SUBMISSION TO PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY INQUIRY INTO THE IMPACT OF THE EXERCISE OF LAW ENFORCEMENT AND INTELLIGENCE POWERS ON FREEDOM OF THE PRESS

31 JULY 2019

Australia's Right to Know coalition of media companies appreciates the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) inquiry into the impact of the exercise of law enforcement and intelligence powers on freedom of the media (the Inquiry).

As the Committee is aware, the catalyst for this Inquiry is the raids by the Australian Federal Police (AFP) on the home of journalist Annika Smethurst and the headquarters of the ABC in Sydney on June 4 and 5, 2019 regarding stories published and broadcast in April 2018 and July 2017 respectively. Recently it has also been publicly revealed that the AFP was planning – but did not execute – a raid on News Corp Australia's Sydney headquarters on June 6, 2019.

We also note that in a similar timeframe 2GB's Ben Fordham told listeners to his program that up to six boats could have been making the journey from Sri Lanka to Australia and that information had come from a senior source in Home Affairs. Shortly after revealing this on air his producer received a call from an official from the Department of Home Affairs, said an investigation would commence as a result of the information becoming public and asked Mr Fordham to assist in the investigation. He was also told the source of the information was the target, not Mr Fordham himself. This is illustrative of a pattern of behaviour that is not just limited to the AFP raids.

EXECUTIVE SUMMARY

The Terms of Reference should be broadly construed

While the AFP raids are the catalyst for the Inquiry, the media organisations represented by ARTK feel strongly that the portrayal of our long-held and serious concerns regarding the precarious state of the Australian public's right to know as being limited to law enforcement and national security matters does not sufficiently reflect the full extent of the issues faced by Australian media companies and the community. In our view, the terms of reference for this inquiry do not sufficiently cover the breadth and complexity of the issues we should be addressing in this forum.

The Joint Media Organisations represented by this submission believe the Terms of Reference for this Inquiry are insufficient to properly cover the full extent of the problems we are facing as a community. We are concerned that this will mean that this Inquiry will not be empowered to look at the full range of laws that impact on the media's ability to report on matters of public interest and the public's right to be informed of such matters. Some have suggested this may be deliberate and reflects an intention to control and limit the debate around these issues and the outcomes that can be delivered.

While we are aware that the Committee cannot set its own Terms of Reference, we would urge the Committee to take the broadest possible interpretation of the Terms of Reference to ensure that this Inquiry considers the full suite of laws impacting the Australian media's ability to report. The need for 'better balance' extends to the entire legislative and regulatory framework that intentionally and unintentionally inhibits the ability of the media to do its job on behalf of the public.

We note that the Terms of Reference also includes an 'any other matters' section. We urge the Committee to consider the broader scope of issues raised in this submission as part of these considerations, thus enabling a broad view to be taken to the matter of media freedom and the public's right to know.

A Free Media is of utmost public importance

Various Government Ministers have claimed in the wake of the recent AFP raids that there is full support for the operation of a free media. Disappointingly, others have suggested that the mere fact that a journalist may be in possession of leaked documents should be sufficient for them to be considered to have committed a criminal offence. This amounts to suggesting that a necessary element in the reporting of matters of public interest is the receipt of information which is not publicly known is sufficient to support a finding of criminal activity on the part of a journalist who is doing nothing other than their job. This it seems to us is the nub of the problem this Inquiry should have as its main focus. How can we ensure that the public's right to be informed of the actions taken by Government in their name is sufficiently protected? There is no reference in any legislation to the importance of the right to know and there are no safeguards in place to force legislators to build protections into legislation.

It is dismissive to describe this situation as merely one that is causing journalists "anxiety". This ignores the very real threat posed to democracy through inaction or bureaucratic and political intervention. It is unlikely any Australian going about their job would not be anxious if they found themselves subject to potential AFP raids, criminal charges and jail time because they communicated something to other members of the public that would be in their best interest to know, even if the Government may not want that information disclosed.

The rising tide of secrecy

In recent years, many legal provisions that undermine and threaten the Australian public's right to know have been passed by the Federal Parliament under the guise of various national security concerns and national security legislation.

The culture of secrecy arising from these legal provisions that unnecessarily restrict Australia's right to know has permeated attitudes and processes more broadly. We have tackled some of these issues on a legislative amendment by legislative amendment basis. But with each of these laws the tide of secrecy rises. This is deeply disturbing in a modern and robust democracy.

The tool that is used – laws that are designed to put journalists in jail for doing their jobs – has a chilling effect on reporting. It is not far-fetched to conclude the impact of the AFP raids, and the approach the Government has taken to the fate of the journalists that are the subject of those search warrants, is intimidatory.

The stories at risk of not being told, of us all not being informed about, rarely involve matters of national security. The stories at risk of not being told, of us all not being informed about, are about the things that affect

ordinary Australians every day like the quality of aged care and how our tax dollars are being spent. Think kerosene baths and pink batts.

As is clear from this submission and the many other submissions we have made to Federal, state and territory jurisdictions over the past decade and even earlier, laws that place restrictions on what the public cannot know are not limited to national security and counter-terrorism. There are a multitude of laws that need attention due to their intended and unintended restrictions that impact the Australian public's right to know.

It is a fact that there is a significant number of existing laws that require reform. The challenge for this Committee is to tackle what is undoubtedly a wide ranging and complex undertaking to ensure that actions live up to the rhetoric around supporting a free media.

The myth of 'balancing' media freedom and national security

The right to free speech, a free media and access to information – in service of the public's right to know – are fundamental to Australia's modern democratic society: a society that prides itself on openness, responsibility and accountability.

However, unlike some comparable modern democracies, Australia has no national laws enshrining these rights. In the US the right to freedom of communication and freedom of the press are enshrined in the First and Fourth Amendments of the Constitution and enacted by state and federal laws. In the United Kingdom, freedom of expression is protected under section 12 of the *Human Rights Act 1998* subject to appropriate restrictions to protect other rights that are considered necessary in a democratic society.

The absence of such an explicit right in Australia means that every law that restricts the public's right to know challenges the fundamental principles that are the foundation of a modern, liberal democratic society.

ARTK proposal for law reform – putting the balance in balancing-act

Law reform is necessary and urgent. The combined effect of more than a decade of laws that individually create a proliferation of ways in which journalists can be exposed to the threat of criminal charges for simply reporting uncomfortable or unpleasant realities is now a matter of serious national concern. For the most part, these laws have very little to do with national security and everything to do with the exercise of power and the desire to avoid scrutiny. We have proposed legislative reforms that directly address the main issues. This is not a menu or a wish list. These are reforms that can and should be implemented immediately and that will go some way to providing the 'better balance' that the public demands.

As it stands, the current so-called balancing act between the public's right to know and the objective of controlling Government information is not a balance at all.

The objective of our law reform proposal is to bring the public's right to know up-front, as an active consideration – the balance in the balancing act – at the beginning of the process.

Conclusion

ARTK has serious reservations about whether this Inquiry is the right way to achieve the outcomes we believe are necessary to redress the combined impact of more than a decade of law making in the name of national security. We urge the Committee to take a broad view of these issues and to take into account that a trust relationship between the media and Government is also a necessary element in protecting our nation's interests.

The Media Organisations represented by this submission are prepared to engage fully with this Inquiry in good faith. We ask only that the Committee approaches this exercise with the same commitment.

Quick and decisive action is warranted. We urge the Committee to respond thoughtfully to the issues raised and provide a concerted response to the issue of media freedom in Australia.

Our proposal for law reform is to introduce

- The right to contest the application for warrants for journalists and media organisations;
- Public sector whistle-blowers must be adequately protected – the current law needs to change;
- A new regime that limits which documents can be stamped secret;
- A properly functioning freedom of information (FOI) regime;
- Exemptions for journalists from laws that would put them in jail for doing their jobs, including security laws enacted over the last seven years; and
- Defamation law reform.

Details of those reforms follow.

1. THE RIGHT TO CONTEST THE APPLICATION FOR WARRANTS FOR JOURNALISTS AND MEDIA ORGANISATIONS

- Applications for the issue of all warrants and compulsory document production powers[1] associated with journalists and media organisations undertaking their professional roles must be contestable. This requires:
  - Applications for all warrants must be made to an independent third party with experience in weighing evidence at the level of a judge of the Supreme Court, Federal Court or High Court. The best outcome is for this to occur in open court in the Supreme Court, Federal Court or High Court.
  - The journalist/media organisation being notified of the application for a warrant
  - The journalist/media organisation being represented at a hearing, presenting the case for the Australian public's right to know including the intrinsic value in confidentiality of journalists' sources and media freedom
  - The independent third party deciding whether to authorise the issuing of a warrant – or not – having considered the positions put by both parties
  - That a warrant can only be authorised if it is necessary for its stated statutory purpose and the material sought cannot be obtained via other means
  - That a warrant can only be authorised if the public interest in accessing the metadata and/or content of a journalist's communication outweighs the public interest in NOT granting access, including, without limitation, the public interest in the public's right to know, the protection of sources including public sector whistle-blowers and media freedom
  - That there be a presumption against allowing access to confidential source material
- The journalist/media organisation has a reasonable period after the warrant is authorised to seek legal recourse including injunctions and judicial review
- A transparency and reporting regime for application of and decisions regarding issuing and authorisation of warrants.

Some may say that a contestable regime for warrants would take the element of 'surprise' out of the equation, and as a result evidence would be destroyed. This is not insurmountable. We recommend that legislative provisions be drafted that prohibits anyone destroying evidence upon receipt of the notification of the application for a warrant. Such an offence would be over and above the fact that once notified of a warrant application, anyone who went about destroying documents would likely be in contempt of court.

We note the Terms of Reference[2] for the Inquiry include the appropriateness of current thresholds for law enforcement and intelligence agencies to access electronic data on devices used by journalists and media organisations.

We also note the Committee is separately undertaking a review of the mandatory data retention regime[3]. This is a requirement under section 187N of the *Telecommunications Interception and Access Act 1979* (the TIA Act).
It is this Act, and the mandatory data retention regime, that contains the Journalist Information Warrant Scheme (JIW Scheme) to which the above term of reference for the Inquiry directly relates.

ARTK made a submission to the Committee's review of the mandatory data regime in earlier in July. That submission has been published (submission 14) and is attached at **Attachment A** to this submission.

[1] For example, section 3ZQO of the *Crimes Act 1914* (Cth) empowers the AFP to apply to a Federal Circuit Court judge for a notice requiring the production of travel information, among other documents. This covers a journalist's flight information.
[2] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/FreedomofthePress/Terms_of_Reference
[3] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime

2. PUBLIC SECTOR WHISTLE-BLOWERS MUST BE ADEQUATELY PROTECTED – THE CURRENT LAW NEEDS TO CHANGE

Public Interest Disclosures

The *Public Interest Disclosure Act* purports to provide protections for public sector whistle-blowers. It falls a long way short of this. Changes required include:

- 'Protections' in all cases require review, public service whistle-blowing should be encouraged and adequate protections must be provided including protections for external public disclosure
- Protection for intelligence agency personnel and staff of Members of Parliament
- Expand the public interest test to remove bias against external disclosure
- Presumption of criminal liability should not lie against the media for using or disclosing identifying information during the course of news gathering
- The ability for identifying sources via journalists' communications and metadata (Journalist Information Warrant Scheme) makes a mockery of the shield law that protects the identity of journalists' sources once proceedings have commenced (ARTK submission to be made to PJCIS)

We note comments by Attorney-General Christian Porter regarding an intention to review the so-called public-sector whistle-blower protections in the *Public Interest Disclosure Act* (Cth) on the basis of a recent judgment by Federal Court Justice John Griffiths. In that judgment[4], Justice Griffiths described the Commonwealth whistle-blower laws as 'technical, obtuse and intractable.'[5]

Justice Griffiths goes on to opine why this may be the case. However, he concludes that it is law-makers – the Parliament – who should address the current state of affairs. Specifically, Justice Griffiths says: *'It is acknowledged that reconciling these competing objects is not an easy exercise and is one for the Parliament. But the outcome is a statute which is largely impenetrable, not only for a lawyer, but even more so for an ordinary member of the public or a person employed in the Commonwealth bureaucracy'.*[6]

We welcome the Attorney-General's commitment to overhauling the relevant Commonwealth law that purports to provide protections for public sector whistle-blowers.[7]

We also note the Report of the Review of the PID Act (the Moss Review Report)[8] and the importance it places on the objectives of the PID Act. Most significantly we note that the Moss Review Report's recommendations as intended to '*encourage and instil a pro-disclosure culture'*.[9]

This reflects a keystone of our concerns and demonstrates why all elements of our law reform proposal should be considered in aggregate – to reverse the secrecy culture and ensure the public's right to know is an active first order consideration.

