ARTK SUBMISSION TO ATTORNEY-GENERAL'S DEPARTMENT REVIEW OF COMMONWEALTH SECRECY PROVISIONS

5 MAY 2023

INTRODUCTION

Australia's Right to Know Coalition (**ARTK**) thanks the Attorney-General's Department for the opportunity to provide submissions for the Review of Secrecy Provisions (**Review**).

ARTK's primary concerns with the current legislative regime are as follows:

1. Clear limiting principles in respect of secrecy provisions have not been adopted;
2. The excessive and unprincipled use of secrecy provisions has a suppressive effect on the media and transparent government in violation of both principles of open government and the associated freedom of political communication;
3. Criminal liability should not be applied to unauthorised dealings with Commonwealth information as a matter of course;
4. The current journalism 'defence' (s 122.5(6) of the Criminal Code) is inadequate in that the criminal standards applicable to the defence make it a 'dead letter' in practical terms for any journalist seeking to rely on it. Journalists remain subject to a real and meaningful prospect of being criminally investigated or caught in the investigative process; and
5. The essential public interest in being informed about activities of government is no longer adequately protected.

At the Department's count, Commonwealth legislation has 849 secrecy offences:

- 11 general secrecy offences in Part 5.6 of the Criminal Code;
- 542 specific secrecy offences in 178 Commonwealth laws; and

- 296 non-disclosure duties in 107 Commonwealth laws which attract criminal liability for unauthorised disclosure of information by current or former Commonwealth officers under s 122.4 of the Criminal Code.

This is excessive in a democratic country and emblematic of the failure of successive Governments to adopt clear, limiting principles in respect of secrecy offences.

Unauthorised dealings with Commonwealth information should not as a matter of course attract criminal liability, especially having regard to the primary public interest in open and accountable government. In that context it should not be sufficient to attract criminal consequences that it is merely inconvenient or embarrassing to the government that information becomes public. Further, there should not be criminal consequences for publication of information where there are already adequate and appropriate consequences in place (e.g. in relation to confidential or personal information).

For secrecy offences to play a legitimate role in a contemporary landscape where the public interest in open government must be treated as essential, they should only be enacted or remain in force where it is clearly demonstrated on a principled basis that they are needed to prevent or address the consequences of serious harm to an identified public interest, and where it is clearly demonstrated that preventing or avoiding that harm outweighs the primary public interest in maintaining open and transparent government.

Finally, and most importantly, journalists should not be subject to criminal consequences for doing their job in bringing stories to light. Such disclosures must be protected even if they cause short term harm to a public interest, because they secure the broader public interest of ensuring the effective functioning of democracy in the longer term.

As has been made clear in ARTK submissions to various reviews and inquiries over the years, the Australian media plays a vital role in holding the government to account and maintaining transparency. A democratic and representative government requires a well-informed public who can freely discuss and criticise their government's decision making. A well-informed public needs journalists who are able to receive information, investigate and report stories without fear of criminal repercussions.

ARTK recognises the importance of protecting national security and the role of all Australians, including the media, in preserving the safety of those involved in those endeavours. ARTK also believes that the law has to preserve the public's right to know and secrecy offences must be limited to circumstances where serious harm would be caused to the public interest.

Currently, as demonstrated by the sheer quantity of secrecy provisions, neither a principled basis for nor restraint in enacting secrecy offences has been applied to the vast array of provisions.

We believe the current review and any consequential reform should seek to limit the necessity for and the uses of excessive criminal liability and, to the extent it is asserted that there is a legitimate basis for an offence that basis, should be principled.

OVERVIEW OF THE SUBMISSION

Detailed responses to the questions posed by the consultation paper are set out in the submission. These responses are summarised as follows below:

QUESTION	SUMMARY OF RESPONSE
1. What principles should govern the framing of general secrecy offences and specific secrecy offences, including the categories of persons and information to which it is appropriate for each of these types of offences to apply?	ARTK has set out the three core principles that should govern the framing of any secrecy offences.
2. Having regard to these principles, are there any general or specific secrecy offences that should be amended or repealed? For any of these offences, are there other forms of action (such as civil or administrative action) that would be more appropriate to protect against unlawful communication or other dealing with the information?	Yes, ARTK identifies below general and specific offences that should be amended. ARTK also submits that any offences that are not compliant with the core principles articulated should be repealed.
3. Are there circumstances in which it is appropriate for a specific secrecy offence to prohibit conduct that is also prohibited by a general secrecy offence?	ARTK concedes that if a principled approach is adopted, then the need for specific offences is largely eliminated. Specific offences tend to create confusion as to the operative offence and undermines a coherent regime of protection of public disclosure, including a journalism exemption.
4. Are the current defences for general secrecy offences available under section 122.5 of the Criminal Code appropriately framed? Are there any amendments or additions to these defences that should be considered?	ARTK believes that the general concept of section 122.5 is appropriate. The defences are not currently appropriately framed, but may be with the appropriate amendments.
5. Are there any defences that should generally be available for specific secrecy offences? Are there amendments or additions to defences for specific secrecy offences that should be considered?	Three defences should be applied across any remaining secrecy offences, being defences for: a) journalists; b) public interest disclosures; and c) disclosures to lawyers.

