stated in the warrant and the requirement that details of the warrant be given to the occupier.

#### *Telecommunications (Interception and Access Act) 1979*

The Telecommunications Interception and Access Act provides for the issuing of warrants to eligible law enforcement and intelligence agencies to intercept communications, access stored communications, or authorise the disclosure of data.

Chapter 4 of the Telecommunications Interception and Access Act enables designated criminal law enforcement agencies and the Australian Security Intelligence Organisation to authorise a carrier to disclose telecommunications data for certain defined purposes such as enforcing the criminal law or for the performance of the Australian Security Intelligence Organisation's functions.

These provisions do not allow for the disclosure of the content of a communication, and only permit such disclosure for a narrow range of purposes. Further, the Telecommunications Interception and Access Act contains reporting and record-keeping obligations.

The journalist information warrant framework was introduced by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* as an added protection mechanism to raise the threshold for agencies' access to telecommunications data in specific cases in which agencies seek to access a journalist's telecommunications data for the purposes of identifying a source. The framework requires criminal law enforcement agencies to obtain a warrant issued by a judge, magistrate, or senior Administrative Appeals Tribunal member (see 'Thresholds for the access of electronic data' below for further information).

Journalist information warrants ensure that press freedom is appropriately considered in the investigation process.

### **Journalist information warrants**

The below information gives an overview of the existing journalist information warrant regime, which provides a specific framework to strictly limit agencies' ability to make authorisations to access a journalist's, or their employer's, telecommunications data for the purposes of identifying a confidential source.

#### *Application of the journalist information warrant framework*

An individual may be subject to a journalist information warrant only if they are working as a journalist in a professional capacity. The Revised Explanatory Memorandum of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act) lists indicators that a person is acting in a professional capacity, including: regular employment, adherence to enforceable ethical standards and membership of a professional body.

*Oversight of journalist information warrants*

Under the regime, the chief officer of the Australian Security Intelligence Organisation or an enforcement agency may request the Attorney-General (for the Australian Security Intelligence Organisation) or the issuing authority (Judge, Magistrate or senior Administrative Appeals Tribunal member) to issue a journalist information warrant in relation to a particular person. This request must specify the facts or grounds on which the requesting agency considers the warrant necessary. This provision requires the requesting law enforcement and integrity agencies to identify that the warrant will be used for: the enforcement of the criminal law; the enforcement of a law imposing a pecuniary penalty; the protection of public revenue; locating a missing person or the investigation of a serious offence. Similarly, the Australian Security Intelligence Organisation must demonstrate the relevance of the warrant to the Australian Security Intelligence Organisation's legitimate functions.

*Balancing of the public interest test*

The Attorney-General or issuing authority must not issue a journalist information warrant unless they are satisfied that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source. In conducting the public interest assessment, an issuing authority must take into account: the extent of the interference in the journalist's privacy; the gravity of the matter for which the warrant is sought; the potential significance of the telecommunications data to the investigation; whether the information could be obtained through other means and any other matter the issuing authority considers relevant. The issuing authority is required to refuse a request to issue a journalist information warrant if the proposal does not meet the stated considerations.

*Contestability of journalist information warrants and role of the Public Interest Advocate*

The journalist information warrant system does not provide the affected person the opportunity to contest the issue of a warrant, as is consistent across Australian national security legislation. However, a Public Interest Advocate (who must be a retired senior judge or a security cleared Queen's Counsel or Senior Counsel) is required to provide an independent and impartial public interest assessment before a journalist information warrant can be issued. The role of the Public Interest Advocate in the journalist information warrant scheme was specifically designed to account for the public interest while ensuring timely review for investigations into serious crimes that impact national security.

The journalist information warrant framework provides for the Public Interest Advocate to make a submission to the issuing authority of the warrant as to the propriety of the enforcement agency's application. Before making an application for a journalist information warrant, the agency requesting the warrant must ensure that a copy of the application is provided to a Public Interest Advocate. The Public Interest Advocate prepares an independent submission to the issuing authority on the proposed undertaking of each application for a journalist information warrant. The Public Interest Advocate's determination should provide the basis for the issuing authority's ultimate decision on whether the warrant is in the public interest. As identified in the Department of Home Affairs' submission into the Committee's inquiry into the Data Retention Act, the role of the Public Interest Advocate in relation to the issuing of a journalist information warrant is outlined in regulations, rather than the Telecommunications Interception and Access Act itself.

*Broadening the application of the journalist information warrant scheme to increase protection for sources*

The purpose of the journalist information warrant scheme is to strictly limit agencies' ability to make authorisations to access a journalist's, or their employer's, telecommunications data for the purposes of identifying a confidential source by requiring agencies to obtain a warrant. Under this scheme, agencies must obtain a journalist information warrant before they can access the telecommunications data of a journalist or their employer for the purpose of identifying a journalist's source. One of the key considerations to be demonstrated by the requesting agency, and assessed by the issuing authority, is "whether reasonable attempts have been made to obtain the information or documents by other means". This requires an agency to have reasonably exhausted other methods of identifying the person of interest in their investigation.