The value of corporate whistle-blowing and reporting corporate missteps, wrong-doings and corruption has never been more valued in Australian society than it is now. There are increased protections for corporate whistle-blowers and improved grievance processes as a result. In contrast, however, public sector whistle-blower laws are deficient and require updating.

---

[4] https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2019/2019fca0548
[5] Ibid. at [17]
[6] Ibid, at [18]
[7] https://www.theaustralian.com.au/business/legal-affairs/porter-flags-plan-to-protect-sources-behind-public-service-leaks/news-story/ebf86d51ecd912dedd8628e6a0382e02
[8] https://www.pmc.gov.au/sites/default/files/publications/pid-act-2013-review-report.pdf
[9] Ibid, at [180]

We look forward to understanding the time frame for the open and accountable review and overhaul of the Commonwealth's whistle-blower laws to deliver the aim of encouraging and instilling a pro-disclosure culture.

Proposed Commonwealth Integrity Commission

Robust regulatory and law enforcement frameworks to deal with corrupt and criminal behaviour should be complemented by news reporting which shines a light on conduct of this nature. Hearings on public sector corruption should be public so that media companies can report on them.

The framework for the proposed Commonwealth Integrity Commission (CIC) should safeguard public broadcasters' role as a provider of public interest journalism. It should ensure confidential sources continue to have confidence to bring allegations of corruption in public service agencies to the attention of public service broadcasters' journalists, without fearing that their documents and/or identity will be revealed, and without public broadcasters' journalists being at risk of being called before a hearing to reveal their sources. Hearings on public sector corruption should be public so that media companies can report on them and the public can have confidence in them.

The CIC scheme could have a chilling effect on journalism if it:

- required public broadcasters to provide information and documents obtained in the course of journalism that are not about the public broadcaster itself, but that relate to allegations of corruption at another agency;
- allowed the CIC to inspect and seize documents without a court order; and/or
- penalised journalists/public broadcasters for failing to provide information which may reveal confidential sources.

Legislation establishing a CIC should, among other things:

- clarify that the scheme applies only to the agency being investigated and not require the heads of the public broadcasters to provide material obtained in the course of journalism to the relevant commissioner;
- if information or documents are required to be provided, require a court order before that material is seized or requested by the CIC, and provide clear grounds for public broadcasters to challenge such orders to protect sources;
- acknowledge the ethical obligations on journalists to protect confidential sources; and
- adopt a broad definition of journalism.

Lastly, but importantly, we note the importance of the application of the Commonwealth shield law regarding the operation of the Commonwealth Integrity Commission. Specifically, the *Evidence Act 1995* (sections 126G and 126H) must apply to the activities of the CIC so that journalists cannot be compelled to answer any question or produce any document that would disclose the identity or enable that identity of a confidential source to be ascertained.

Public broadcasters have made detailed submissions to Government setting out specific proposals relating to these amendments. Through the consultation process, both the ABC and SBS have raised concerns about the proposed legislation and its potential to cause unintended consequences by impinging public interest journalism.

3. A NEW REGIME THAT LIMITS WHICH DOCUMENTS CAN BE STAMPED SECRET

Legal experts such as Bret Walker SC, who previously held the Commonwealth role of Independent National Security Legislation Monitor (INSLM), have recommended 'new overarching legislation that defines in a restrictive fashion what information must be kept secret'.

Conversely, and importantly, that will also define what information will not be kept secret.

We support this. Any new framework must include a public transparency requirement via auditing and reporting requirements. Auditing and reporting should consist of two elements: regularly scheduled audits (for example annual) and random audits.

All audits must include a public report, to be published publicly within (say) 30 days of the completion of the audit. The necessity for timely reporting as a transparency and accountability measure cannot be undervalued. This would also ensure this reporting does not replicate the unnecessary delays of reporting currently evidenced under the TIA Act.

4. A PROPERLY FUNCTIONING FREEDOM OF INFORMATION REGIME

The Government can also shut down reporting through the FOI process. FOI laws require meaningful attention and improvement in all aspects. A review of FOI laws must include a panel of FOI 'user' experts and this must include specialist journalist representatives.

The last attention given to the Commonwealth FOI process was the Hawke Review in 2012. We made a detailed submission to that review.[10] The issues we raised in 2012 remain in 2019 including, but not limited to:

- Journalists continue to encounter barriers to accessing information including systemic delays in processing, failures of agencies to assist with applications and poor decision making;
- Review processes are inadequate and alternative means of review at an early stage must be available (for example, Administrative Appeals Tribunal);
- Exemptions should not be expanded or 'reformulated' (eg, the provision of frank and fearless advice);
- The cost of applications is often a disincentive to seek information; and
- Processing time assessments and limits are tools to defeat FOI applications.

The 2013 Final Report of the Hawke Review[11] recommended that a comprehensive review of the FOI Act be undertaken[12]. This has not occurred.

Further, we made a submission to the Senate Legal and Constitutional Affairs Committee regarding the *Freedom of Information Amendment (New Arrangements) Bill 2014.*

We raised then that the Government was yet to provide a response to the Hawke Report into Commonwealth FOI laws. We also noted that while we did not support many recommendations from the Hawke Report, we strongly supported the proposal for a comprehensive review of the FOI Act and its operations. We also recommended such a review should be conducted by a broadly-based expert panel, including media representatives, and should be announced in early 2015. We suggested that the Senate Legal and Constitutional Affairs Committee support this recommendation as there were, and continue to be, a number of problems with the current FOI regime. For example:

- In some instances, there were regularly delays past the 30 day timeframe for decision making on requests from media organisations, making it difficult for the media to use FOI to report on government in a timely fashion;
- Some agencies often advised journalists that an FOI request has been refused in accordance with section 24AA because the work would involve a substantial and unreasonable diversion of agency resources. Agencies should be properly resources to respond to FOI requests. This aspect of the FOI Act needs urgent reform as agencies appear to be failing to consider the importance of the public

[10] https://www.ag.gov.au/Consultations/Pages/ReviewofFOIlaws.aspx
[11] https://www.ag.gov.au/Consultations/Documents/ReviewofFOIlaws/FOI%20report.pdf
[12] Ibid. Recommendation 1, p4

interest and the real value to efficient government from early exposure of policy and program failures through FOI compared to the administrative cost of processing requests; and
- The use of disclosure logs is a significant deterrent to media organisations investing in FOI investigations, to the detriment of an informed public and open and transparent government.

As we said above, these issues remain today as they did in 2014 and in 2012.

We urge the Government to undertake a comprehensive review of the FOI Act as a matter of urgency.

We also recommend transparency measures – including auditing and reporting – are elements of a reviewed Commonwealth FOI regime.

5. JOURNALISTS MUST BE EXEMPTED FROM NATIONAL SECURITY LAWS ENACTED OVER THE LAST SEVEN YEARS THAT WOULD PUT THEM IN JAIL FOR DOING THEIR JOBS

We have provided detailed analysis to the PJCIS on previous occasions regarding the following, including that exemptions for public interest reporting are essential for:
- Section 35P of the *ASIO Act*;
- Journalist Information Warrant Scheme at Division 4C of the *Telecommunications Interception and Access Act*;
- *Criminal Code Act, Part 5.2 – Espionage and related offences; Part 5.6 – Secrecy of information,* section 119.7 – Foreign incursions and recruitment; section 80.2C – Advocating terrorism; and
- *Crimes Act* – sections 15HK (controlled operations, unauthorised disclosure of information) and section 3ZZHA (delayed notification search warrants, unauthorised disclosure of information).

ARTK has made submissions to PJCIS inquiries regarding these provisions when they were introduced as enacting legislation. In each submission we recommended an exemption apply to public interest news reporting.

- **Section 35P of the *ASIO Act*** was enacted by the *National Security Amendment Bill (No.1) 2014*. ARTK made a submission to the PJCIS inquiry into that Bill. It should also be noted we made submissions and gave evidence to the INSLM review of section 35P of the *ASIO Act*.

  In our submission of 6 August 2014 we clearly articulated that we do not seek to undermine Australia's national security, nor the safety of the men and women involved in intelligence and national security operations.

  Further, over many years there has been useful dialogue between security officials and producers and editors of media organisations that has led to considered outcomes. Journalists and editors have demonstrated over time that such matters can be approached in a reasoned and responsible manner. We hold that this approach should continue to be preferred over attempts to codify news reporting and criminalise journalists for doing their jobs.

  While section 35P was amended following review by the INSLM, we remain dissatisfied with the provision and the way in which it undermines reporting. This is particularly so when Special Intelligence Operations (SIOs) by their very nature will be undisclosed. This uncertainty will expose journalists to an unacceptable level of risk and consequentially have a chilling effect on the reportage of all intelligence and national security material. A journalist or editor will simply have no way of knowing whether the matter they are reporting may or may not be related to an SIO. We express this as information that 'may or may not be' related to an SIO because:

  - It may or may not be known if the information is related to intelligence operations, and whether or not that intelligence operation is an SIO;

- *'relates to'* is not defined and therefore the breadth of relevance is unknowable;
- It is unclear whether SIO status can be conferred on an operation retrospectively – i.e. if information has been 'disclosed,' whether any operation that it may be associated with or related to can be retrospectively allocated SIO status; and
- It is likely that clarity about any of these aspects would only come to light after information is disclosed – particularly in the case of reporting in the public interest.

To illustrate, the discloser may not be aware that the information relates to an SIO, nor whether the information is core/key/central to an SIO, and even less aware as to where the boundaries may lie for information that may or may not 'relate to' an SIO.

So the discloser – who may be a journalist, doing what they are legitimately entitled to do as part of their job – could be jailed for disclosing information that is related to an SIO, even if they were not aware of it at the time, or it was not an SIO at the time of the report.

This uncertainty is intensified as the proposed criminal offence is based on the disclosure of information that relates to an SIO – regardless of to whom the disclosure was made. For example, a journalist who checks with his/her editor or producer regarding the information and/or the story could be jailed for responsibly doing their job, even if the information is not ultimately broadcast or published.

To illustrate this further, if the producer or editor disclosed the information to anyone in the course of making an editorial decision, then the source, the journalist and the editor could all be jailed. The conversations that are currently able to be had as media outlets make responsible decisions about disclosure in the public interest, would be denied under the legislation, because any disclosure by anyone – to anyone – would be a criminal offence.

It is also observed that it is the intelligence agency that determines an intelligence operation as an SIO, and would also determine the 'related' nature of the information to the SIO.

We reflect also on the Forward of the Committee's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*[13]particularly the references to the Boston bombings and the murder of a British Soldier on the streets of London. These incidents are indeed concerning. If these incidents, or incidents such as these, were or became the subject to an SIO, then under the proposed amendments, journalists may be unable to report – including on incidents that may have been witnessed by a small or large number of members of the public, for fear of being charged with a criminal offence.

We also notes that section 35P to the ASIO Act also entrenches the currently inadequate protections for whistle-blowers regarding intelligence information. As a foundation of freedom of communication, we draw attention to this matter and highlight that it further erodes freedom of speech and freedom of the media in Australia. Specifically, proposed section 35P makes it a criminal offence punishable by jail, for anyone, including a whistle-blower, to disclose information that relates to an SIO.

We made further submissions to the INSLM review of 35P. We include here two (2) scenarios that were put forward then to illustrate how section 35P may be engaged.