QUESTION	SUMMARY OF RESPONSE
6. What principles should determine how the public interest journalism defence to the general secrecy offences in Part 5.6 of the Criminal Code is framed?	ARTK has set out the principles that should be applied.
7. Having regard to those principles, is the current public interest journalism defence in Part 5.6 of the Criminal Code appropriately framed? If not, what amendments should be considered?	ARTK does not consider the current public interest journalism defence to be appropriately framed.
8. Should the public interest journalism defence to the general secrecy offences in Part 5.6 of the Criminal Code identify factors that may be considered for the purposes of determining whether the communication or other dealing with the information may be in the public interest?	ARTK does not consider the defence should identify factors for consideration, as this would exacerbate the existing issues with the defence.
9. Should a public interest journalism defence modelled on subsection 122.5(6) of the Criminal Code be considered for specific secrecy offences, and for which offences would it be an appropriate defence?	ARTK supports a journalism protection modelled on subsection 122.5(6) being adopted for all disclosure offences.
10. Should the requirement for the Attorney-General's consent to prosecute a journalist for certain offences, which is currently imposed by a ministerial direction, be maintained? If so, should this requirement be legislated?	ARTK believes consent should be a requirement, and this requirement should be legislated.

CORE PRINCIPLES

There are three core principles which should govern whether secrecy provisions are implemented or otherwise preserved in Australia:

1. All non-disclosure/secrecy offences must protect the paramount importance of the Australian people's right to know about the conduct of its own government and its administrative actions. This requires robust journalist protections.
2. Any criminal sanction must require an intention to cause harm to a recognisable public interest.
3. There must be clear, meaningful and serious harm to a recognisable public interest, and any criminal sanction must be proportional to address that harm.

Without these principles in place, Australia is left in a position where there is a severe chilling effect on journalism, as journalists cannot report for fear they have unknowingly breached one of the many secrecy provisions and will face criminal consequences. ARTK sets out below detailed responses the consultation paper's questions having regard to these core principles.

It is important to note that, as discussed further below, including an element of "*reasonableness*" in any offence is **not sufficient** to meet the standard set by the principles. What this does is convert a criminal court trying the charges into an after-the-fact censorship board tasked with evaluating the professional standards and methodology of the journalist, where the consequences of the court disagreeing with the journalist's approach is jail. This is wrong in principle and creates a chilling effect on journalism as effective as an outright ban.

Question One: What principles should govern the framing of general secrecy offences and specific offences, including categories of persons and information to which it is appropriate for each of these types of offences to apply.

ARTK has set out above the core principles that should be applied and expands on these below.

PRINCIPLE ONE: All non-disclosure/secrecy offences must protect the paramount importance of the Australian people's right to know about the conduct of its own government and its administrative actions. This requires robust journalist protections.

Current law and practice does not protect this essential public interest and legislative reform is now essential

1.1 The protections that journalists require are not for the benefit of journalists.

1.2 It is unhelpful to characterise journalists' contributions to this discussion as a request for 'special' or preferential treatment. Such characterisations do not take account of the fact that all current secrecy laws provide for the use of protected information by certain people for certain purposes. What those permitted uses are ultimately comes down to one of two things:

(a) the view of those formulating the original secrecy law about which uses of government information were and were not in the public interest. The concept of what uses are in the public interest can and should change over time; and

(b) the unspoken liberal democratic assumptions of the architects of these laws and their expectations of how secrecy laws would be administered in practice, namely, to be exceptional in their application and confined to cases of actual, concrete harm.

1.3 On this last point, the architects of the original laws would likely be deeply concerned by the increasingly administrative application of criminal liability to deal with internal disciplinary matters. This is particularly the case where the action by a public servant or journalist that is the subject of criminal investigation was to raise concerns about government wrongdoing or misconduct. The architects would likely say that no law enforcement agency or prosecuting authority would or should use a secrecy law to prosecute a public servant or journalist in such cases, and that the issue was never addressed in legislation because it was assumed law enforcement and prosecutors would share basic liberal democratic assumptions and bring a nuanced and reasonable attitude to the administration of the criminal law.

1.4 In fact, for many decades a sensible and constructive attitude of police and security services was the norm. The clear understanding was that secrecy offences were to be administered having regard to

the public interest and in proportion to the actual (serious) harm to the public of any revelation. The exceptional nature of such laws – and the need to carefully manage the risks their administration could pose to a free and democratic society – was fully appreciated within government.

1.5 ARTK now asks government to recognise that one essential public interest – the public interest in the public being informed about the activities of its own government – is no longer adequately protected. It is let down by existing legislation and increased layers of secrecy that envelopes the Commonwealth government ecosystem which leaves legislative reform as the only viable option.

There is an essential and overriding public interest in the public being informed of the actions of its own government

1.6 The reasons for the public's right to know about the activities of its own government are clear and uncontroversial.

1.7 The free exchange of information about the activities of politicians and public servants is the only effective safeguard against government abuse, excess and mismanagement. Human behaviour adapts for the better where there is a credible risk that poor behaviour or underperformance will be identified and exposed.

1.8 The Commonwealth has failed to build a culture of transparency, as evidenced by increasingly seeking or claiming more secrecy over administrative matters and departmental resistance to openness. Government cannot ever be the sole or effective investigator of itself, as any judgments it makes about its own internal matters are conflicted and self-interested, even if approached with the best of motives. Its investigatory approaches and conclusions are therefore invariably compromised.

1.9 There are many examples that illustrate these endemic problems including evidence emerging from the Robodebt Royal Commission detailing the dysfunctional culture of decision-making within departments,[1] and the Jenkins report detailing the culture and practices of bullying, sexual harassment, and sexual assault in Commonwealth Parliamentary workplaces.[2] Both examples show that, left to its own devices, the Commonwealth is unable to identify and resolve serious internal problems.