The scheme does not put additional protections in place for agencies' access to the telecommunications data of the source, where the agency is not relying on a journalist's data to identify this source. The policy justification underpinning the current journalist information warrant scheme is to protect the relationship of trust between a journalist and their source. The journalist information warrant scheme is not intended to prevent law enforcement from pursuing other means of identifying a suspect who has leaked classified information without accessing a journalist's data.

As discussed above, other Commonwealth legislation contains protections for whistle-blowers who seek to make disclosures which are genuinely in the public interest. External disclosures are subject to different processes. The legislative frameworks that impact upon whistle-blowers and the media remain under review to ensure that they continue to strike the right balance, and that they are reasonable, effective and fit for purpose.

For example, a privilege exists under the *Evidence Act 1995* in relation to journalist sources. Sections 126J and 126K provide for the presumption that a journalist or their employer are not required to provide information that would enable a source's identity to be ascertained, if the journalist has promised not to disclose their source's identity.

This presumption can be rebutted in circumstances where the public interest in the disclosure of that evidence outweighs any likely adverse effect of the disclosure for the informant or another person as well as the public interest in communication of information to the public by the media. For the court to be satisfied that such a disclosure is in the public interest, the public interest must outweigh:

- any likely adverse effect of disclosure upon the source of the information or any other person, and
- the public interest in freedom of the press that requires journalists to be able to obtain information from sources.

## Issue of warrants

At a Commonwealth level, the level of oversight in issuing warrants varies depending on the type of warrant and, in appropriate circumstances, may differ depending on which agency is seeking the warrant. The following table broadly summarises the relevant types of warrants, associated legislative frameworks and the officers who may issue each warrant:

Type of warrant	Provision	Issuing officer
Search warrant	Section 3E, <i>Crimes Act 1914</i>	<ul style="list-style-type: none"> <li>• Magistrate</li> <li>• Justice of the Peace</li> <li>• Other person employed in a court of a State or Territory who is authorised to issue search warrants or warrants for arrest</li> </ul>
Interception warrant	Sections 9, 9A, 10, 46 and 46A, <i>Telecommunications (Interception and Access) Act 1979</i>	<ul style="list-style-type: none"> <li>• Eligible Judge</li> <li>• Nominated Administrative Appeals Tribunal member</li> <li>• Appointed Magistrate (except for interception warrants)</li> </ul>
Stored communications warrant	Section 116, <i>Telecommunications (Interception and Access) Act 1979</i>	<i>For certain warrants issued to ASIO</i> <ul style="list-style-type: none"> <li>• Attorney-General</li> </ul>
Journalist information warrant	Sections 180L, 180M and 180T, <i>Telecommunications (Interception and Access) Act 1979</i>	<ul style="list-style-type: none"> <li>• Director-General of Security (for warrants issued in an emergency)</li> </ul>

Computer access warrant	Section 27C, <i>Surveillance Devices Act 2004</i>	<ul style="list-style-type: none"> <li>• Eligible Judge</li> <li>• Nominated Administrative Appeals Tribunal member</li> </ul>
Surveillance devices warrant	Section 16, <i>Surveillance Devices Act 2004</i>	

As outlined above, restrictions as to who is authorised to issue warrants varies, with warrants permitting law enforcement to undertake particularly intrusive activities required to be issued by an eligible Judge, appointed Magistrate or nominated Administrative Appeals Tribunal member. Each warrant type also has specific requirements and thresholds that must be met prior to issuing a warrant. On each occasion, the issuing officer must ensure that the relevant subjective and/or objective tests set out in the legislation are met prior to issuing a warrant.

For example, section 3E of the Crimes Act requires the issuing officer to be satisfied on information provided on oath or affirmation that there are reasonable grounds for suspecting that there is, or will be within the next 72 hours, evidential material at a premises, prior to issuing a search warrant. The requisite level of satisfaction that the issuing officer must reach to issue a search warrant does not vary or lessen simply because the officer holds of a position other than that of a Judge.

It is not uncommon for officers other than Judges to be authorised to issue search warrants, with such requirements varying between the Commonwealth, states and territories. As an example, section 48 of the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) authorises Magistrates, Local Court registrars and authorised officers of the NSW Attorney-General's Department to issue search warrants (other than covert or criminal organisation search warrants).<sup>1</sup> If the warrant sought is a covert search warrant or criminal organisation search warrant, then issuing of such warrants is restricted to eligible Judges, being a nominated Judge of the Supreme Court of NSW.<sup>2</sup>

The Australian Federal Police has indicated that it currently encounters operational difficulties with the availability of magistrates. For example, in some jurisdictions where there are no on-call magistrates it can be difficult to have applications heard outside of a court hours. If amendments were introduced to increase judicial oversight of the above warrant schemes, by requiring such warrants to be issued by a Judge in all circumstances, the Australian Federal Police anticipates that these operational difficulties will increase.