Scenario 1 – Melbourne terror raids – scenario based on actual events

13 http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm at *vii*

In the days following anti-terror raids conducted throughout Melbourne in September 2012, a report was published in *The Australian*[14] (see **Attachment B**) which described the immediate impetus for the raids – an ASIO informer embedded within a group with terrorist links left his mobile phone behind and his messages with his ASIO contact were discovered by the group and published by them.

It is conceivable that this operation would have been conducted as an SIO were it taking place today, for example if the ASIO informer were in fact an ASIO agent and required authorisation under the auspices of an SIO for his contact with the terrorist group. If that were the case:

a) The reporter involved might suspect that the operation was an SIO. At that point, the reporter faces the decision whether to proceed with investigating a story, the publication of which may prove to be illegal;
b) In any event, the reporter has no way of knowing with certainty whether the operation was an SIO since no source would be likely to provide such information given they would be breaching the law by disclosing its existence;
c) It is likely in those circumstances that the reporter would at best receive a 'cannot confirm or deny' response from official sources without the means to make further inquiries or to know whether the SIO was ongoing;
d) The reporter, editor and ultimately the publisher are left with a choice either to self-censor and drop the story or run the risk of breaching section 35P(1) or (2) if they publish.

<u>Scenario 2 – Hypothetical scenario</u>

A situation could conceivably arise whereby two ASIO agents are involved in the covert penetration of a suspected terror cell of young men with histories of drug trafficking, but who have recently been seduced by ISIS and who are believed to be considering a terrorist attack.

Both ASIO agents effectively work undercover in trying to win the trust of the group to learn of their plans. It is likely in these circumstances that the operation may be authorised as an SIO.

In the course of their work, one of the ASIO agents realises that his partner is becoming too close to the group, and suspects that he is actually involved in the unauthorised trafficking of drugs, lining his own pocket outside the terms of the SIO. He suspects his partner is playing down the terror threat that this group poses in order to protect his own racket. In frustration the 'good' ASIO agent goes to his superiors but they ignore him, as does the Inspector General of Intelligence and Security, telling him that his partner is authorised to dabble in drugs with the group in order to win their trust and that there is no evidence that he has gone to the 'dark side'.

The ASIO agent believes that his partner has gone rogue and wants to expose it. He provides information to a journalist who prepares a major report on the rogue ASIO agent. The journalist approaches the Government for comment, but the spokesperson asserts only that it would be illegal to publish any such story. The journalist has a reasonable basis to believe the operation has been conducted as an SIO, and therefore would be subject, together with the editorial chain, to five (5) or 10 years jail if the story were published.

In those circumstances, it can be assumed that the story is never written. The ASIO agent goes unpunished for two years until he is finally caught by ASIO's internal investigators and his employment quietly terminated. No-one knows anything publicly and they never will. And dangerous or illegal activity engaged in by the ASIO agent whilst trafficking on his own account, including activity that might pose a serious threat to Australia's national security interests, would remain permanently secret.

[14] http://www.theaustralian.com.au/news/nation/how-informers-fears-triggered-terror-raids/story-e6frg6nf-1226474501095

The lack of public scrutiny effectively means that ASIO and the Government are unlikely to be under any pressure to take firm measures to ensure that similar events do not occur again.

- **Journalist Information Warrant Scheme** at Division 4C of the *Telecommunications Interception and Access Act* was enacted by in the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (mandatory data retention regime) and the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* and consequent regulations. ARTK made a submission to the PJCIS inquiry into this matter and engaged with the then Attorney-General , the Minister for Communications, the Shadow Attorney-General , the Shadow Minister for Communications and the Attorney-General's Department over the course of this legislative/regulatory process.

  See Attachment A for ARTK's 4 July 2019 submission to the PJCIS regarding the Scheme.

- ***Criminal Code Act, Part 5.2 – Espionage and related offences; Part 5.6 – Secrecy of information*** were introduced in the *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (the Bill). ARTK made several submissions to the PJCIS inquiry into that Bill.

- **Section 119.7 of the *Criminal Code Act*** (foreign incursions and recruitment) was enacted by the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*. ARTK made a submission to the PJCIS inquiry into that Bill.

  In our submission of 3 October 2014, we explained that Proposed section 119.7 deals with the recruitment of persons to serve in or with an armed force in a foreign country; and proposed subsections 119.7(2) and 119.7(3) address *'publishing recruitment advertisements'*[15] which include news items that may relate to such matters.

  <u>Lack of clarity about the 'news items' that are the source of recruitment or information about serving in or with an armed force in a foreign country</u>

  There is a lack of clarity regarding 'what' it is – particularly at 119.7(3), and particularly as it relates to a news item – that is being targeted.

  <u>Lack of clarity regarding who the offence is targeting</u>

  There is also lack of clarity regarding 'who' the person is, or who is the target of the offence, that is committing the crime by 'publishing' the advertisement or news item.

  It could be envisaged that 119.7(2) and 119.7(3) may apply to – and not be limited to – the following separately, or a combination of any or all:
  - Persons associated with a media company's advertising arm or agency, including people responsible for advertisement bookings; and/or
  - Persons associated with a media company's newsroom or production; and/or
  - A director of a company; and/or
  - Editors, producers, journalists; and/or
  - Other persons that may be a party to any of the publishing/broadcast functions associated with (i) and (ii) of 119.7(2) and 119.7(3) and the above.

  <u>Serious risk to innocent publication of advertisements and news items</u>

[15] http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s976_first-senate/toc_pdf/1420720.pdf;fileType=application%2Fpdf, p91

We have grave concerns regarding 119.7(3) and the implications for publication of legitimate advertisements and news.

This is particularly the case when the advertisements or news items may, on face value, be benign and indeed legitimate, and also lack 'reckless' conduct in their publishing.

Further, the relevant information (such as location or travel information) or purpose (such as recruitment) of such advertisements or news items may only be known after the fact – and possibly still not known by the advertiser, or the person taking the ad booking, or the journalist or the editor. That is, it may only be known some time afterwards that the purpose of, or information contained in the ad or news item, or the location or place indicated in the ad or news item, or the travel information in an ad or news item, was instructive about or related to, serving in any capacity in or with an armed force in a foreign country.

To illustrate, if a broadcaster or publisher was to run an advertisement or a news item about a prayer meeting or a picnic, and it comes to pass that the event – which may or may not have been central to the advertisement or story – was used as cover for a recruitment drive or to disseminate information about, or direct people to another source of information about possible opportunities to serve in armed forces in foreign countries, then it is possible that any or all people involved in broadcasting or publishing the advertisement or story would be imprisoned for 10 years. This would be the case even if the conduct was not 'reckless.'

Such measures will almost certainly impact on the free flow of information in society – especially when the parties to the advertisements and news items are acting in good faith and communicating in the public interest. The serious implications of such a broad provision for news gathering and reporting, and also for legitimate business interests, cannot be overstated.

We note our concerns with subsection (3), which does not require the conduct to be *'reckless'* are heightened when there is no defence available to 'publishing recruitment advertisements' at subsections (2) and (3).

<u>Low threshold of subsection 119.7(2)</u>

We are concerned with the low threshold of subsection 119.7(2), in that it would only need to be proved that a person – including but not limited to a director of a company, an editor, a journalist, a person responsible for advertisement bookings, a combination of any or all of these people, and possibly additional persons that may be a party to an advertisement or a news item; where 'consideration' was provided – was 'reckless' as to the purpose of the advertisement or news item (that being to recruit persons to serve in any capacity in or with an armed force in a foreign country).

<u>The breadth of 'procured by' and 'or any other consideration' infringes on legitimate news gathering</u>

Both 119.7(2)(a)(ii) and 119.7(3)(a)(ii) stipulate that an element of the offence is that the person publishes in Australia *'an item of news that was procured by the provision or promise of money or any other consideration.'*

It is unclear from whom the promise of money or any other consideration needs to come from. For example, a news item that is licensed or purchased by a media organisation from a news agency and subsequently broadcast could be captured by this provision.

'Any other consideration' could be satisfied by buying a source, confidential or otherwise, a cup of coffee, or paying a taxi fare or train ticket – all of which are legitimate aspects of news gathering.

Also, and similar to comments made above, it is unclear what behaviour this qualification is targeting.

In the absence of clarity, combined with the breadth of the element and the fact that it would apply to legitimate news gathering, in our view the proposed element overreaches and infringes on legitimate news gathering processes.

- **Section 80.2C of the *Criminal Code Act*** (advocating terrorism) was enacted by the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*. ARTK made a submission to the PJCIS inquiry into that Bill.

  In our submission of 3 October 2014 we highlighted the issues that arise from the term 'advocates' as defined as 'counsels, promotes, encourages or urges'. Further, the element of 'recklessness' and the ambiguity with the definition of 'advocates' has the potential to limit discussion, debate and exploration of terrorism in news and current affairs reporting

  As ARTK-member MEAA noted in its submission: 'The definition of "advocacy" could now be used to constrain free speech. For journalists, it could also capture reporting of legitimate news stories that reported on banned advocacy…" That is the very offence that Australian journalist Peter Greste was charged with when tried and imprisoned by Egyptian authorities.

  In today's news terms, if a journalist interviews the Australian widow of an ISIS fighter in a Syrian refugee camp, and what that person says is reported which may include something like 'the Caliphate is not over', the journalist could be guilty of the offence and charged. Similar examples could include an Australian soldier fighting with Kurdish forces.

  Also, 'under the new offence of "advocating" terrorism, journalists could also be caught for counselling, promoting, encouraging or urging a whistle-blower to leak a document. Indeed, the provision is drawn so widely, that urging leaking of documents in general terms may fall within this clause,' the submission concluded.

  The submission went on to note that: '"promotion" would criminalise generally accepted definitions of freedom of expression. And because the "terrorism" definition extends to actions against foreign governments, it would capture advocates of even legitimate actions against foreign oppressive regimes. This offence could also capture journalists reporting on foreign powers using documents that have been leaked to them.'

- **Section 3ZZHA of the *Crimes Act*** (delayed notification search warrants, unauthorised disclosure of information) was enacted by the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*. ARTK made a submission to the PJCIS inquiry into that Bill; and
- **Sections 15HK of the *Crimes Act*** (controlled operations, unauthorised disclosure of information) formed the basis[16] for section 3ZZHA of the *Crimes Act*.

  In our submission of 3 October 2014, we said the insertion of section 3ZZHA to the *Crimes Act 1914* (the Crimes Act) would see journalists jailed for undertaking and discharging their legitimate role in our modern democratic society – reporting in the public interest. Such an approach is untenable. We recommend that this provision not be included in the legislation.

[16] The Explanatory memorandum of the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* states the (then) proposed section 3HHZA of the Crimes Act '*mirrors a similar offence for disclosing information relating to the controlled operation (section 15HK of the Crimes Act)'*

If, however, the Government is not minded to remove the provision, we request that a public interest exception be included at proposed section 3ZZHA(2).

Given that the Explanatory Memorandum of the Bill states that this '*mirrors a similar offence for disclosing information relating to the controlled operation (section 15HK of the Crimes Act)'*[17] we request that Bill be amended to incorporate a similar change to section 15HK of the *Crimes Act 1914*.

– **Conclusion**

These provisions are the tip of the iceberg regarding criminalising public interest reporting.

In addition to laws which criminalise journalists for doing their jobs, the Parliament has also recently passed the *Counter-Terrorism (Temporary Exclusion Orders) Bill 2019* which gives the relevant Minister the power to prevent a person aged 14 years or over from coming back to Australia for up to two years at a time on a number of grounds, including that the person has been assessed by ASIO to be 'directly or indirectly a risk to security for reasons related to politically motivated violence'.[18] We are extremely concerned that the scope of this provision as drafted may capture journalists or whistle-blowers who publish information about misconduct or national security matters, allowing the Minister to issue an order preventing those individuals from entering Australia. Laws such as these further contribute to deterring journalists from reporting on matters in the public interest, and whistle-blowers from coming forward.