[1] Tom Burton, 'Robo-debt is a case study in bad government and public service failure', *The Australian Financial Review* (online, 9 March 2023) <https://www.afr.com/politics/federal/robo-debt-is-a-case-study-in-bad-government-and-public-service-failure-20230309-p5cqob>; Luke Henriques-Gomes, 'Robodebt: five years of lies, mistakes and failures that caused a $1.8bn scandal', *The Guardian* (online, 11 March 2023) <https://www.theguardian.com/australia-news/2023/mar/11/robodebt-five-years-of-lies-mistakes-and-failures-that-caused-a-18bn-scandal>.
[2] Kate Jenkins, *Set the Standard: Report on the Independent Review into Commonwealth Parliamentary Workplaces* (Final Report, Australian Human Rights Commission, November 2021).

1.10 The contention that the existence of integrity bodies – in particular, the National Anti-Corruption Commission (**NACC**) – can allow government to continue to operate in secret because misconduct can now be addressed by these new, purely internal mechanisms, is not well founded. In particular:

(a) The NACC is not yet established and it will take some time for its functions to be properly entrenched. It will never have the capability to identify all instances of corruption or appropriately or effectively deal with all instances of corruption it identifies. That is not a negative reflection on those who will set up and lead the organisation; rather it is a reflection of the enormity of the task and inherent human and institutional limitations.

(b) The NACC's jurisdiction is directed only to the most serious forms of misconduct. Its function is not directed to investigating maladministration, for example, which can have profoundly negative consequences for the community. Also, given the non-binding nature of its findings, and the secrecy that is to attach to those findings, the Australian public have no guarantee that any adverse findings the NACC makes, could or will result in change within government.

(c) It has never been suggested at State or Territory level that an integrity body could ever be a completed substitute for journalism and reporting of government impropriety.

1.11 Ultimately, our system of democratic government requires the public have a clear and accurate picture of those they elect and those who serve in senior levels of the public service. A vast number of the offences identified directly prevent disclosure and most indirectly create a culture of secrecy. If secrecy laws can be used as a shield to prevent the public being informed about maladministration, misconduct or even corruption within government, the democratic system breaks down. Unsuitable people who make bad decisions will simply be re-elected or will remain in senior positions within the public service. Similarly, if the public cannot trust the picture presented to it of its government because of a veil of secrecy, then trust in democracy also breaks down.

1.12 The actions of those within government can cause serious damage to the national and other public interests. The damage and harm done to the public interest by those in whom the Australian public have placed their trust should and must be called out, as should personal failings that call into question a person's fitness to lead or which contradict the implied or explicit claims a person has made to secure office. A public official whose actions have caused harm or who has otherwise acted improperly cannot be able to avoid exposure merely by saying, "you cannot report my actions because it will harm a 'national interest'". That simply engages media in a cover up. The longer term national and public interest is served by disclosure of such information, because exposure is the only way to avoid the same mistakes and errors occurring again in future. Even when acting competently, the

internal actions of government may raise major issues that impact the lives of Australians and/or the direction of the country.

1.13 In all these instances, disclosure of such information by the media is democracy-reinforcing. Bringing these matters to light serves a broader, longer-term and essential public interest: the public interest in the Australian community being able to make informed decisions about its government and the direction of the country.

1.14 That public interest in disclosing information and of giving an accurate picture of the activities of the Australian government must, subject to very confined exceptions,[3] trump the protection of any competing recognisable public interests that may in the short term be harmed by a particular disclosure. This is because disclosures of this kind made for this purpose ensure the very integrity of the Australian system of government and its ability to make informed, proper and rational collective decisions that accord with community expectations in the longer term. Disclosures of this kind ensure the proper functioning of the system that identifies all other downstream public interests and how they are best managed, and in that sense is a measure directed to protecting the system for making decisions and so is best characterised as serving a 'greater' public interest.

1.15 A society that does not allow the scrutiny of those who lead it is not, in the final analysis, functional. It cannot self-correct.

1.16 Discussion within the Commonwealth about the role of secrecy and its enforcement through the criminal law has often missed a central point: the Australian government belongs to the Australian people. The information the Australian government holds or which relates to its operations belongs to the Australian people. There may be cases where there may be a public interest in withholding, often just for a period, information belonging to the Australian people from the Australian people. So be it, provided the case is compelling and the approach is ultimately endorsed by the Australian people. But it is not for government to dictate what is 'suitable' for the public to learn about its own government, where such decisions at least carry the *real risk* that they may promote the personal or institutional self-interest of those presuming to wield such powers over their fellow citizens.

The role of the media in promoting public transparency

1.17 Consistent with the current exceptions and defences available for more recent secrecy offences, protections for the disclosure of government information that are made to further the public interest

[3] For example, those now set out in Criminal Code s 122.5(7).

are appropriately confined to journalists acting in a professional capacity and those who support their operations within media organisations.

1.18 Journalists are bound by a broadly understood code of professional ethics. They are accountable in various ways for their professional journalistic judgements – including oversight through the Press Council, the Australian Communications and Media Authority and internal professional standards reviews within professional media organisations.

1.19 Journalists acting in a professional capacity and those who support their operations have demonstrated a responsible and even-handed approach to reporting that has earnt the Australian people's trust. They make careful, deliberative decisions to ensure that material is published without jeopardising lives or other essential interests. There have not been "Wikileaks" style disclosures from the media where vast amounts of highly sensitive material which can put lives in danger is simply uploaded to a website. The contrast between these is stark and important.

The public interest in the public being informed of the actions of its own government requires pre-publication certainty that reporting will not result in criminal investigation or prosecution

The realistic prospect of investigation and prosecution creates a chilling effect on public interest journalism no different to simply criminalising disclosures by journalists

1.20 A journalist should only be required to hold a bona fide belief that the disclosure was in the public interest.

1.21 There is a key difficulty with the current protections that seek to advance the public interest in ensuring the Australian people are meaningfully informed of the actions of their own government.