Submissions to the Parliamentary Joint Committee inquiry also suggested the implementation of a legislated public interest test, to be applied by an issuing officer when issuing a search warrant in relation to a journalist or media organisation. Pursuant to section 37(2) of the *Australian Federal Police Act 1979* (Australian Federal Police Act), the Minister for Home Affairs issued a direction to the Australian Federal Police on 8 August 2019, requiring the Australian Federal Police to consider the importance of a free and open press as well as broader public interest implications, and to exhaust alternative investigative actions, before undertaking investigative action involving journalists. The Ministerial Direction, in conjunction with the existing subjective and/or objective tests an issuing officer must consider prior to issuing a warrant, ensure that the public interest is a key consideration in the issuing of search warrants in relation to journalists and media organisations.

## Operational independence of the Australian Federal Police

A key function of the Australian Federal Police is, and must remain, the enforcement of the criminal law. The Australian Federal Police has a statutory function to act independently from Government when conducting investigations into breaches of Commonwealth law. The Australian Federal Police cannot legally be directed by the Government, an individual Minister, or a Department to exercise, or abstain from exercising, police powers in an individual investigation. This includes investigating all forms of criminal conduct including investigations into the possible commission of offences relating to the unauthorised disclosure of information.

<sup>1</sup> *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) ss 3, 46 and 48.

<sup>2</sup> *Ibid* ss 46, 46B and 48.

On 9 August 2019, the Minister for Home Affairs issued a Ministerial Direction to the Australian Federal Police Commissioner outlining the Government's expectations for the Australian Federal Police in relation to investigative action involving a professional journalist in the context of an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer. The Direction was issued under subsection 37(2) of the *Australian Federal Police Act 1979*, which allows the Minister to, after seeking the advice of the Australian Federal Police Commissioner and of the Secretary, give written directions with respect to the general policy to be pursued in relation to the performance of the Australian Federal Police's functions. Nothing in the Direction constrains the ability of the Australian Federal Police to investigate possible breaches of Commonwealth law.

The Australian Federal Police submission to this inquiry further addresses referral practices in relation to unauthorised disclosures of sensitive information.

## Related matters

Public discussion, including in the context of the Parliamentary Joint Committee on Intelligence and Security's inquiry (the Parliamentary Joint Committee inquiry), has raised various proposals with regard to legislative frameworks relating to freedom of the press, primarily the exercise of law enforcement and intelligence powers against journalists and media organisations. A number of submissions to this Committee have also raised similar proposals to those made to the Parliamentary Joint Committee. The key proposals or issues raised are discussed in detail below.

### Amendments to secrecy offences

A number of submissions to the Parliamentary Joint Committee inquiry proposed amendments to the secrecy offences in the Criminal Code. These are discussed in detail below.

#### *Exemptions from national security laws for a broadly defined class of 'journalists'*

Expanding the scope of exemptions for journalists to any person who publishes information on the internet would create a very broad and imprecise immunity that would significantly undermine the operation of national security laws. In particular, consideration may be required as to whether such an expanded exemption would undermine the fundamental purpose of secrecy offences to prevent harmful disclosures of Government information.

#### *Inclusion of public interest as an element for secrecy offences in Part 5.6 of the Criminal Code*

In considering proposals to incorporate 'public interest' as an element of the offence rather than a defence or exemption, the benefits and costs of requiring the prosecution to prove this additional element beyond reasonable doubt need to be taken into account.

Such an approach would increase the complexity of a prosecution as, in addition to proving that a disclosure is harmful the prosecution would also need to prove that the conduct was not in the 'public interest' and that the person was not 'engaged in the business of reporting news etc'. It would require the prosecution to prove the non-existence of these additional elements in every prosecution, even where they were not relevant. This would be significantly burdensome for the prosecution when compared to the current approach of Part 5.6 of the Criminal Code, which provides defences for the defendant to raise as appropriate and only where relevant to the individual facts and circumstances of the particular case.

Further, there is unlikely to be a substantive benefit given the offences are targeted only at disclosures that cause harm and already provide clear exemptions for those who are reporting news and current affairs in the public interest.

#### *Attorney-General consent for all offences that may be used to prosecute journalists*

Offences in Part 5.6 of the Criminal Code and a number of other offences already contain a provision requiring the consent of the Attorney-General prior to commencing a prosecution.

There are other offences across the Commonwealth statute book that could potentially be used to prosecute journalists, but further consideration could be given to offences for which it may be appropriate to do so.

## Classification of documents as secret

Submissions to the Parliamentary Joint Committee inquiry proposed that there should be limits on which documents should be stamped 'secret' and that audit mechanisms should be introduced to confirm appropriate classification of information.