As Professor George Williams AO has written on many occasions (see **Attachment C**)[19], there have been more than 75 laws passed since 11 September 2001 for national security and counter-terrorism purposes. Professor Williams recently said that *'this far exceeds the number of similar laws passed by Britain and the US. Our laws also differ because they go further in heightening government secrecy. They represent an assault on freedom of the press unique to Australia.'*[20]

ARTK has expressed our support for the Government's focus on safety for the Australian public in relation to these threats. However, what we do not agree with are the restrictions many of these laws, separately and in aggregate, put on informing Australians about matters of public interest.

Note – the legislative provisions relating to the above (excluding the JIW Scheme) are at **Attachment D.**

6. DEFAMATION LAW REFORM

We are actively involved in the current Council of Attorney's General review of the unified defamation law.

We note that the ARTK has made a submission[21] to the COAG Discussion Paper regarding the review of the model defamation provisions. We have also made a supplementary submission[22] to the Discussion Paper. Lastly, we have also expressed our significant concerns regarding the recent decision in the NSW Supreme

[17] http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/s976_ems_d5aff32a-9c65-43b1-a13e-8ffd4c023831/upload_pdf/79502em.pdf;fileType=application%2Fpdf at [643]
[18] Clause 10(2)(b)
[19] For example, 10 June 2019, *Australia is a world-beater in the secrecy Olympics*, *The Australian* (in full at Attachment B)
[20] Ibid
[21] https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/defamation-submission-aust-right-to-know.pdf
[22] https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/defamation-submission-aust-right-to-know-supplementary.pdf

Court[23] found that media companies are liable in defamation matters as publishers of comments posted on their Facebook pages by third party users.

In summary, we are seeking the following:

- Update the law to be fit-for-purpose for digital news reporting;
- Fix the aspects of the law which do not operate as intended; and
- Ensure the Commonwealth is a signatory to the Intergovernmental Agreement (and consequential amendments to the *Federal Court Act*) so that defamation law and procedure is aligned across all jurisdictions, including in the Federal Court.

Given there is an existing process for review of these laws we will refrain from unnecessarily taking the Committee's time on this issue.

However, we will take the opportunity to focus on the issues arising in the Discussion Paper regarding the jurisdiction and issues in the Federal Court, particularly the roles of juries.

Question 8 of the COAG Discussion Paper asks: *Should the Federal Court of Australia Act 1976 (Cth) be amended to provide for jury trials in the Federal Court in defamation actions unless that court dispenses with a jury for the reasons set out in clause 21(3) of the Model Defamation Provisions – depending on the answer to question 7 – on an application by the opposing party or on its own motion?*

In response ARTK has put the following:

ARTK has serious concerns about jurisdictional inconsistency of the provisions and procedures regarding juries in defamation cases.

As the Discussion Paper states, juries continue to have no role in any ACT, South Australia or Northern Territory defamation cases. There is also a presumption that juries will not play a role in defamation cases heard in the Federal Court.

While both of these scenarios are concerning, the inconsistency is most glaring between the Federal Court and the Model Defamation Provisions (MDP).

As the Discussion Paper details, in *Wing v Fairfax Media Publications Pty Limited* the Full Federal Court held that since there is direct inconsistency between sections 39 and 40 of the *Federal Court of Australia Act 1979* (Cth) (which provide for a presumption that civil trials are to be by a judge without a jury) and sections 21 and 22 of the MDP (under which any party in defamation proceedings may elect for the proceedings to be tried by a jury), the NSW provisions cannot be binding on the Federal Court by reason of that inconsistency and are not relevant to the exercise of the discretion in section 40 to order a jury.

This situation leads to forum shopping, as can be seen from the number of recent high profile cases being commenced in the Federal Court, presumably to avoid a jury on the basis that plaintiffs perceive their prospects of success as being greater before a judge sitting alone.

ARTK considers that juries are best placed to act as the "ordinary reasonable reader" in defamation cases and to apply community standards appropriately and conscientiously.

Accordingly, ARTK recommends that:

- The Federal Government must become a signatory to the Intergovernmental Agreement for the MDP; and

[23] Voller v Nationwide News Pty Ltd; Voller v Fairfax Media Publications Pty Ltd; Voller v Australian News Channel Pty Ltd [2019] NSWSC 766, at https://www.caselaw.nsw.gov.au/decision/5d0c5f4be4b08c5b85d8a60d

- The Federal Government must amend the *Federal Court of Australia Act 1976* (Cth) to incorporate sections 21 and 22 of the MDP. This is a more specific recommendation than that proposed in the Discussion Paper. We believe this is necessary because it is important that the provisions and procedures be precisely the same across jurisdictions; and

Such changes would ensure consistency across jurisdictions and extinguish any incentive/s for forum shopping. It would also meet the object of the MDP to promote uniform laws throughout Australia.

<u>An effective summary dismissal procedure</u>

ARTK recommends that a summary dismissal procedure for defamation be legislated, including the ability for defendants to raise strike out arguments and capacity arguments in relation to the imputations pleaded by a plaintiff at an early stage in proceedings, rather than being matters deferred to trial. This will require changes to the docket process of certain courts, including the Federal Court, such that the summary dismissal process is not 'kicked down the road' but rather should be at the start – before significant costs and resources of all parties and the court have been allocated and/or expended.

We agree that defamation claims are capable of being misused in circumstances mounting to abuse of process, and an effective summary dismissal procedure to prevent those claims going to full hearing is an essential part of the law. However some Australian courts are reluctant to accept or apply the principles of proportionality at first instance and appellate levels.

Lastly, we note for the Committee that ARTK has engaged with the Federal Court regarding the drafting of a Practice Note for defamation cases. We are hopeful this will align the Federal Court with other states, for example NSW where the vast majority of defamation cases are brought, to assist with the 'uniformity' of the law and processes.

ATTACHMENT A

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY REVIEW OF THE MANDATORY DATA RETENTION REGIME

4 JULY 2019

Australia's Right to Know coalition of media organisations welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security review of the mandatory data retention regime of the *Telecommunications (Interception and Access) Act)* 1979 (the TIA Act).

The mandatory data retention regime is a legislative framework which requires carriers, carriage service providers and internet service providers to retain a defined set of telecommunications data for two years, ensuring that such data remains available for law enforcement and national security investigations. Under this framework, approved law enforcement agencies are able to access this data without a warrant.

Concerns expressed in relation to freedom of the press and access to journalists' metadata during the introduction of the legislation resulted in the inclusion of a Journalist Information Warrant scheme (JIW Scheme) at Division 4C of the TIA Act. These amendments entail intelligence organisations and law enforcement wanting to access journalists' data to discover their sources would first have to seek a warrant.

THE JOURNALIST INFORMATION WARRANT SCHEME REQUIRES IMMEDIATE AMENDMENT

While the intention of JIW Scheme may have been well-meaning, as it currently stands it does little to meaningfully deliver its stated aims. The JIW Scheme is poorly drafted, cloaked in secrecy and does nothing to address concerns relating to identification of journalists' sources. In our view the JIW Scheme and related legislation relating to access to journalists' records more broadly require fundamental reconsideration and immediate amendments.

The current investigations and associated AFP raids into reporting by News Corp's Annika Smethurst and the ABC have shone a spotlight on the erosion of fundamental press freedoms that is the cumulative effect of multiple pieces of legislation, including this one. It is critical that any law in this area is proportionate to the concerns the law is seeking to address.

In our view, the JIW Scheme and the Mandatory Data Retention regime do not pass this test. It is now incumbent on this Committee and the Government of Australia to take action to ensure that the public's right to

know is appropriately balanced with the harms that are sought to be addressed in relation to national security. The Government's objectives must be clearly stated and well defined and where these objectives may impact on press freedom, the measures to address them must be no more than is reasonably necessary to achieve the overall national interest, which includes the national interest in open and accountable Government and public administration.

ARTK strongly holds that our recommended amendments to the JIW Scheme and related legislation will assist to ensure the Australian public's right to know is actively considered in 'balancing' the actions of law enforcement and intelligence activities. The recommended amendments are vital to the fundamental role of news reporting in Australia's right to know.

LEGISLATIVE AMENDMENTS REQUIRED

Foremost, we recommend that accessing the metadata and/or content of journalists' communications for any reason or purpose associated with undertaking professional journalistic activity should not be the subject of any authorisation for disclosure, including any warrant issued, under the TIA Act. That is, we believe that journalists who are reporting in the public interest should be exempt from the operation of this legislation.

If this is not accepted, then we strongly contend that the JIW Scheme must be overhauled as detailed below:

1. A Journalist Information Warrant (JIW) is required for ALL warrants sought under the TIA Act when the subject of the warrant is a journalist, media organisation or similar; and

2. An application for a JIW must be contestable and authorised only if the public interest in accessing the metadata and/or content of a journalist's communication outweighs the public interest in NOT granting access; and

3. The JIW Scheme must apply consistently to ASIO and enforcement agencies; and

4. Transparency across all elements of the JIW Scheme is required.

DETAILED ANALYSIS OF RECOMMENDED AMENDMENTS ABOVE

Lack of transparency = Lack of 'evidence'

Unfortunately, our submission is mostly devoid of evidence of the way in which the JIW Scheme has operated and the role played by the PIAs, since the commencement of the JIWS in 2015 because of the secrecy provisions which apply to the applications for, and approvals of, JIWs.

However, we are aware that:

- There has been at least one breach of the TIA Act by the AFP where, in the process of an investigation, an AFP member accessed Call Charge Records and telecommunications data pertaining to a journalist without a Journalist Information Warrant being issued, in breach of the TIA Act;[24]

- The AFP has admitted that they had obtained another journalist's metadata, prior to the commencement of the JIW Scheme, at the request of the Department of Immigration in order to determine the journalist's sources of a story published by *Guardian Australia*[25] that revealed that a

[24] AFP statement; and reporting AFP admits illegally obtaining journalist's phone records; Police illegally obtained journalist's phone records under new metadata retention regime; Scheming police is spin over data raid
[25] See https://www.theguardian.com/world/2014/apr/17/australian-ship-went-far-deeper-into-indonesian-waters-than-disclosed?CMP=share_btn_tw

Customs vessel had entered deeper into Indonesian waters than previously disclosed. Whilst not in breach of any law, the incident assists to indicate the types of matters in which Commonwealth enforcement authorities consider there to be a greater public interest in disclosure than in the protection of fundamental freedoms, such as confidential information, privacy and the public's right to know; and

- At least two PIAs have been appointed[26].

Recent investigations

In addition, three recent events of grave concern to the media involve the use of AFP warrants or other investigative powers directly affecting journalists and related to their confidential sources.

i. First, the AFP raid at the home of News Corp journalist Annika Smethurst on 4 June 2019 involved a search of the entire contents of Ms Smethurst's home in order to identify the source of an article written in April 2018 which suggested that the government was considering allowing surveillance of its citizens by the Australian Signals Directorate;

ii. The raid at the premises of the ABC in relation to documents featured in ABC reporting known as "the Afghan files" about aspects of Australia's special forces in Afghanistan occurring during the period 2009-2013, which had been published in 2017; and

iii. The third incident involved the questioning of 2GB and Sky News journalist, Ben Fordham regarding information which he had broadcast on 2GB to the effect that the Department of Home Affairs was investigating the passage of six asylum seeker boats from Sri Lanka to Australia.

OPTION 1 – EXEMPTION FOR PUBLIC INTEREST REPORTING

We are aware of no evidence to suggest that the accessing of journalists' information to identify confidential sources of news reports plays a sufficiently useful role in the performance of the proper functions of Australia's security and other enforcement agencies that it would outweigh the importance of the public interest in protecting the identity of confidential sources to the media. To the contrary, it is clear that the continued existence of legislative power which allows such access is likely to have a serious chilling effect on public interest reporting in Australia, and is extremely vulnerable to circumvention. Sources of important public interest information are unlikely to make any contact with the media if they fear that those communications can be traced. Similarly, journalists are likely to be wary of publishing reports which expose Government decision making and policy information for fear of being the subject of intrusive search powers, including of their metadata records – for any purpose, not just to identify sources – as a result.