1.22 The law as it stands purports to protect public interest journalism from criminal prosecution in some situations.[4] But in reality, even where those protections exist, the current law subjects journalists to a real and meaningful prospect of being criminally investigated, charged, and brought before a Court to justify their reporting. That creates a chilling effect on public interest journalism as effective as if the law simply imposed an outright ban on journalists disclosing government information.

1.23 Investigatory processes, or the ever-present threat of their use, can be used to deter journalists. Any theoretical and contingent prospect of ultimate vindication after a stressful, disruptive and expensive criminal investigation and trial is a cold and meaningless comfort. It is ultimately this fear of investigation and prosecution, even if the journalist is ultimately vindicated, which will stay the hand

[4] Criminal Code s 122.5(6).

of a journalist in publishing newsworthy material as effectively as an outright criminal ban on publication.

The need to establish a "reasonable belief" that a specific disclosure of information is in the "public interest" creates a chilling effect on public interest journalism. A journalist should only be required to hold a bone fide belief

1.24 This realistic fear of a criminal investigation and charges arises from the requirement of journalist exemptions and defences that the journalist "*reasonably*" believe that their conduct in disclosing information was in the public interest.[5]

1.25 This requires the tribunal of fact, likely a magistrate, to make an evaluative finding about the reasons subjectively held by the journalist for publishing material and to consider any other objective circumstances of the publication to determine whether *in the eyes of the tribunal of fact* there were facts or other circumstances that could have inclined a rational person to hold that view. That is, the belief must be objectively justifiable.[6] The question is not what the journalist thought about the general newsworthiness of the story, but what the journalist subjectively believed about "*engaging in that conduct*" – i.e. engaging in the communication, removal, holding or otherwise dealing with the "*relevant information*", with the "*relevant information*" being the actual information that is the subject of the secrecy offence. So the question is not whether the story itself was believed by the journalist to be in the public interest. The question is more granular and answered by asking whether the particular disclosure of particular information as part of the story was "*reasonably believed*" by the journalist to be in the "*public interest*".

1.26 This puts an effective duty on the journalist to adduce or point to evidence that would objectively justify their reasons for using particular information in a particular way. That is the only practical way to establish that there was a belief by the journalist that the disclosure of particular secrecy information was in the public interest and that there was a rational and reasonable basis for that belief. In practical terms that defeats the protection provided.

1.27 This may well require the exposure of journalist sources. If the journalist must deal with the question of why they thought it appropriate to disclose particular information and if the nature or content of information itself is insufficient to explain the position, this naturally leads to the question of who supplied the information and how reliable that person was.

[5] Criminal Code s 122.5(6)(a),(b)(ii).
[6] *Oblach v The Queen* (2005) 65 NSWLR 75 at [55]-[57], [59]-[60] (Spigelman CJ), [74], [81] (Sully J) [88], [90]-[91] (Hulme J); *George v Rockett* (1990) 170 CLR 104 at [8].

1.28 It is the granular nature of the inquiry that makes it more likely a journalist will need to disclose their own methods and sources, rather than simply point to objective facts and circumstances. It is one thing to say: objective facts and circumstances point to why it was in the public interest to publish a story about potentially illegal bugging operations by police. It is another thing entirely to have to justify, by references to objective facts and circumstances, why the journalist chose to disclose particular information taken from a particular internal police memorandum, or chose to publish a photograph of a relevant "top secret" document, where the broader story could well have been told in some form and in some fashion *without making explicit reference to that material.*

1.29 It is established journalistic practice to receive and consider 'background' material, often of a highly sensitive nature, which is used to corroborate a story and identify lines of inquiry but which cannot for various reasons be used itself. What journalists hold back is as much a matter of professional journalistic practice as what they publish. If a defendant cannot point to objective facts and circumstances to explain why *particular* information was disclosed, they will be required to give evidence. In giving evidence, a prosecutor would be entitled to cross-examine on this issue of the journalist's methods and their sources and ask why, ultimately, the material in question was published and not simply used as background material or held back for another reason, even if the story itself is accepted to have been otherwise newsworthy.

1.30 Journalists simply cannot conduct their profession without being able to give binding assurances of confidentiality to their sources. Cross-examination places the journalist in an impossible position. As reasonableness is routinely seen by Australian courts as having a factually calibrated quality, what is encompassed within the 'public interest' may be affected by what is at risk. The more that is at risk from a particular disclosure, the more a court is likely to hold that more can be expected of the person who must justify their conduct in publishing or their holding of a particular belief.

1.31 This then leaves the tribunal of fact to assess whether the circumstances of the case, including any explanation by the journalist, is sufficient for it to be said the journalist had "*reasonable grounds*" for disclosing the relevant government information. This qualitative evaluation by the Court about the nature and value of a journalist's investigation and work product turns the Court into a de facto, after-the-fact censorship board sitting in judgment on the journalists' professional conduct in circumstances where the court is ill-equipped to effectively deal what might arise in such a contest: magistrates are not trained to evaluate journalistic methods or standards, nor Judges trained on how to instruct juries on them. But the consequence for the 'censor' disagreeing with the journalist is jail.

1.32 The magistrate may conclude, for example, that the story was newsworthy, but that the disclosure of particular classified documents was neither appropriate nor could be regarded by any right-thinking

person as appropriate, and that therefore the journalist did not have "*reasonable grounds*" to believe that the disclosure of *particular documents* was in the "*public interest*". The application of this criteria to this particular context carries the inherent risk of allowing the magistrate's own subjective view on what was and what was not appropriate to publish as 'good' or 'responsible' journalism to inform his or her view of whether the journalist had "*reasonable grounds*" for believing what they did was in fact in the public interest. The history of the interpretation of reasonableness in the courts has caused it to be a dead letter concept for journalists and the media.[7]

1.33 The prospect of the above process and its inherent uncertainties has a chilling effect on journalism because the more unpredictable the question of whether the protection applies, the greater the doubt over its potential application in the facts of any given case, and the more confident police and prosecuting authorities will be to proceed through an investigation to a trial.