The use of information classifications, including secret and top secret, is already clearly defined and limited under the Protective Security Policy Framework, and in the *Criminal Code Act 1995* (Criminal Code) in relation to the application of secrecy offences. Under the Protective Security Policy Framework, information is only to be classified secret where the compromise of the information would be expected to cause 'serious damage' to the national interest, organisations or individuals. Information is only to be classified top secret where the compromise of the information would be expected to cause 'exceptionally grave damage' to the national interest, organisations or individuals.

The Protective Security Policy Framework is mandatory for all non-corporate Commonwealth entities under section 21 of the *Public Governance, Performance and Accountability Act 2013* (Public Governance, Performance and Accountability Act) (to the extent consistent with their legislation) and represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies under the Public Governance, Performance and Accountability Act. As at 9 August 2019, there are 101 non-corporate Commonwealth entities, which includes all Commonwealth departments and law enforcement and intelligence agencies.

The application of particular security classification markings does not, in itself, create any legal consequences. The secrecy offences in the Criminal Code will only apply to information that has a security classification of secret or top secret if the prosecution can prove that the classification was applied in accordance with the Protective Security Policy Framework such that the information, if disclosed, could be expected to cause serious damage to the national interest or organisations or individuals, or exceptionally grave damage to the national interest (see definition of 'security classification' in section 90.5 of the Criminal Code). This would have to be demonstrated in any prosecution. In addition to that, as part of the Attorney-General's requirement to give written consent to any prosecution, the Attorney is also required, in any prosecution for those offences, to certify that any information that is security classified has been appropriately classified as secret or top secret, as applicable.

In view of the above, the costs of creating an audit mechanism for classification of documents – such as appointing an independent person – are likely to outweigh the benefits, particularly as there is no indication that there is a systemic issue with the classification of information.

## Defamation

Submissions to the Parliamentary Joint Committee inquiry raised concerns about the procedures and provisions in defamation cases across Australia. These issues are currently being considered by the Council of Attorneys-General Defamation Working Party.

While the Attorney-General's Department is representing the Commonwealth on the Council of Attorneys-General Defamation Working Party, the Commonwealth is not currently a party to the Intergovernmental Agreement and has not enacted a defamation law. Accordingly, reform to defamation law is primarily a matter for the states and territories.

The proposal to introduce a right to trial by jury in Federal Court defamation matters requires further consideration as it would have practical and resourcing implications. In the Federal Court, the starting point for civil trials is by judge alone without a jury. In addition, there is not a consistent approach in the use of juries in civil trials amongst the states and territories – in New South Wales, Victoria, Queensland, Western Australia and Tasmania, either party may elect for a jury, unless the court orders otherwise, whereas in South Australia, the Australian Capital Territory and Northern Territory, juries have no role.

## Media Freedom Act

Some submissions to the Parliamentary Joint Committee inquiry proposed that there should be legislated recognition of the freedom of the press.

The Australian common law provides particularly strong protections for freedom of speech related to public affairs and political matters. The courts have also recognised an implied constitutional freedom of political communication. Laws which restrict communication about government or politics are invalid if they impermissibly infringe the implied freedom.

Legislative frameworks already contain a suite of protections, including high thresholds and safeguards in the framing of relevant powers, requirements to seek warrants from appropriate issuing authorities and a discrete framework for journalist information warrants under the Telecommunications Interception and Access Act to enable the protection of confidential sources.

Press freedom is not absolute and a broad immunity from the application of Australian laws would not be appropriate. International human rights law recognises that limitations on press freedom are permissible where they are reasonable, necessary and proportionate for the pursuit of a legitimate objective such as the protection of the rights or reputations of others or the protection of national security. This needs to be determined on a case-by-case in the context of particular legislative restrictions. The potential consequential impacts of any immunities or protections for media also need to be taken into account as they could also impede law enforcement's ability to investigate other (non-journalist) persons of interest, and investigate persons who are journalists by occupation in situations that do not relate to public interest reporting.

## Contested warrants

A number of submissions to the Parliamentary Joint Committee inquiry called for the introduction for contested hearings in relation to search warrants issued against journalists or media organisations, citing the use of such a scheme in the United Kingdom.

Under United Kingdom criminal legislation, there are a number of avenues for obtaining evidential material from professional journalists, depending on the kind of material sought and the nature of the suspected offence – these include by search warrant and, in a limited set of circumstances, by production order.

Search warrants in the United Kingdom broadly operate in a similar manner to the Australian context. Search warrants are available to law enforcement under a range of legislation, such as the *Official Secrets Act 1911* (UK) (Official Secrets Act). Where requirements under the legislation are met, search warrants may authorise law enforcement to enter (by force if necessary) and search a premises and seize evidence. Search warrants are obtained via an *ex parte* hearing, meaning there is no opportunity for the issuing of the warrant to be contested.