On the basis of the limited amount of information available to us, as indicated above, it is difficult to see how the identification of the source of information in those examples could be said to provide sufficient assistance to the protection of genuine security interests as to outweigh the recognised public interest in protecting the confidentiality of sources. In some cases, the information allegedly provided by the source is simply not significant. In others, it is old and possibly out of date.

The media organisations which comprise ARTK have a proven record of consulting with Government and exercising appropriate editorial discretion to ensure that no matter which would truly threaten Australia's national security is published by them.

[26] Former South Australian Supreme Court judge Kevin Duggan and former Queensland Supreme Court judge John Muir: https://www.smh.com.au/politics/federal/malcolm-turnbull-appoints-exjudges-to-defend-journalists-under-data-retention-laws-20160124-gmczxg.html

It is vital that secretive and extensive disclosure powers are not then used, and do not appear to be used, to prevent and punish the publication of stories which are merely embarrassing for our Government.

Alternatively, ARTK submits that only in cases of investigations relating directly to Australia's national security should journalists' metadata be the subject of any application for access, on the strict conditions outlined below.

OPTION 2 – OVERHAUL OF THE JIW SCHEME

As we have expressed above, if an exemption is not accepted, then the JIW Scheme must be overhauled consistent along four subject areas detailed below.

These changes find support in the recommendations of the Senate Legal and Constitutional Affairs Committee Inquiry into *The current investigative processes and powers of the Australian Federal Police in relation to non-criminal matters,*[27] including that the Commonwealth Government introduces laws regarding accessing information or records from media organisations during investigations by the Australian Federal Police.

We detail our changes below.

JIW required for ALL warrants sought under the TIA Act where the subject is a journalist/media organisation

Presently, a JIW is only required in relation to accessing the metadata relating to a particular person if the relevant authorising person "knows or reasonably believes that particular person to be a journalist or an employee of a journalist and the purpose of the authorisation is to identify another person believed to be a source".

Change is required for two reasons:

i. Presently, a JIW is ONLY required for access to a journalist's metadata but not any other information and data accessible by warrants – for example intercepted telecommunications (dealt with in Chapter 2 of the TIA Act) and stored communications (dealt with in Chapter 3 of the TIA Act). This must be rectified; and

ii. A JIW is only required where the purpose is to identify a source. This is far too narrow and requires amendment. As we have put previously, the JIW is focused on the purpose rather than the effect of accessing the data. However, a JIW should be obtained regardless of whether or not the journalists' data is accessed for the purpose of identifying sources.

    Limiting the application of the JIW process to circumstances where the purpose of data access is to identify journalists' sources provides inadequate protection to journalist's sources which are revealed when the data is accessed for any other purpose – and not subject to the JIW process. This makes the JIW scheme vulnerable to circumvention. There is no case to support the use of disclosure of other information held by journalists.

The application for a JIW must be first approved by the Attorney General and the scheme must be applied equally across the types of applicants involved

It is our strong view that any application for a JIW (including a JIW for journalist's information other than metadata which is dealt with above) must not be made without the Attorney General first approving the making of the application. The application should then be contestable as outlined below.

---

27 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/AFP_Inquiry/report/~/media/Committees/Senate/committee/legcon_ctte/AFP_Inquiry/report/report.pdf

Requiring the Attorney General to adopt a 'gate-keeper' role at this early stage will ensure that the warrant application process is engaged only once the Attorney General has confirmed that a genuine issue of national security has arisen and that a JIW may be justified in the protection of that interest.

The JIW Scheme must apply consistently to ASIO and enforcement agencies

Currently, there are differences which apply to ASIO and enforcement agencies as to whom a request to issue a JIW must be made and the tests which apply to those authorising persons for the purpose of determining those applications.

- In the case of ASIO – the Director General of Security requests the Attorney General to issue a JIW (at section 180J). Under s180L, the Attorney General must not issue a JIW unless they are satisfied that AISO's functions would extend to the making of authorisations to disclose the information in relation to the particular person (i.e. the journalist). Those functions allow disclosure where ASIO "is satisfied that the disclosure would be in connection with the performance by [ASIO] of its functions" (at sections 175 and 176).

- In the case of other enforcement agencies (including the AFP) – an application for a JIW must be made to a Part 4-1 issuing authority, such as a Judge. The issuing authority must not issue a JIW unless satisfied that the warrant is reasonably necessary for making authorisations for certain permitted purposes, namely enforcement of the criminal law (at section 178, finding a missing person (at section 178A), enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (at section 179), investigation of a serious offence (at section 180), or enforcing foreign and international laws (at section 180A and 180B).

We recommend the JIW Scheme be applied consistently and so must require that:

i. Both ASIO and other enforcement agencies must apply first to the Attorney General for initial approval to make the application and then to an independent third party (say a Court) issuing authority for adjudication;
ii. The issuing authority should be a person who is a judge of a court created by the Parliament only. This would require some simple amendments to s6DC of the TIA Act; by deleting subsections (1)(a)(iii), (1)(b) and (2)(b); and
iii. The issuing authority must not issue a JIW unless satisfied, following a contested application as outlined below, that it is reasonably necessary to do so in the protection of Australia's national security interests.

An application for a JIW must be contestable

It is our strong view that any application for a JIW must be contestable.

This should be done by allowing the journalist or media organisation who is the subject of the warrant application to make submissions as to the public interest in NOT accessing the data/information. This would involve the following steps in aggregate:

- The journalist/publisher being notified of the application for a JIW;
- The journalist/publisher being represented at a hearing, presenting the case for the Australian public's right to know including the intrinsic value in confidentiality of journalists' sources and media freedom;
- That hearing being heard by an independent third party issuing authority with experience in weighing evidence, at the level of Supreme Court, Federal Court or High Court Judge; and
- That independent third party issuing authority making a decision whether or not to authorise the issuing of a warrant after having considered the positions put for each party; and

- A warrant can only be authorised if the public interest in accessing the metadata and/or content of a journalist's communication outweighs the public interest in NOT granting access, including, without limitation, the public interest in:
    - The public's right to know
    - The importance of sources including public sector whistle-blowers
    - The protection of identities of sources including but not limited to public sector whistle-blowers
    - Media freedom

Other

Additionally, some relatively minor amendments would then be required to the regulations to ensure that:

(a) PIAs are independent of government

In order to make clear that the Prime Minister, having appointed the PIA as a person eligible under s 13(1)(a) or having had that person properly appointed by a former Prime Minister, cannot subsequently change the level of security clearance that he or she "considers appropriate" for that PIA, then reg 24(2)(c)(ii), should be changed to read: "ceases to hold a security clearance to *the* level that the Prime Minister *considered* appropriate *when the person was declared to be a Public Interest Advocate".* Otherwise, the Prime Minister could easily terminate PIAs, contrary to the intention evinced by the restricted grounds of misbehaviour, incapacity and insolvency.

(b) PIAs should be appropriately remunerated for their work

Regulation 20(3) should be amended to enable a PIA to negotiate a higher daily rate with the approval of the Office of Legal Services Coordination or the Attorney-General. It should also be amended to enable a PIA to negotiate terms on which he or she may be paid a higher daily rate on a one-off basis to reflect the necessity to perform more than 6 hours' work in a day, particularly in light of the realistic possibility that applications for JIWs may be made urgently. Both these amendments would be consistent with the *Legal Services Directions 2005* (see Appendix D, cll 5 and 9).

(c) The PIA must have all relevant information before them

Regulation 16 should be amended in two respects.

i. First, the provision of further information to a PIA should be mandatory rather than discretionary.

ii. Second it should be the further information itself, and not merely a summary of it, which is provided to the PIA. This deals with the present gap in the regulations whereby there is a requirement that an applicant for a JIW to ensure that a copy of the proposed request or application is given to a PIA (regs 11(1), 12(1), and 12(2)), but this does not extend to "further information" relating to requests or applications which are given to the Attorney General or Part 4-1 issuing authority under ss 180K or 180R of the Act. No reason is identified in reg 16 for *not* providing the PIA with the further information: the discretion is entirely unstructured and subject to no explicit constraints. In our view, there is no good reason why the PIA should not be provided with the further information (it may be noted that the regulations require that PIAs will either hold relevant security clearance, or be appropriately qualified to deal appropriately with sensitive information, so legitimate secrecy cannot be the reason)

In either case, it is important to bear in mind that the whole scheme of Division 4C of Pt 4-1 is that there are *competing* public interests that must be weighed by the independent third party issuing authority – the public interest in issuing a JIW and the public interest in NOT issuing the JIW.

Transparency across all elements of the JIW Scheme is required

Transparency must be introduced into the JIW application process, as indicated above and such that it be legislated that:

- The journalist must be notified of the application for a JIW; and
- The journalist must be able to obtain representation for the hearing; and
- A record of the hearing must be publicly available.

Further, the public interest in transparent operation of Australian law and enforcement requires the introduction of meaningful annual reporting requirements for the JIW Scheme.

This must include – but not be limited to – disaggregated reporting of the number of applications and authorisations of Journalist Information Warrants made by ASIO and enforcement agencies by each type, and summaries of hearings. This must be a legislated reporting requirement. The reporting should be included in the TIA Act annual report. As there is often an extended passage of time after the end of the financial year that the TIA Act annual report as tabled and made public, we also recommend that the Parliamentary Joint Committee on Intelligence and Security receive the report and it be made public in a timelier fashion.

THE AUSTRALIAN

Australia is a world-beater in the secrecy Olympics

GEORGE WILLIAMS
Follow @ProfGWilliams

By **GEORGE WILLIAMS**, COLUMNIST
12:00AM JUNE 10, 2019 • 98 COMMENTS

It comes as no surprise that the Australian Federal Police has begun to raid journalists. The events of last week are the culmination of nearly two decades of lawmaking by our national parliament. Our elected representatives have armed the police and intelligence agencies with formidable powers that can be used against the media. They have simply begun to use them.

Our politicians have sold these laws on the basis that they are needed to protect the community from terrorism and foreign interference. Strong laws are needed in these areas, but they do not justify absolute government secrecy. Nor are they a reason for jailing journalists who report in the public interest. In fact, the converse is true. The greater the power conferred on government, the greater the need for a strong media.

Australia leads the world in enacting national security and counter-terrorism laws. About 75 have been passed by our federal parliament since September 11, 2001. This far exceeds the number of similar laws passed by Britain and the US. Our laws also differ because they go further in heightening government secrecy. They represent an assault on freedom of the press unique to Australia.

Australia has a statute book littered with laws that enable sources to be identified, whistleblowers to be shut down and journalists to be jailed. Time after time when politicians were questioned about these laws, they said that they would not be used against the media.

They said these laws were about combating terrorism, and that our leaders could be trusted to ensure that over-broad powers were not used to damage our democracy. Basing freedom of the press on trusting those who have the most to gain from muzzling the media was never a wise idea.

The focus over recent days has been on laws that permit the police to seize data and documents from journalists in aid of prosecuting people who reveal government secrets. Many laws now permit this. For example, section 35P of the ASIO Act makes it a criminal offence to disclose information about special intelligence operations in which ASIO officers are granted immunity from civil and criminal liability.

A person can be jailed for up to five years merely for disclosing information about such an operation. There is no exception for reporting in the public interest.

Of even greater concern are laws that undermine media freedom in secret. One example is the ability of enforcement agencies to access the metadata of journalists, including things like mobile phone records. This information can be accessed to identify the source of a media story without notifying the journalist. The information can then be used to prosecute people who have supplied information to the journalist.

Another example is the power held by ASIO allowing it to compel any person, including journalists, to answer questions for the purpose of gathering intelligence. A person may even be detained in secret for up to a week. A journalist will face jail for up to five years if they fail to answer every question put to them. Any person who writes or tweets about the use of this power faces another five years.

I could go on with other examples, many of which were forgotten once the debate over each law died down. Yet these laws remain in force, and can be used at the discretion of the authorities.