1.34 Police in particular are likely to see the application of the protection as a matter of the journalist '*explaining themselves to the Court*' and progress an investigation on the basis that the issue is something ultimately to be resolved at trial. This means that every time a journalist publishes a story they have a real and genuine fear of investigation, prosecution, and ultimately having to demonstrate the value of the reporting to a magistrate who may well be unsympathetic, will be untrained in journalistic ethics and methods, and faced with ambiguous legislative direction. It is obvious that this fear will stay the hand of journalists when deciding whether or not to report stories they believe are objectively in the public interest.

1.35 These problems exacerbate another feature of current administrative practice. It is the routine practice of government to provide 'no comment' and refuse to confirm basic facts about a story. If a journalist receives a document marked "*secret*", the usual practice is that the agency in question will refuse to confirm that the document is authentic or that the stamp is current. That adds to the chilling effect on journalism because the journalist is left in a state of doubt or uncertainty, increasing their criminal exposure because it becomes harder for the journalist to establish that they had "*reasonable grounds*" to publish the document if, in fact, it turns out to be authentic.

1.36 Instead of the need to establish "*reasonable grounds*", a journalist should only be required to hold a "*bone fide"* belief that the disclosure of information subject to a secrecy offence was in the public interest. A "*bone fide*" requirement means the magistrate or other tribunal of fact is not required to make these inappropriately broad discretionary judgements that seek to second guess journalistic methodology and professional practices. This is what the related defence in s 122.5(5A) is directed

[7] See, for example, *Morgan v John Fairfax & Sons Ltd (No 2)* (1991) 23 NSWLR 374 at 387–8

towards, which provides that it is a defence where a person deals with information for the primary purpose of obtaining or providing "*in good faith*" certain kinds of legal advice. There is no principled reason that justifies a stricter and more onerous standard in the case of journalists receiving and disclosing information than lawyers.

The need to discharge an evidential onus also creates a chilling effect on journalism

1.37 Discussion of onus and standard of proof is often confused and sometimes at cross-purposes. ARTK, to bring clarity to the issue, seeks first to clarify what it sees to be the appropriate handling of onus of proof questions under a statutory journalist protection, then explain why it sees this is appropriate.

1.38 A journalist should not be under any evidential or legal burden to establish that a journalist protection applies. The prosecution should remain at all times under a duty to establish the absence of the protection applying beyond a reasonable doubt.

1.39 A journalist should need only raise a reasonable doubt about whether the protection applies by the close of the prosecution's case in order to secure an acquittal, and need not otherwise raise matters or adduce evidence showing that the protection may apply in order for the issue to become 'live' in the trial.

1.40 There are several reasons why a journalist protection should be treated as defining the scope of the offence to a primary disclosure offence in this way. These reasons take journalist protections outside the limited category of statutory "*defences*", "*exceptions*" or "*excuses*" where placing an evidentiary burden on the defendant may be seen as appropriate.

1.41 The effect of placing an evidentiary burden on a defendant to establish a matter is that the defendant is required to adduce or point to evidence "*that suggests a reasonable possibility that the matter exists or does not exist*".[8] Once that evidential onus is discharged, the legal burden then shifts to the prosecution to negate all the elements of the matter raised by the defendant beyond a reasonable doubt.[9] This is generally the framework now in place for the journalist defence in s 122.5(6) of the Criminal Code, which operates as a stated "*defence*" to the primary disclosure offences set out in the balance of Division 122 of the Criminal Code.

1.42 The difference between cases where an evidential onus sits on the defendant and cases where a circumstance acts to define the scope of the offence is the need for the defendant to credibly put the

[8] Criminal Code s 13.3(1),(6).
[9] Criminal Code s 13.1(2).

matters which are the subject of the evidential onus in play before the prosecutor is under any obligation to deal with those issues at trial. This is a flaw in the current provision.

1.43 The Commonwealth's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* states that provisions which impose an evidentiary onus on defendants reverse the fundamental principle of criminal law that the prosecution must prove every element of the offence and are appropriate only in limited circumstances.[10] The ramifications of this are wider, as explained by the Senate Scrutiny of Bills Committee:

> "*At common law, it is ordinarily the duty of the prosecution to prove all elements of an offence. This is an important aspect of the right to be presumed innocent until proven guilty. Provisions that reverse the burden of proof and require a defendant to disprove, or raise evidence to disprove, one or more elements of an offence, interfere with this common law right*."[11]

1.44 In the case of journalist protections, reversing this fundamental principle and abrogating the right to be presumed innocent has two specific negative impacts.

1.45 The first is that, where a journalist protection is the subject of a defendant's evidentiary burden, the journalist will usually need to go into evidence in order to discharge their evidential burden. This is because the prosecutor's case does not need to deal with all of the material which will establish whether the journalist protection applies, and so is not under any obligation to provide evidence that the defendant can point to in order to say that their evidential burden has been discharged.

1.46 For example, the prosecutor is not required to allege or prove that the defendant made the disclosure in their capacity as a "*person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media*" or deal with any of the circumstances that will touch on whether the journalist reasonably believed that the disclosure of particular information was in the "*public interest*", other than potentially adducing evidence of the act of publishing the story (the act of "*communication*") itself. That being said, the offence may well be triggered before this point in time (the act of "*dealing with*" information), so there may be no evidence before the court that the person was a journalist or obtained the material to prepare a story with a view to publication. For all the Court may be able infer from the prosecutor's case, the journalist may have received the material for the purposes of espionage or to blackmail.