In a limited set of circumstances, such as where the legislative requirements for the issue of a search warrant are not met, law enforcement may seek to obtain journalistic material under a production order. An application for a production order must be heard *inter partes*, which provides an opportunity for the issuing of the order to be contested.<sup>3</sup> This would not relate to the production of documents such as those to support an unauthorised disclosure of material investigation as this would, given the threshold of the offences, use a search warrant. A production order might be used in scenarios where the police would require access to news footage of an event to assist with an investigation.

The United Kingdom's search warrants laws are currently under review by the United Kingdom Law Commission, including the production order provisions discussed above. As such, caution should be exercised in relying upon the United Kingdom as a basis for reforming the laws governing search and seizure of journalistic material in Australia until the outcomes of that review are known. Further information about warrant schemes in Canada, New Zealand, the United Kingdom and the United States, and the interaction of such schemes with journalists and media organisations, is provided at **Attachment A**.

<sup>3</sup> United Kingdom Law Commission, 'Search Warrant Consultation Paper'188 (see footnote 726). *R v Leicester Crown Court ex parte DPP* [1987] 1 WLR 1371 established the requirement for applications for orders of this nature to be heard *inter partes*.

As required by the 'Ministerial Direction to the Australian Federal Police Commissioner relating to investigative action involving a professional journalist or news media organisation in the context of an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer', the Australian Federal Police are expected to exhaust alternative investigative actions prior to executing a search warrant upon a professional journalist or media organisation when investigating the unauthorised disclosure of classified material. Alternative investigative actions may include, where appropriate, seeking voluntary assistance from a journalist or media organisations. As such, the execution of search warrants upon journalists and media organisations are effectively already used as a mechanism of last resort in such circumstances whereby evidence is sought from media organisations and journalists.

As demonstrated by legal proceedings brought against the Australian Federal Police by the Australian Broadcasting Corporation and News Corp Australia, journalists and media organisations have access to legal recourse through which the validity of a warrant may be challenged, during which access to seized materials may be restricted.

Implementing a mandatory procedure by which the issuing of a search warrant can be contested before it is exercised has the potential to undermine the efficacy of such a warrant, and the ability of law enforcement or intelligence agencies to effectively investigate criminal activities. For example, providing an opportunity to contest a warrant would necessarily alert a person of interest (potentially including a suspect) to the existence and particulars of a law enforcement investigation, and may provide an opportunity to destroy evidence, or relocate evidence to another location or jurisdiction. In comparable jurisdictions, such as the United Kingdom, contestability only applies to production order regimes (which apply to a limited set of circumstances) rather than to the issue of search warrants.

Although such consequences may not transpire on every occasion, should an opportunity be provided to contest the issuing of a warrant, there remains a real and substantial risk that the effectiveness of law enforcement and intelligence investigations could be compromised through an inability to collect evidence. It is critical that law enforcement and intelligence agencies can continue to exercise their powers, including through the execution of search warrants, to support investigations into leaks of classified material, which have the potential to cause grave damage to Australia's national interest, organisations or individuals.

Submissions have also proposed the implementation of a Public Interest Advocate model for the issuing of search warrants against journalists and media organisation, similar to the regime utilised under the *Telecommunications Interception and Access Act 1979* (Telecommunications Interception and Access Act) in relation to journalist information warrants (discussed above). Under the journalist information warrant scheme, a Public Interest Advocate has up to seven days to prepare a submission in relation to the issuing of a journalist information warrant.

There is a small but significant risk that a Public Interest Advocate regime could cause delays to investigations unrelated to whistle-blowing. The Public Interest Advocate model is not limited to unauthorised disclosure investigations and there is potential for a situation where police need to identify a journalist's source for an investigation entirely unrelated to whistle-blowing, and where the investigation needs to progress quickly due to ongoing harm, or risk of imminent harm to the community or an individual. The current legislative regime anticipates such situations and provides a framework where police can obtain a search warrant within minutes over the phone in urgent cases. A Public Interest Advocate regime may also have an impact on the ability of the Australian Federal Police to collect evidence about Commonwealth officials who have committed offences by disclosing sensitive material.

The departments also note that the existing Commonwealth search warrant legislative framework includes subjective and/or objective tests for each warrant which must be met prior to issuing a warrant. The requirement for issuing authorities to ensure these tests are met is intended to provide assurance that the issue of a warrant is appropriate in the context of the relevant law enforcement investigation. Where a party believes the requisite test was not properly considered, they can seek judicial review of the decision to issue the warrant on that basis.