Put together, their impact and scope is shocking in showing how far media freedom has deteriorated. They are the sorts of laws one might expect in a police state rather than a democracy like Australia.

We can thank our politicians for these laws. They have used the fear of terrorism and threats to community safety to enact laws that shield government from scrutiny. Our

liberties have had too few defenders. Each of the laws that restrict media freedom and freedom of speech has been passed with bipartisan support. Parliament has long ceased to be the protector of our democratic rights.

Australia's legal landscape has made this possible. We are the only democratic nation without strong national protection for freedom of speech and of the press.

The best we have is an implied freedom of political communication derived from our Constitution. But this has been applied rarely by the High Court, and is likely to be of limited value where national security and the media are concerned.

We lack anything like the first amendment to the US constitution, which states in unequivocal terms that "congress shall make no law ... abridging the freedom of speech, or of the press". Nor do we possess the protections of free speech found in Britain's Human Rights Act 1998, the Canadian Charter of Rights and Freedoms 1982 or the New Zealand Bill of Rights Act 1990.

Laws such as these make a difference. They counterbalance the desire of governments to keep embarrassing and damaging material secret. They also provide legal backing to the media in reporting such information.

If we want to avoid more raids and the further erosion of media freedom, we must convince parliament to enact long overdue protection for freedom of speech and of the press.

George Williams is dean of law at the University of NSW.

GEORGE WILLIAMS, COLUMNIST
George Williams AO is one of Australia's leading constitutional lawyers, having worked for many years as an academic and as a barrister. He is the Dean and Anthony Mason Professor at the Faculty of Law, Univers... Read more

More stories on this topic

- Second press freedom probe
- Christchurch reports cleared
- Leaking charges still on table

THE AUSTRALIAN

How informer's fears triggered terror raids

By **CAMERON STEWART**
THEAUSTRALIAN
12:00AM SEPTEMBER 15, 2012

AN ASIO informer who was caught spying on a hardline Muslim group in Melbourne warned the spy agency that it was asking him to do things that could compromise his safety.

The informer, who had infiltrated a radical group at the al-Furqan Islamic Centre in Springvale, told ASIO in July he wanted "a relocation and name change if rumours spread about me" because ASIO was asking him to "rock up at events on my own".

That informer is now believed to be in hiding with police protection after his identity was uncovered by the group late last month, forcing police to conduct sweeping counter-terrorism raids across 12 Melbourne properties this week.

A man alleged to be a member of the group, Adnan Karabegovic, 23, has been charged with allegedly collecting al-Qa'ida magazines, including one that touts the Sydney Opera House as a potential terrorist target.

For at least three months, ASIO used a Melbourne man to infiltrate the group of about 30 hardline Muslims led by a radical Bosnian self-styled sheik called Harun Mehicevic, also known as Abu Talha. But the counter-terror investigation, the largest since Operation Neath in 2009, unravelled suddenly late last month when members of the group obtained the informant's mobile phone containing a string of text messages with his ASIO contact known as "Jay".

The group photographed the text messages and posted them on the al-Furqan Centre's Facebook page two weeks ago, placing the man in immediate danger and leaving ASIO without a contact.

Authorities are believed to have been monitoring the Springvale al-Furqan group for years because of its hardline Salafist interpretation of Islam, its open hostility towards the West and its support for jihadist causes.

The group, whose beliefs are rejected by mainstream Islamic groups, was set up a decade ago by Harun after he became frustrated by the moderate Islam taught at his regular mosque at Noble Park.

It is unclear when ASIO was able to recruit an informer to infiltrate the group, but from that moment the spy agency had unparalleled access to the group's activities.

The published text messages date from late May this year when the informer tells Jay "I have the screen shots on USB", to which Jay replied: "Did it say his real name or where he was from", before asking the informer to "get some" CDs from the al-Furqan centre.

For the next two months, Jay from ASIO and the informer swap text messages every few days, with the informer passing on details of people's whereabouts, their activities and their background.

The informer sometimes gets frustrated with the secretive Jay, chiding him on text saying "u never answer ur fone".

At around this time, the informer writes: "spoke to him on fb (Facebook) and he put up pics and locations." To which Jay responds: "Cool, did he say why he went there."

On one occasion Jay appears to get frustrated with the informer's casual approach. When the informer writes: "Yeh, shouldn't be a prob inshallah (God willing)." Jay replies: "No inshallah! It should be a lecture on Ramadan."

In mid-July, the informer appears to get weary of ASIO's constant requests. On July 13, when Jay asks him to go to al-Furqan on the following Sunday, the informer replies: "I'll do AF cos I got nuffin on but you owe me."

Also on July 13, the informer texts Jay the licence plate of a green Commodore, but four days later, on July 17, when Jay asks the informer to attend a fundraising function for the rebuilding of the Dandenong mosque, the informer expresses concern. He warns ASIO may need to help him start a new life if he is caught. "Bro I'll go but I'm telling u, ur doing a relocation and name change if rumors spread bout me cos I don't know nel there and then I just star(t) rockinn up at events. On my own too."

Jay tries to calm him, saying "u prob won't need to go was just checking your availability in case anything popped up", to which the informer replies, "yeh yeh u want me to go, just gimme details

wen u hav em."

The following day, the informer tells Jay he will try to befriend a person of interest but says he doesn't want ASIO to therefore doubt his loyalty.

"Just letting you know b4 I c him and become friendly, don't want any backfire from the Canberra guys again."

On July 22, the informer tells Jay that a new person of interest has "just popped out of the woodwork, he is a revert of a few months with a half naked Greek girlfriend he kept from a previous life", to which Jay replies "ha ha lucky him".

At Jay's request, the informer keeps him updated about which members of the group are travelling and, at times, what restaurant or prayer centre they are in. Jay peppers him with questions about CDs used by the group and also about upcoming Islamic functions and who is going to attend.

On August 9, the two men meet at Lygon Court in Carlton for a briefing, but in an omen of what was to come, on August 13 the informer texts Jay apologising for being out of touch, saying "sorry left fone in car".

This potentially dangerous breach did not faze Jay, who continued to use phone text to pass on his requests.

On August 15, Jay asks the informer why a member of the al-Furqan group was asking questions about a police officer. "Did he say why he wanted to know about him," asks Jay.

The informer replies: "(he) said somfin bout a guy who he's been noticing around. He's just paranoid. Lightening doesn't strike twice."

But it seems the group's paranoia was well placed. Within a week of this message, the informer's phone had fallen into the hands of the al-Furqan group.

On or around August 22, at 5am, the group obtained the iPhone and read through more than 60 texts to ASIO's Jay.

ASIO knew almost immediately that the game was up and presumably moved fast to protect its exposed informer.

On August 22, a group member, Yasin Rizvic, posted on Facebook that "by the will of Allah The Almighty The Best of Plotters, we expose a spy amongst us -- working for ASIO, one of his Facebook names is (name delated) . . . so if you have him as a friend delete him."

Two days later, the al-Furqan website posted a rambling hour-long sermon from Harun, who spoke bitterly about the spy in their midst. He took aim at ASIO, the West and the US, making it clear that any Muslim who co-operated with intelligence agencies had betrayed their religion.

On August 26, photos of the texts sent between Jay and the informer were posted on the al-Furqan centre's Facebook page.

For the next 10 days, police and intelligence forces debated how they should respond to this extraordinary outing of an ASIO informer. Harun, the group's spiritual leader, was in Bosnia, but the decision was ultimately made that they should swoop sooner rather than later. On Wednesday, Australian Federal Police and Victoria Police launched raids of properties across Melbourne, catching the al-Furqan group by surprise. As police were breaking through the door of the centre on Wednesday morning, its Facebook page was promising that Abu Talha (Harun) "Tonight will be giving a live talk from Bosnia".

Instead of giving his sermon, Harun learned his centre and his home had been raided that day.

Victoria's third major counter-terrorism operation in eight years had been triggered, but in the most unusual of circumstances.

ATTACHMENT D – LEGISLATIVE PROVISIONS

ASIO Act – section 35P

Unauthorised disclosure of information

Disclosures by entrusted persons

(1) A person commits an offence if:

(a) the person is, or has been, an entrusted person; and

(b) information came to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and

(c) the person discloses the information; and

(d) the information relates to a special intelligence operation.

Penalty: Imprisonment for 5 years.

Note: Recklessness is the fault element for paragraphs (1)(b) and (d)--see section 5.6 of the *Criminal Code* .

(1A) Strict liability applies to paragraph (1)(a).

Note: For strict liability, see section 6.1 of the *Criminal Code*.

(1B) A person commits an offence if:

(a) the person is, or has been, an entrusted person; and

(b) information came to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and

(c) the person discloses the information; and

(d) the information relates to a special intelligence operation; and

(e) either or both of the following subparagraphs apply:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation;

(ii) the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 10 years.

Note: Recklessness is the fault element for paragraphs (1B)(b) and (d) and subparagraph (1B)(e)(ii)--see section 5.6 of the *Criminal Code*.

(1C) Strict liability applies to paragraph (1B)(a).

Note: For strict liability, see section 6.1 of the *Criminal Code* .

Other disclosures

(2) A person commits an offence if:

(a) the person discloses information; and

(b) the information relates to a special intelligence operation; and

(c) the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 5 years.

Note: Recklessness is the fault element for paragraphs (2)(b) and (c)--see section 5.6 of the *Criminal Code* .

(2A) A person commits an offence if:

(a) the person discloses information; and

(b) the information relates to a special intelligence operation; and

(c) either or both of the following subparagraphs apply:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation;

(ii) the person knows that the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 10 years.

Note: Recklessness is the fault element for paragraph (2A)(b)--see section 5.6 of the *Criminal Code* .

Exceptions

(3) Subsections (1) to (2A) do not apply if the disclosure was:

(a) in connection with the administration or execution of this Division; or

(b) for the purposes of any legal proceedings arising out of or otherwise related to this Division or of any report of any such proceedings; or

(c) in accordance with any requirement imposed by law; or

(d) in connection with the performance of functions or duties, or the exercise of powers, of the Organisation; or

(e) for the purpose of obtaining legal advice in relation to the special intelligence operation; or

(f) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986* ; or

(g) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.

Note: A defendant bears an evidential burden in relation to the matters in this subsection--seesubsection 13.3(3) of the *Criminal Code* .

(3A) Subsections (2) and (2A) do not apply to a person disclosing information if:

(a) the information has already been communicated, or made available, to the public (the ***prior publication***); and

(b) the person was not involved in the prior publication (whether directly or indirectly); and

(c) at the time of the disclosure, the person believes that the disclosure:

(i) will not endanger the health or safety of any person; and

(ii) will not prejudice the effective conduct of a special intelligence operation; and

(d) having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

Note: A defendant bears an evidential burden in relation to the matters in subsection (3A)—see subsection 13.3(3) of the *Criminal Code*.

Extended geographical jurisdiction

(4) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction--category D) applies to an offence against subsection (1), (1B), (2) or (2A).

(5) Subsection (4) does not, by implication, affect the interpretation of any other provision of this Act.

Criminal Code Act

Division 122—Secrecy of information

122.1 Communication and other dealings with inherently harmful information by current and former Commonwealth officers etc.

Communication of inherently harmful information

(1) A person commits an offence if:

(a) the person communicates information; and

(b) the information is inherently harmful information; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note 1: For exceptions to the offences in this section, see section 122.5.

Note 2: The fault elements for this offence are intention for paragraph (1)(a) and recklessness for paragraphs (1)(b) and (c) (see section 5.6).

Penalty: Imprisonment for 7 years.

Other dealings with inherently harmful information

(2) A person commits an offence if:

(a) the person deals with information (other than by communicating it); and

(b) the information is inherently harmful information; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note: The fault elements for this offence are intention for paragraph (2)(a) and recklessness for paragraphs (2)(b) and (c) (see section 5.6).

Penalty: Imprisonment for 3 years.