---

[10] Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) (***Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers***), 50.

[11] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 1 of 2018, 7 February 2018) (***7 February 2018 Scrutiny Digest***), 84-85.

1.47 An effective duty to go into evidence where an onus of proof is reversed is not a theoretical risk.

1.48 In *R v Khazaal,*[12] the High Court considered the operation of s 101.5(1) of the Criminal Code (the offence of making a document connected with assistance in a terrorist act knowing of that connection). The defendant relied on the *defence*" or "*exception*" to liability to this offense under s 101.5(5) of the Criminal Code – by asserting that the collection or making of the document was not intended to facilitate preparation for, the engagement of a person in, or assistance in, more than one terrorist act. Mr Khazaal contended that he was a journalist researching and publishing information in relation to Islam and not acting with the requisite purpose.

1.49 As with s 122.5(6), an evidential burden sat on the defendant to establish this matter.

1.50 During Mr Khazaal's trial, there was evidence he had acted in such a role in the past. But the issue was establishing his intent or purpose *behind the particular publication*. The High Court held that even where an evidentiary burden may be satisfied by 'slender evidence' taken at its most favourable to the accused, there was no evidence of the purpose associated with that particular publication. On that issue, in a passage adopted as correct by the High Court, McLellan CJ at CL on appeal found that *"apart from the document itself, without (the defendant) giving evidence or there being other evidence from which his intention could be inferred, the evidential burden could not be discharged. There was nothing to suggest that he did not have the relevant intention."*[13]

1.51 This meant that Mr Khazaal was under an effective duty to go into evidence, which abrogated his right to silence.

1.52 To similar effect, the fact that a journalist needs to establish the current "*defence*' in s 122.5(6) in relation to particular information in a particular publication, and must do so in circumstances where the prosecution case need not deal with the key integers of making out that "*defence*", makes it difficult – if not impossible – for any journalist **not** to have to go into evidence to make the "*defence*" out.

1.53 The difficulty with requiring a journalist go into evidence is outlined above at paragraphs 1.29 to 1.30 and 1.45. If a journalist is required to give evidence, that exercise is likely to jeopardise the journalist's sources, as a prosecutor may cross-examine the journalist in relation to *any* matters relevant to the charges. For the reasons given above, that may include interrogating the journalist's journalistic

[12] *R v Khazaal* (2012) 246 CLR 601 (***R v Khazaal***).
[13] *R v Khazaal* at [20], [74]-[76].

methods and approach to ascertain whether they had "*reasonable grounds*" for believing that the particular disclosure of particular information was in the "*public interest*".

1.54 Indeed, the prospect that a confidential source may need to be disclosed to secure an acquittal simply creates a perverse incentive to prosecute journalists in order to uncover their sources so that the source themselves may be identified and prosecuted. More importantly, a journalist would only be able in those circumstances to avail themselves of the defence by abandoning their professional and ethical obligation to the confidential source. This means the defence in most cases will be illusory.

1.55 The second and related difficulty is that where a journalist is subject to an evidential burden on an issue, the matter is treated as something broadly within the exclusive knowledge of the defendant and a matter for the defendant to agitate at trial. So much follows from the fact that whether a matter is "*peculiarly within the knowledge of the defendant*" is actually one of the criteria set by the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* for making a matter the subject of a defendant's evidential onus in the first place. It stands to reason that, whenever a journalist protection is the subject of a defendant's evidential onus, police and prosecutors will approach their respective investigations or prosecutorial decisions by focusing on whether there has been a primary offence committed – and not whether the protection applies.

1.56 This will subject journalists to the same needless police interference seen in the criminal investigations of Ms Smethurst, then of News Corp Australia, and Mr Brown of the ABC, including heavy-handed and clearly excessive police raids (which were illegal in the case of Ms Smethurst),[14] public accusations of alleged criminality, and ultimately, the need to defend a criminal trial where the outcome in the journalist's favour is very much in doubt.[15] All that will have a significant chilling effect on journalism whatever the ultimate, theoretical outcome of a criminal trial.

1.57 It is not to the point that the prosecution guidelines of Commonwealth require a prosecutor to "*have regard to any lines of defence which are plainly open to, or have been indicated by, the alleged offender*" when assessing whether a prosecution has "*reasonable prospects*" of success.[16] If the preceding police investigation has not been directed to the issue of whether a journalist protection is available, then a prosecutor is going to have insufficient material to decide that a prosecution should

[14] *Smethurst v Commissioner of Police (Cth)* (2020) 272 CLR 177, 206 (Kiefel CJ, Bell and Keane JJ); 227 (Gageler J); 236 (Nettle J); 246 (Gordon J); 265 (Edelman J).
[15] For the reasons given above, because of the overly broad discretionary role of magistrates and other tribunals of fact in assessing whether the journalist protection is in fact available.
[16] Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth: Guidelines for the Making of Decisions in the Prosecution Process* (July 2021), accessible at https://www.cdpp.gov.au/sites/default/files/Prosecution%20Policy%20of%20the%20Commonwealth%20as%20updated%2019%20July%202021.pdf, [2.6].

be dropped because the journalist protection is available. The guideline does not inform the conduct of the preceding, highly disruptive, police investigation. Nor is the guideline enforceable or indeed immutable – it could change tomorrow.