## Reporting requirements relating to Public Interest Advocates

Submissions to the the Parliamentary Joint Committee inquiry suggested the introduction of annual reporting requirements regarding the number and identity of Public Interest Advocates and the number of cases where a Public Interest Advocate either successfully or unsuccessfully opposed a journalist information warrant. The number and identity of Public Interest Advocates has been tabled in Parliament, and is publicly available.<sup>4</sup> However, the proposal for additional transparency measures in relation to Public Interest Advocates should be carefully considered, including in light of any benefits or risks associated with a former judicial officer being publicly identified as a Public Interest Advocate and disclosure of their actions in the course of their duty – either in general or in relation to a particular journalist information warrant.

## Broader application of the public interest test for other types of Telecommunications (Interception and Access) warrants

Under the regime of oversight governing the more intrusive powers such as telecommunications interception warrants, stored communications access warrants, computer access warrants and surveillance device warrants, agencies must apply to the Attorney-General or an eligible Judge or nominated Administrative Appeals Tribunal member in order to obtain a warrant. There are also strict thresholds for the types of serious offences those warrants can be granted for. This level of oversight and the restrictions on when such warrants can be used is designed to protect the public interest by ensuring that such intrusive powers are only used where strictly necessary for the purpose of investigating serious offences or in the interests of national security.

Such warrants would not be available to law enforcement for the purpose of investigating the offence of unauthorised disclosure of information by Commonwealth officers because this is a two year offence and therefore does not meet the threshold for a 'serious offence' or 'serious contravention' for the purpose of the Telecommunications Interception and Access Act or a 'relevant offence' for the purpose of the *Surveillance Devices Act 2004*. These warrants may be available for investigations of the more serious offences under Part 5.6 of the Criminal Code such as communicating inherently harmful information or of Commonwealth officers communicating information which causes, or is likely to cause, harm to Australia's interests.

The journalist information warrant scheme was introduced in response to concerns raised in the Parliamentary Joint Committee on Intelligence and Security's 2014 inquiry into the proposed mandatory data retention regime under the Telecommunications Interception and Access Act. These concerns related to agencies' access to 'privileged or otherwise sensitive' metadata for the purpose of identifying a journalist's confidential sources. Such added protections and mandated consideration of the public interest was considered necessary to balance the interest in protecting journalists in relation to authorisations for access to telecommunications data which may be made internally by an approved Australian Security Intelligence Organisation employee or authorised officer of an enforcement agency. As noted by the Inspector-General of Intelligence and Security, authorisations for access to telecommunications data are less intrusive than other powers under the Telecommunications Interception and Access Act as they do not allow for access to the content of a communication. The journalist information warrant scheme aims to balance the public interest in protecting journalists' sources, while ensuring agencies have the investigative tools necessary to investigate offences and protect the Australian community.

## Public reporting requirements for the Australian Security Intelligence Organisation

An existing reporting mechanism in relation to journalist information warrants is provided in section 94 of the Australian Security Intelligence Organisation Act. It provides that the Director-General of the Australian Security Intelligence Organisation must include mandated statements in the annual report, including statements on the number of 'journalist information warrants' issued during the relevant period and the number of authorisations made under journalist information warrants. The report, in its whole form, is provided to the Minister and the Leader of the Opposition. The Minister is then responsible for tabling the report, but may, after receiving advice from the Director-General, make deletions to the report as considered

<sup>4</sup> The list of eight Public Interest Advocates appointed in 2015 was included in information tabled before the Senate Standing Committee on Legal and Constitutional Affairs in response to question AE16/099 from then Senator Ludwig.

necessary to avoid prejudice to either security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs or the privacy of individuals.

The use of journalist information warrants by all other agencies are reported publicly in the Telecommunications Interception and Access Act Annual Reports. The Australian Security Intelligence Organisation currently reports to the Attorney-General on its use of special powers, being the Australian Security Intelligence Organisation's most intrusive powers. This includes the Australian Security Intelligence Organisation's special powers (section 34 of the Australian Security Intelligence Organisation Act), special powers relating to terrorism offences (section 34ZH) and special intelligence operations (section 35Q).

## Attachment A

## Five Eyes' search warrant schemes and protections for journalists

This attachment briefly sets out the search warrants schemes utilised in other Five Eyes countries, with a particular focus on how such schemes apply to journalists and media organisations. Where applicable, protections for journalists against the disclosure of confidential sources are also discussed.

### Canada

In 2017, Canada introduced the *Journalistic Sources Protection Act* (SC 2017, c. 22) which amended the *Criminal Code* (RSC 1985, c. C-46) and the *Canada Evidence Act* (RSC 1985, c. C-5) with the aim of protecting the confidentiality of journalists' sources. In particular, amendments to the Canada Evidence Act enable journalists to refuse to disclose information or documents to a court, person or body, if the information or documents identify or are likely to identify a journalistic source, unless:

- the material cannot be obtained by any other reasonable means, and
- the public interest in the administration of justice outweighs the public interest in preserving the confidentiality of the journalistic source.

In applying this public interest test, the court, body or authority must have regard to the importance of the information or document to a central issue in the proceeding, the freedom of the press and the impact of disclosure on the journalistic source and the journalist.