Information removed from, or held outside, proper place of custody

(3) A person commits an offence if:

(a) the person:

(i) removes information from a proper place of custody for the information; or
(ii) holds information outside a proper place of custody for the information; and

(b) the information is inherently harmful information; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note: The fault elements for this offence are intention for paragraph (3)(a) and recklessness for paragraphs (3)(b) and (c) (see section 5.6).

Penalty: Imprisonment for 3 years.

Failure to comply with direction regarding information

(4) A person commits an offence if:

(a) the person is given a direction; and

(b) the direction is a lawful direction regarding the retention, use or disposal of information; and

(c) the person fails to comply with the direction; and

(ca) the failure to comply with the direction results in a risk to the security of the information; and

(d) the information is inherently harmful information; and

(e) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note: The fault elements for this offence are intention for paragraph (4)(c) and recklessness for paragraphs (4)(a), (b), (ca), (d) and (e) (see section 5.6).

Penalty: Imprisonment for 3 years.

122.2 Conduct by current and former Commonwealth officers etc. causing harm to Australia's interests

Communication causing harm to Australia's interests

(1) A person commits an offence if:

(a) the person communicates information; and

(b) either:

(i) the communication causes harm to Australia's interests; or
(ii) the communication will or is likely to cause harm to Australia's interests; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note 1: For the definition of ***cause harm to Australia's interests***, see section 121.1.

Note 2: For exceptions to the offences in this section, see section 122.5.

Penalty: Imprisonment for 7 years.

Other conduct causing harm to Australia's interests

(2) A person commits an offence if:

(a) the person deals with information (other than by communicating it); and

(b) either:

(i) the dealing causes harm to Australia's interests; or
(ii) the dealing will or is likely to cause harm to Australia's interests; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Penalty: Imprisonment for 3 years.

Information removed from, or held outside, proper place of custody

(3) A person commits an offence if:

(a) the person:

(i) removes information from a proper place of custody for the information; or
(ii) holds information outside a proper place of custody for the information; and

(b) either:

(i) the removal or holding causes harm to Australia's interests; or
(ii) the removal or holding will or is likely to cause harm to Australia's interests; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Penalty: Imprisonment for 3 years.

Failure to comply with direction regarding information

(4) A person commits an offence if:

(a) the person is given a direction; and

(b) the direction is a lawful direction regarding the retention, use or disposal of information; and

(c) the person fails to comply with the direction; and

(d) either:

(i) the failure to comply causes harm to Australia's interests; or
(ii) the failure to comply will or is likely to cause harm to Australia's interests; and

(e) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Penalty: Imprisonment for 3 years.

122.3 Aggravated offence

(1) A person commits an offence against this section if:

(a) the person commits an offence against section 122.1 or 122.2 (the ***underlying offence***); and

(b) any of the following circumstances exist in relation to the commission of the underlying offence:

(ii) if the commission of the underlying offence involves a record—the record is marked with a code word, "for Australian eyes only" or as prescribed by the regulations for the purposes of this subparagraph;

(iii) the commission of the underlying offence involves 5 or more records each of which has a security classification;

(iv) the commission of the underlying offence involves the person altering a record to remove or conceal its security classification;

(v) at the time the person committed the underlying offence, the person held an Australian Government security clearance allowing the person to access information that has a security classification of at least secret.

Penalty:

(a) if the penalty for the underlying offence is imprisonment for 7 years—imprisonment for 10 years; or

(b) if the penalty for the underlying offence is imprisonment for 3 years—imprisonment for 5 years.

(2) There is no fault element for the physical element in paragraph (1)(a) other than the fault elements (however described), if any, for the underlying offence.

(4) To avoid doubt:

(a) a person does not commit an underlying offence for the purposes of paragraph (1)(a) if the person has a defence to the underlying offence; and

(b) a person may be convicted of an offence against this section even if the person has not been convicted of the underlying offence.

122.4 Unauthorised disclosure of information by current and former Commonwealth officers etc.

(1) A person commits an offence if:

(a) the person communicates information; and

(b) the person made or obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the person is under a duty not to disclose the information; and

(d) the duty arises under a law of the Commonwealth.

Penalty: Imprisonment for 2 years.

(2) Absolute liability applies in relation to paragraph (1)(d).

Sunset provision

(3) This section does not apply in relation to any communication of information that occurs after the end of 5 years after this section commences.

122.4A Communicating and dealing with information by non-Commonwealth officers etc.

Communication of information

(1) A person commits an offence if:

(a) the person communicates information; and

(b) the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(d) any one or more of the following applies:

(i) the information has a security classification of secret or top secret;
(ii) the communication of the information damages the security or defence of Australia;
(iii) the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth;
(iv) the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

Note 1: For exceptions to the offences in this section, see section 122.5.

Note 2: The fault elements for this offence are intention for paragraph (1)(a) and recklessness for paragraphs (1)(b) to (d) (see section 5.6).

Penalty: Imprisonment for 5 years.

Other dealings with information

(2) A person commits an offence if:

(a) the person deals with information (other than by communicating it); and

(b) the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(d) any one or more of the following applies:

(i) the information has a security classification of secret or top secret;
(ii) the dealing with the information damages the security or defence of Australia;
(iii) the dealing with the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against of a law of the Commonwealth;
(iv) the dealing with the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

Note: The fault elements for this offence are intention for paragraph (2)(a) and recklessness for paragraphs (2)(b) to (d) (see section 5.6).

Penalty: Imprisonment for 2 years.

Proof of identity not required

(3) In proceedings for an offence against this section, the prosecution is not required to prove the identity of the other person referred to in paragraph (1)(c) or (2)(c).

122.5 Defences

Powers, functions and duties in a person's capacity as a public official etc. or under arrangement

(1) It is a defence to a prosecution for an offence by a person against this Division that:

(a) the person was exercising a power, or performing a function or duty, in the person's capacity as a public official or a person who is otherwise engaged to perform work for a Commonwealth entity; or

(b) the person communicated, removed, held or otherwise dealt with the information in accordance with an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information.

Note: A defendant may bear an evidential burden in relation to the matters in this subsection (see subsection (12) of this section and subsection 13.3(3)).

Information that is already public

(2) It is a defence to a prosecution for an offence by a person against this Division that the relevant information has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information communicated etc. to integrity agency

(3) It is a defence to a prosecution for an offence by a person against this Division that the person communicated the relevant information, or removed, held or otherwise dealt with the relevant information for the purpose of communicating it:

(a) to any of the following:

(i) the Inspector-General of Intelligence and Security, or a person engaged or employed to assist the Inspector-General as described in subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*;

(ii) the Commonwealth Ombudsman, or another officer within the meaning of subsection 35(1) of the *Ombudsman Act 1976*;

(iia) the Australian Information Commissioner, a member of the staff of the Office of the Australian Information Commissioner, or a consultant engaged under the *Australian Information Commissioner Act 2010*;

(iii) the Law Enforcement Integrity Commissioner, a staff member of ACLEI, or a consultant to, or a person made available to, the Integrity Commissioner under the *Law Enforcement Integrity Commissioner Act 2006*; and

(b) for the purpose of the Inspector-General, the Ombudsman, the Australian Information Commissioner or the Law Enforcement Integrity Commissioner (as the case requires) exercising a power, or performing a function or duty.

Note: A person mentioned in paragraph (3)(a) does not bear an evidential burden in relation to the matters in this subsection (see subsection (12)).

Information communicated etc. in accordance with the Public Interest Disclosure Act 2013 or the Freedom of Information Act 1982

(4) It is a defence to a prosecution for an offence by a person against this Division that the person communicated the relevant information, or removed, held or otherwise dealt with the relevant information for the purpose of communicating it, in accordance with:

(a) the *Public Interest Disclosure Act 2013*; or

(b) the *Freedom of Information Act 1982*.

Note: A defendant may bear an evidential burden in relation to the matters in this subsection (see subsection (12) of this section and subsection 13.3(3)).

Information communicated etc. for the purpose of reporting offences and maladministration

(4A) It is a defence to a prosecution for an offence by a person against this Division that the person communicated, removed, held or otherwise dealt with the relevant information for the primary purpose of reporting, to an appropriate agency of the Commonwealth, a State or a Territory:

(a) a criminal offence, or alleged criminal offence, against a law of the Commonwealth; or

(b) maladministration relating to the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth; or

(c) maladministration relating to the performance of functions of the Australian Federal Police under:

(i) the *Australian Federal Police Act 1979*; or
(ii) the *Proceeds of Crime Act 2002*.

Note: A defendant may bear an evidential burden in relation to the matters in this subsection (see subsection (12) of this section and subsection 13.3(3)).

Information communicated etc. to a court or tribunal

(5) It is a defence to a prosecution for an offence by a person against this Division that the person communicated the relevant information, or removed, held or otherwise dealt with the relevant information for the purpose of communicating it, to a court or tribunal (whether or not as a result of a requirement).

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information communicated etc. for the purposes of obtaining or providing legal advice

(5A) It is a defence to a prosecution for an offence by a person against this Division that the person communicated, removed, held or otherwise dealt with the relevant information for the primary purpose of obtaining or providing, in good faith, legal advice in relation to:

(a) an offence against this Part; or

(b) the application of any right, privilege, immunity or defence (whether or not in this Part) in relation to such an offence;

whether that advice was obtained or provided before or after the person engaged in the conduct constituting the offence.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information communicated etc. by persons engaged in business of reporting news etc.

(6) It is a defence to a prosecution for an offence by a person against this Division that the person communicated, removed, held or otherwise dealt with the relevant information in the person's capacity as a person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media, and:

(a) at that time, the person reasonably believed that engaging in that conduct was in the public interest (see subsection (7)); or

(b) the person:

(i) was, at that time, a member of the administrative staff of an entity that was engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media; and

(ii) acted under the direction of a journalist, editor or lawyer who was also a member of the staff of the entity, and who reasonably believed that engaging in that conduct was in the public interest (see subsection (7)).

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

(7) Without limiting paragraph (6)(a) or (b), a person may not reasonably believe that communicating, removing, holding or otherwise dealing with information is in the public interest if:

(a) engaging in that conduct would be an offence under section 92 of the *Australian Security Intelligence Organisation Act 1979* (publication of identity of ASIO employee or ASIO affiliate); or

(b) engaging in that conduct would be an offence under section 41 of the *Intelligence Services Act 2001* (publication of identity of staff); or

(c) engaging in that conduct would be an offence under section 22, 22A or 22B of the *Witness Protection Act 1994* (offences relating to Commonwealth, Territory, State participants or information about the national witness protection program); or

(d) that conduct was engaged in for the purpose of directly or indirectly assisting a foreign intelligence agency or a foreign military organisation.

Information that has been previously communicated

(8) It is a defence to a prosecution for an offence by a person against this Division if:

(a) the person did not make or obtain the relevant information by reason of any of the following:

(i) his or her being, or having been, a Commonwealth officer;

(ii) his or her being otherwise engaged to perform work for a Commonwealth entity;

(iii) an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information; and

(b) the information has already been communicated, or made available, to the public (the ***prior publication***); and

(c) the person was not involved in the prior publication (whether directly or indirectly); and

(d) at the time of the communication, removal, holding or dealing, the person believes that engaging in that conduct will not cause harm to Australia's interests or the security or defence of Australia; and

(e) having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information relating to a person etc.

(9) It is a defence to a prosecution for an offence by a person against this Division if:

(a) the person did not make or obtain the relevant information by reason of any of the following:

(i) his or her being, or having been, a Commonwealth officer;
(ii) his or her being otherwise engaged to perform work for a Commonwealth entity;
(iii) an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information; and

(b) at the time of the communication, removal, holding or dealing, the person believes that the making or obtaining of the information by the person was required or authorised by law; and

(c) having regard to the circumstances of the making or obtaining of the information, the person has reasonable grounds for that belief; and

(d) any of the following apply:

(i) the person communicates the information to the person to whom the information relates;
(ii) the person is the person to whom the information relates;
(iii) the communication, removal, holding or dealing is in accordance with the express or implied consent of the person to whom the information relates.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

(10) To avoid doubt, a defence to an offence may constitute an authorisation for the purposes of paragraph (9)(b).