1.58 On the other hand, if the journalist protection operates to define the scope of the primary disclosure offence, then these issues largely resolve. Police and prosecutors must focus, at the inception of an investigation, on the question of whether the journalist protection exists, and would only proceed beyond initial investigatory stages where clearly satisfied that the protection does not apply. The chilling effect on journalism from protracted police investigations and subsequent prosecutions would be mitigated, and costly, aborted criminal investigations and trials (born in large part by government) avoided.

1.59 Ultimately, it is not clear why an evidentiary onus is in fact now placed on a journalist to establish the existing, limited journalist protection contained in Division 122 of the Criminal Code.

1.60 The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* makes clear that placing an evidentiary onus on a defendant is appropriate only in limited cases.[17] Many of the core considerations listed in the guide for deciding to place an onus on the defendant have no application to journalist disclosures. In particular, whether or not a person *subjectively held* a belief that their actions were or were not in the public interest, and whether or not there were "*reasonable grounds*" for that belief, is not a matter "*peculiarly*" within the knowledge of the defendant but a matter which the prosecution could readily establish by inference from objective facts, just as prosecutors must establish most issues dealing with the state of mind of an accused by inference. To similar effect, if the provision was recast to require the prosecution to dispel any reasonable doubt that a journalist did not hold a *bone fide* belief that there conduct was in the public interest, such a matter could also readily be established by inference from objective facts. Nor is there any reason to see why it would be "*significantly more difficult and costly for the prosecution to disprove the matter than for the defendant to establish the matter*".

1.61 The relevant explanatory materials did not meaningfully direct themselves to these requirements, nor justify their assertion, made in relation to the journalist defence and other related defences that all imposed an evidential onus on a defendant, that "*requiring the prosecution to prove beyond reasonable doubt that a person's conduct was not for [a relevant purpose] would often prove an insurmountable barrier to a successful prosecution*".[18] That statement does not appear to make sense:

[17] *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, 50-51.
[18] Revised Explanatory Memorandum, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018* (Cth), [1643].

the prosecution would always have to disprove the existence of a journalist defence beyond a reasonable doubt. The issue was simply whether it needed to do so in all cases, or simply in cases where the journalist had discharged the evidential onus first.

1.62 Indeed, the varying reasons given as to why an evidential onus was to be placed on defendants in establishing the various defences in Division 122 of the Criminal Code were all rejected by the Senate Scrutiny of Bills Committee as either not to the point or incorrect.[19]

1.63 So ultimately, the use of the existing onus of proof provisions in Division 122 of the Criminal Code as a template for future necessary reform is bad in principle and will likely lead to an adverse scrutiny report that may jeopardise passage of this critical legislation.[20]

1.64 The appropriate approach is instead reflected in the secrecy offence "*defence*" which deals with disclosures to integrity bodies such as the Inspector General of Intelligence and security, the Commonwealth Ombudsman, the Information Commissioner, and the Law Enforcement Integrity Commission, where the legislation provides that a defendant <u>does not</u> bear any evidential onus in relation to establishing that they dealt with information for the purposes of providing the material to these bodies. This leads inescapably to the conclusion that the prosecution bears the onus in relation to all elements of the primary offence and so called "*defence*" – although the Criminal Code does not appear to make that explicit.[21] When it comes to questions of onus of proof, there can be no principled reason to distinguish these cases from cases where a person discloses material to the public as a journalist.

1.65 The correct approach is also reflected in the more recent offence in s 474.47(1) of the Criminal Code of using a carriage service to incite property damage or theft on agricultural land. Under s 474.47(2), that offence "*does not apply to material if the material relates to a news report, or current affairs report, that (a) is in the public interest: and (b) is made by a person working in a professional capacity as a journalist*." Again, a defendant does not bear an evidential onus in a prosecution under this section and again the inescapable conclusion is that the prosecution must discharge the usual criminal onus. There is no principled basis to distinguish the operation of this more recent journalist protection from the other existing protections contained in Division 122 of the same criminal code.

1.66 These matters all compellingly speak to the need for any statutory journalist protection <u>to not impose either an evidential or legal onus on an accused.</u>

---

[19] *7 February 2018 Scrutiny Digest,* 84-88 [1.276]-[1.286]; Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 4 of 2018, 28 March 2018), 21-28 [2.35]-[2.54].
[20] See, in particular, Senate, Parliament of Australia, *Standing Order 24* (15 July 2014), 24(1)(a).
[21] Criminal Code s 122.5(3), (12).

1.67 As a concluding comment, ARTK notes the missed opportunity for raising evidential onus in the Consultation Paper for any evaluative discussion. The terms of reference make specific reference to considering the suitability and framing of general and specific secrecy offences having regard to the principles set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers.* However, serious concerns about the compatibility of the existing Division 122 "*defences*" have been expressed by the Scrutiny of Bills Committee, which means there is particular importance in the Commonwealth reaching a balanced and considered view on this issue that appropriately protects the basic human rights of accused persons.

Journalist protections must cover all disclosure offences

1.68 No reasons have been advanced for why a journalist protection, subject to the limited exceptions now provided for in Division 122 to that protection, is not appropriate for each and every disclosure offence created by Commonwealth law. The public interest is the Australian public being meaningfully informed of the behavior of its own government applies to each and every instance where disclosure of government information is criminalised.

PRINCIPLE TWO: Any criminal sanction must require an intention to cause harm to a recognisable public interest

1.69 For the reasons to be given in relation to Principle Three, criminal laws dealing with the disclosure of government information must be confined to disclosures which cause serious harm to a clearly identified public interest.