For these purposes of these provisions, a journalist is defined as a person whose main occupation is to contribute directly to the collection, writing or production of information for dissemination by the media, or any person who assists such a person. A journalistic source is defined as a source who confidentially provides information to a journalist on the basis of an undertaking by the journalist not to divulge the source's identity, and whose anonymity is essential to the relationship between the journalist and the source.

Amendments to the Canadian Criminal Code also impose greater requirements upon the issuing of warrants, authorisations and orders, for applications relating to a journalist's communications and materials relating to or in the possession of a journalist. For such an application, a judge may only issue a warrant, authorisation or order if they are satisfied that:

- there is no other way by which the information can reasonably be obtained, and
- the public interest in the investigation and prosecution of a criminal offence outweighs the journalist's right to privacy in gathering and disseminating information.

These requirements are imposed in addition to the other requirements that must be met for the issuing of a warrant, authorisation or order. In determining an application, a judge may, at their discretion, request that a special advocate provide observations on these requirements, in the interests of freedom of the press.

However, these additional requirements do not apply in relation to an application for a warrant, authorisation or order that is made in relation to the commission of an offence by a journalist. If an application is made in relation to an offence committed by a journalist, the issuing judge may order that some or all materials seized under the warrant, authorisation or order be sealed and kept in the custody of the court, if the judge considers such a requirement is necessary to protect a journalistic source.

### New Zealand

Section 68 of the *Evidence Act 2006* (NZ) provides for the protection of confidentiality of journalists' sources. If a journalist has promised an informant not to disclose the informant's identity, neither the journalist nor his or her employer is compellable in a civil or criminal proceeding to answer questions or produce documents that would disclose the identity of the informant or enable the informant's identity to be discovered.

However, a Judge of the New Zealand High Court may order that this protection does not apply if, having regard to the issues to be determined in a civil or criminal proceeding, the public interest in the disclosure of the evidence of the informant's identity outweighs:

- any likely adverse effect of the disclosure on the informant or any other person, and
- the public interest in the communication of facts and opinion to the public by the news media and in the ability of the news media to access sources of facts.

A journalist is defined a person who, in the normal course of their work, may be given information by an informant in the expectation that the information may be published in a news medium. A news medium is defined as a medium for the dissemination of news or observations on news to the public or a section of the public.

The protection for journalists contained in section 126K of the *Evidence Act 1995* is broadly based upon this provision, as discussed above.

#### *Search and Surveillance Act 2012 (NZ)*

Section 6 of the Search and Surveillance Act provides that a search warrant may be issued if the Judge or issuing officer is satisfied that there are reasonable grounds to:

- suspect that an offence punishable by imprisonment has been, is being, or will be committed, and
- believe that the search will find evidential material in respect of the offence, in or on the warrant premises or vehicle.

In accordance with sections 142-147 of the Search and Surveillance Act, privileged materials may be seized under warrant, but not searched, pending subsequent adjudication by the New Zealand High Court over a claim of privilege. If a claim of privilege is upheld over the seized materials, these materials must be returned to the claimant. Various privileges are recognised for the purposes of these provisions, including the protection of confidentiality of journalists' sources. However, privileges do not apply in respect of communications or information if that communication or information was made, received, compiled or prepared:

- for a dishonest purpose, or
- to enable or aid any person to commit or plan to commit what the person claiming privilege knew, or ought reasonably to have known, to be an offence.

## **United Kingdom**

The United Kingdom Law Commission is currently reviewing the laws governing search warrants, with the aim of clarifying and rationalising the United Kingdom's search warrant laws.<sup>5</sup> At present, the Law Commission has described the current search warrant laws as outdated, overly complex and inconsistent, particularly in the application of safeguards aimed at protection certain material, such as privileged information. The United Kingdom has 176 search warrant provisions, excluding warrants to enter premises and warrants to enter and inspect premises.

Caution should be exercised in using the United Kingdom's laws as a benchmark or model upon which to base potential reforms to Australia's search warrant schemes until the outcomes of that review are known.

#### *Police and Criminal Evidence Act 1984 (PACE Act)*

Pursuant to section 8 of the PACE Act, on the basis of information provided by a police constable, a justice of the peace may issue a search warrant if satisfied that there are reasonable grounds for believing that:

- an indictable offence has been committed, and

<sup>5</sup> Further information on the United Kingdom Law Commission's search warrants review is available at: <https://www.lawcom.gov.uk/project/search-warrants/>. It is noted that the United Kingdom's search warrant laws apply in England and Wales.

- there are materials on the premises which are likely to be of substantial value to the investigation of the offences and likely to be relevant evidence, and
- one of a number of accessibility conditions is satisfied, establishing that it would not be practicable to gain entry to the premises or access to the materials without a search warrant.