Removing, holding or otherwise dealing with information for the purposes of communicating information

(11) For the purposes of subsection (3), (4), (5) or (5A), it is not necessary to prove that information, that was removed, held or otherwise dealt with for the purposes of communicating it, was actually communicated.

Burden of proof for integrity agency officials

(12) Despite subsection 13.3(3), in a prosecution for an offence against this Division, a person mentioned in subparagraph (3)(a)(i), (ii), (iia) or (iii) does not bear an evidential burden in relation to the matter in:

(a) subsection (1), (4) or (4A); or

(b) either of the following:

(i) subparagraph (3)(a)(i), (ii), (iia) or (iii);
(ii) paragraph (3)(b), to the extent that that paragraph relates to the Inspector-General of Intelligence and Security, the Ombudsman, the Australian Information Commissioner or the Law Enforcement Integrity Commissioner.

Defences do not limit each other

(13) No defence in this section limits the operation of any other defence in this section.

*ARTK Note – there is no similar defence to the espionage offences at Part 5.2 of the Criminal Code Act

121.1 Definitions

(1) In this Part:

cause harm to Australia's interests means to:

(a) interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth; or

(b) interfere with or prejudice the performance of functions of the Australian Federal Police under:

(i) paragraph 8(1)(be) of the *Australian Federal Police Act 1979* (protective and custodial functions); or
(ii) the *Proceeds of Crime Act 2002*; or

(c) harm or prejudice Australia's international relations in relation to information that was communicated in confidence:

(i) by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and
(ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; or

(f) harm or prejudice the health or safety of the Australian public or a section of the Australian public; or

(g) harm or prejudice the security or defence of Australia.

inherently harmful information means information that is any of the following:

(a) security classified information;

(c) information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions;

(e) information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency.

deal: a person ***deals*** with information or an article if the person does any of the following in relation to the information or article:

(a) receives or obtains it;

(b) collects it;

(c) possesses it;

(d) makes a record of it;

(e) copies it;

(f) alters it;

(g) conceals it;

(h) communicates it;

(i) publishes it;

(j) makes it available.

make available information or an article includes:

(a) place it somewhere it can be accessed by another person; and

(b) give it to an intermediary to give to the intended recipient; and

(c) describe how to obtain access to it, or describe methods that are likely to facilitate access to it (for example, set out the name of a website, an IP address, a URL, a password, or the name of a newsgroup).

Criminal Code Act – section 119.7

Recruiting persons to serve in or with an armed force in a foreign country

Recruiting others to serve with foreign armed forces

(1) A person commits an offence if the person recruits, in Australia, another person to serve in any capacity in or with an armed force in a foreign country.

Penalty: Imprisonment for 10 years.

Publishing recruitment advertisements

(2) A person commits an offence if:

(a) the person publishes in Australia:

(i) an advertisement; or
(ii) an item of news that was procured by the provision or promise of money or any other consideration; and

(b) the person is reckless as to the fact that the publication of the advertisement or item of news is for the purpose of recruiting persons to serve in any capacity in or with an armed force in a foreign country.

Penalty: Imprisonment for 10 years.

(3) A person commits an offence if:

(a) the person publishes in Australia:

(i) an advertisement; or
(ii) an item of news that was procured by the provision or promise of money or any other consideration; and

(b) the advertisement or item of news contains information:

(i) relating to the place at which, or the manner in which, persons may make applications to serve, or obtain information relating to service, in any capacity in or with an armed force in a foreign country; or
(ii) relating to the manner in which persons may travel to a foreign country for the purpose of serving in any capacity in or with an armed force in a foreign country.

Penalty: Imprisonment for 10 years.

Criminal Code Act – section 80.2C

Advocating terrorism

(1) A person commits an offence if:

(a) the person advocates:

(i) the doing of a terrorist act; or
(ii) the commission of a terrorism offence referred to in subsection (2); and

(b) the person engages in that conduct reckless as to whether another person will:

(i) engage in a terrorist act; or
(ii) commit a terrorism offence referred to in subsection (2).

Note: There is a defence in section 80.3 for acts done in good faith.

Penalty: Imprisonment for 5 years.

(2) A terrorism offence is referred to in this subsection if:

(a) the offence is punishable on conviction by imprisonment for 5 years or more; and

(b) the offence is not:

(i) an offence against section 11.1 (attempt), 11.4 (incitement) or 11.5 (conspiracy) to the extent that it relates to a terrorism offence; or
(ii) a terrorism offence that a person is taken to have committed because of section 11.2 (complicity and common purpose), 11.2A (joint commission) or 11.3 (commission by proxy).

Definitions

(3) In this section:

advocates: a person ***advocates*** the doing of a terrorist act or the commission of a terrorism offence if the person counsels, promotes, encourages or urges the doing of a terrorist act or the commission of a terrorism offence.

terrorism offence has the same meaning as in subsection 3(1) of the *Crimes Act 1914*.

terrorist act has the same meaning as in section 100.1.

(4) A reference in this section to advocating the doing of a terrorist act or the commission of a terrorism offence includes a reference to:

(a) advocating the doing of a terrorist act or the commission of a terrorism offence, even if a terrorist act or terrorism offence does not occur; and

(b) advocating the doing of a specific terrorist act or the commission of a specific terrorism offence; and

(c) advocating the doing of more than one terrorist act or the commission of more than one terrorism offence.

Crimes Act 1914 – Section 15HK

Unauthorised disclosure of information (controlled operations)

Disclosures by entrusted persons

(1) A person commits an offence if:

(a) the person is, or has been, an entrusted person; and

(b) information came to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and

(c) the person discloses the information; and

(d) the information relates to a controlled operation.

Note: Recklessness is the fault element for paragraphs (1)(b) and (d)--see section 5.6 of the *Criminal Code* .

Penalty: Imprisonment for 2 years.

(1A) Strict liability applies to paragraph (1)(a).

Note: For strict liability, see section 6.1 of the *Criminal Code* .

(1B) A person commits an offence if:

(a) the person is, or has been, an entrusted person; and

(b) information came to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and

(c) the person discloses the information; and

(d) the information relates to a controlled operation; and

(e) either or both of the following subparagraphs apply:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a controlled operation;

(ii) the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a controlled operation.

Note: Recklessness i s the fault element for paragraphs (1B)(b) and (d) and subparagraph (1B)(e)(ii)--see section 5.6 of the *Criminal Code* .

Penalty: Imprisonment for 10 years.

(1C) Strict liability applies to paragraph (1B)(a).

Note: For strict liability, see section 6.1 of the *Criminal Code* .

Other disclosures

(1D) A person commits an offence if:

(a) the person discloses information; and

(b) the information relates to a controlled operation; and

(c) the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a controlled operation.

Note: Recklessness is the fault element for paragraphs (1D)(b) and (c)--see section 5.6 of the *Criminal Code* .

Penalty: Imprisonment for 2 years.

(1E) A person commits an offence if:

(a) the person discloses information; and

(b) the information relates to a controlled operation; and

(c) either or both of the following subparagraphs apply:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a controlled operation;

(ii) the person knows that the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a controlled operation.

Note: Recklessness is the fault element for paragraph (1E)(b)--see section 5.6 of the *Criminal Code* .

Penalty: Imprisonment for 10 years.

Exceptions--general

(2) Subsections (1) to (1E) do not apply if the disclosure was:

(a) in connection with the administration or execution of this Part; or

(b) for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings; or

(c) for the purposes of obtaining legal advice in relation to the controlled operation; or

(d) in accordance with any requirement imposed by law; or

(e) in connection with the performance of functions or duties, or the exercise of powers, of a law enforcement agency.

Note: A defendant bears an evidential burden in relation to the matters in this subsection--see subsection 13.3(3) of the *Criminal Code* .

Exceptions--integrity testing controlled operation authority

(2A) Subsections (1) to (1E) do not apply, in the case of a controlled operation authorised by an integrity testing controlled operation authority (granted on the basis that an integrity testing authority is in effect), if the disclosure was:

(a) in any of the circumstances mentioned in paragraphs (2)(a) to (e); or

(b) in connection with the administration or execution of Part IABA, or the *Law Enforcement Integrity Commissioner Act 2006* , in relation to the integrity testing authority; or

(c) for the purposes of any disciplinary or legal action in relation to a staff member of a target agency, if arising out of, or otherwise related to, the controlled operation; or

(d) in relation to the integrity testing authority:

(i) for the purposes of any disciplinary or legal action in relation to a staff member of a target agency, if arising out of, or otherwise related to, an integrity testing operation authorised by the authority; or

(ii) to an authority of the Commonwealth, a State or a Territory, if the disclosure relates to the misconduct of an employee or officer of the authority.

Note: A defendant bears an evidential burden in relation to the matters in this subsection--see subsection 13.3(3) of the *Criminal Code* .

Exception--misconduct

(3) Subsections (1) to (1E) do not apply if:

(a) the person (the ***discloser***) discloses the information to the Ombudsman or the Integrity Commissioner; and

(b) the discloser informs the person to whom the disclosure is made of the discloser's identity before making the disclosure; and

(c) the information concerns:

(i) a corruption issue within the meaning of the *Law Enforcement Integrity Commissioner Act 2006* (see section 7 of that Act) in relation to a controlled operation; or

(ii) misconduct in relation to a controlled operation; and

(d) the discloser considers that the information may assist a person referred to in paragraph (a) to perform the person's functions or duties; and

(e) the discloser makes the disclosure in good faith.

Note: A defendant bears an evidential burden in relation to the matters in this subsection--see subsection 13.3(3) of the Criminal Code.

Exception--previously published information

(4) Subsections (1D) and (1E) do not apply to a person disclosing information if:

(a) the information has already been communicated, or made available, to the public (the prior publication); and

(b) the person was not involved in the prior publication (whether directly or indirectly); and

(c) at the time of the disclosure, the person believes that the disclosure:

(i) will not endanger the health or safety of any person; and

(ii) will not prejudice the effective conduct of a controlled operation; and

(d) having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

Note: A defendant bears an evidential burden in relation to the matters in subsection (4)--
see subsection 13.3(3) of the *Criminal Code* .

Crimes Act 1914 – Section 3ZZHA

Unauthorised disclosure of information (delayed notification search warrants)

(1) A person commits an offence if:

(a) the person discloses information; and

(b) the information relates to:

(i) an application for a delayed notification search warrant; or

(ii) the execution of a delayed notification search warrant; or

(iii) a report under section 3ZZFA in relation to a delayed notification search warrant; or

(iv) a warrant premises occupier's notice or an adjoining premises occupier's notice prepared in relation to a delayed notification search warrant.

Penalty: Imprisonment for 2 years.

(2) Each of the following is an exception to the offence created by subsection (1):

(a) the disclosure is in connection with the administration or execution of this Part;

(aa) the disclosure is for the purposes of obtaining or providing legal advice related to this Part;

(b) the disclosure is for the purposes of any legal proceeding arising out of or otherwise related to this Part or of any report of any such proceedings;

(c) the disclosure is in accordance with any requirement imposed by law;

(d) the disclosure is for the purposes of:

(i) the performance of duties or functions or the exercise of powers under or in relation to this Part; or

(ii) the performance of duties or functions or the exercise of powers by a law enforcement officer, an officer of the Australian Security Intelligence Organisation, a staff member of the Australian Secret Intelligence Service or a person seconded to either of those bodies;

(da) the disclosure is made by anyone to the Ombudsman, a Deputy Commonwealth Ombudsman or a member of the Ombudsman's staff (whether in connection with the exercise of powers or performance of functions under Division 7, in connection with a complaint made to the Ombudsman or in any other circumstances);

(e) the disclosure is made after a warrant premises occupier's notice or an adjoining premises occupier's notice has been given in relation to the warrant;

(f) the disclosure is made after a direction has been given under subsection 3ZZDA(4) or 3ZZDB(4) in relation to the warrant.

Note: A defendant bears an evidential burden in relation to a matter in subsection (2)--see subsection 13.3(3) of the *Criminal Code* .