However, some types of materials are protected against search and seizure under search warrant, including materials subject to legal professional privilege, medical records, confidential business records and journalistic materials. The United Kingdom distinguishes journalistic material as being:

- ‘special procedure material’ if the journalistic material is not confidential, or
- ‘excluded material’ if the journalistic material is confidential.

‘Special procedure material’ and ‘excluded material’ cannot be searched for under a search warrant issued under section 8 of the PACE Act and, if such materials are found during the course of a search, these materials cannot be seized under the warrant. In a limited set of circumstances, law enforcement may seek to obtain journalistic material under a production order.

#### *Obtaining special procedure material*

To obtain ‘special procedure material’, a Circuit or District Judge may issue a production order under Schedule 1 of the PACE Act, which requires the occupier of a premises to produce those materials to law enforcement or, if issuing a production order is not practicable, a warrant may be issued. An application for a production order under Schedule 1 of the PACE Act must be made *inter partes*, which would provide the journalist of media organisation in possession of the journalistic materials with an opportunity to contest the issuing of the production order.<sup>6</sup>

#### *Obtaining excluded material*

‘Excluded material’ cannot be obtained under a production order issued under Schedule 1 of the PACE Act, unless the material would have been available under legislation enacted prior to 1984, such as under the Official Secrets Act (as discussed below).

#### *Exceptions relating to arrest*

Confidential and non-confidential journalistic materials may also be searched for and seized under an entry and search undertaken after an arrest, or under a search conducted upon arrest.<sup>7</sup>

#### *Official Secrets Act 1911*

Pursuant to subsection 9(1) of the Official Secrets Act, a search warrant may be issued if there are reasonable grounds to suspect that an offence has been, or is about to be, committed under the Official Secrets Act. Despite the restrictions on obtaining ‘special procedure material’ and ‘excluded material’, Schedule 1 of the PACE Act provides that a search warrant may be issued to obtain these types of material if the search of a premises for such material could have been authorised under another law.<sup>8</sup> It is an offence against the Official Secrets Act to communicate documents or information that might be directly or indirectly useful to an enemy, if the person making the communication is acting for any purpose prejudicial to the interests or safety of the State.<sup>9</sup> As such, a search warrant may be used to obtain confidential and non-confidential journalistic material in circumstances whereby a Government official has provided national security information or classified material to a journalist or media organisation, if the Government official’s conduct constitutes an offence under the Official Secrets Act.

## **United States**

The First Amendment contained in the United States’ Bill of Rights prohibits Congress from enacting laws that prohibit freedom of speech and freedom of the press, although it is noted that these rights do not confer additional protections upon journalists and media organisations above the rights conferred upon

<sup>6</sup> Ibid 188 (see footnote 726).

<sup>7</sup> Above n 8, 32, 88 [2.53, [4.104]]; *Police and Criminal Evidence Act 1984* (UK) ss 18, 19, 20 and 32.

<sup>8</sup> *Police and Criminal Evidence Act 1984* (UK) sch 1 paras 3 and 12.

<sup>9</sup> *Official Secrets Act 2011* (UK) sub-s 1(1).

individuals.<sup>10</sup> Federally, the United States has enacted the *Privacy Protection Act* (42 USC) which provides that law enforcement agencies must seek a subpoena to obtain access to a journalist's documentary and work product materials, unless:

- there is probable cause to believe that the journalist has committed an offence other than an offence involving the receipt, possession, communication or withholding of material or information (unless that information or material relates to national defence, child exploitation, is classified, or is restricted data), or
- the information or material sought is necessary to prevent injury or death, or
- the journalist is likely to destroy the information or material if a subpoena was issued.<sup>11</sup>

By requiring a subpoena to be issued, apart from in the instances above, this provides journalists and media organisations with an opportunity to challenge the subpoena before material or information has been provided to law enforcement, as opposed to challenging the validity of a search warrant after law enforcement have already seized the material or information. Despite this protection, the United States has not enacted shield laws at a federal level to protect the confidentiality of journalistic sources. However, many states of the United States have introduced legislation or recognised common law protections that allow journalists to refuse to disclose confidential or unpublished information, including information about a source's identity.<sup>12</sup>

<sup>10</sup> Cornell Law School Legal Information Institute, 'First Amendment Freedom of Speech/Freedom of the Press' <[https://www.law.cornell.edu/wex/first\\_amendment](https://www.law.cornell.edu/wex/first_amendment)>.

<sup>11</sup> *Privacy Protection Act*, 42 USC § 2000aa.

<sup>12</sup> Jonathan Peters, 'Shield laws and journalist's privilege: The basics every reporter should know' (2016, Columbia Journalism Review) <[https://www.cjr.org/united\\_states\\_project/journalists\\_privilege\\_shield\\_law\\_primer.php](https://www.cjr.org/united_states_project/journalists_privilege_shield_law_primer.php)>.