1.70 Such offences must also have, as their fault element, an intention to cause that harm.

1.71 Recklessness, in contrast, is not the appropriate standard.

1.72 Recklessness, for the purposes of all Commonwealth offences, is defined this way:[22]

> *(1) A person is reckless with respect to a circumstance if:*
>
> *(a) he or she is aware of a substantial risk that the circumstance exists or will exists; and*
>
> *(b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.*
>
> *(2) A person is reckless with respect to a result if:*

[22] Criminal Code s 5.4.

(a) he or she is aware of a substantial risk that the result will occur; and

(b) having regard to the circumstances known to him or her, it is unjustified to take the risk.

(3) The question whether taking the risk is unjustifiable is one of fact.

1.73 Applied to a prospective resultant harm, the first limb is actual subjective knowledge of a "*substantial risk*" that a result will ensue.

1.74 Any person disclosing information would be alive to a vast range of possibilities in life. Furthermore, the nature of the harms that might be occasioned to government interests are not only many and varied but also contestable. But under this formulation, a person who simply countenances a real or substantial risk that X may result from their disclosure will satisfy the first limb and would face a meaningful risk of prosecution, even though they may be countenancing possibilities Y and Z at the same time and indeed may consider those other possibilities more likely. The person faces a meaningful risk of prosecution because countenancing that risk would satisfy one of the two key elements of the recklessness test. The remaining amorphous question of whether it was "*unjustifiable*" to take the risk that disclosure would cause X is something a prosecutor could quite easily take to jury or magistrate to resolve.

1.75 However, when a person deals with government there is often no way for a person to confirm or discount any suspicions that they happen to be holding. This is because the invariable practice of government is not to comment when asked to confirm a suspicion – particularly in relation to national security or law enforcement matters.[23] It is however unfair to subject a person to a meaningful risk of criminal prosecution for holding a suspicion about matter X, when the person supposedly aggrieved if X were to happen refuses to confirm or deny whether X is in fact going to happen. In these scenarios, it is government's refusal to engage and answer a reasonable question which is the real driver of harm.

1.76 Subjecting members of the community to a meaningful risk of criminal liability simply for countenancing a real risk that government itself refuses to confirm or deny also creates a "chilling effect" – legitimate discussion about the actions of government will be suppressed in all cases where the fact that the disclosure may have some kind of adverse effect on some kind of recognisable governmental interest cannot, in substance, be ruled out.

[23] The Hon. Roger Gyles AO QC, Independent National Security Legislation Monitor, *Report on the impact on journalists of section 35P of the ASIO Act* (October 2015), 12-13, in particular [15].

1.77 It is useful to illustrate these points. Sadly, the scenario is based, with some minor changes, on the true facts of the Sheraton Hotel incident.

1.78 An intelligence agency stages a plain clothes exercise in a major hotel in the Melbourne CBD. The offices seek to physically force access to a hotel room. Guests are terrified and call the manager. The manager confronts the intruders. He is manhandled into a lift. The intelligence officers then make a disorderly exit through the hotel's lobby and kitchen. They brandish weapons in front of guests and staff.[24]

1.79 Say the hotel manager considers it a real possibility that the intruders are from the intelligence services and appreciates that any immediate disclosure to the police could compromise an in-progress intelligence operation. Is it to be contended that this subjective awareness should put the manager, if he were to call the police, at meaningful risk of prosecution, even though it was more likely that the intruders were *pretending* to be conducting intelligence service operation to stage a burglary from a hotel room? Is it to be contended that the manager should be placed at risk of having to explain to a jury or a magistrate, why he thought it was "*reasonable*" to make a disclosure to police?

PRINCIPLE THREE: There must be clear, meaningful and serious harm to a recognisable public interest, and any criminal sanction must be proportional to address that harm

1.80 An essential integer to the proposition that criminal liability should only be imposed where the disclosure of information causes serious harm to a clearly identified public interest is that the extent of liability, i.e. the sanction, is proportional to the harm identified.

1.81 This reflects a broader requirement that applies to all offending: criminal sanction in this and all other contexts must be reserved only for the most serious behaviours which cause clear, meaningful and serious harm to a recognisable public interest. Taking away a person's freedom, the suspension of a person's other social and political rights upon incarceration or conviction, and the lifelong stigma and other legal and economic consequences of a criminal conviction are society's most serious sanctions and can only be appropriate when the community's recognised interests have been appreciably damaged by a person's behaviour. The fact that behaviour may cause offence or embarrassment to others – and in particular to those in government or the public service – can never justify a member of the community being jailed or threatened with prosecution. The use of criminal sanction must also be a proportionate and appropriate response to any harm.

[24] *A v Hayden (No 2)* (1984) 156 CLR 532, 539-540.

1.82 These considerations are sharpened when it comes to offences dealing with the disclosure of government information, which raise two additional matters of principle.

1.83 First, as discussed in relation to Principle One, there is an overriding, democracy reinforcing public interest in ensuring that the Australian people are meaningfully informed of the actions of their government. That requires, for the reasons given, journalist protections which allow for the disclosure of information by journalists which may cause, in the short term, damage to particular public interests. This is because such disclosures by journalists are directed to ensuring the proper functioning of democracy and the integrity of the system for making collective decisions as a nation. This means that, at least in relation to journalists, the existence of real harm to some form of public interest is a necessary but not sufficient condition for establishing criminal liability.

1.84 Secondly, the fact that information held by the Australian government is owned by the Australian people and that there are very compelling public policy reasons to ensure transparency and accountability of government means that particular care must be applied to recognising the kinds of public interests that would warrant protection, and in assessing whether a criminal law sanction is appropriate and proportional to preventing or addressing harm to those public interests. Ultimately, a public interest that is recognised as sufficient for these purposes has to be a public interest that is appropriate to protect under a liberal democratic framework that recognises the inherent need for open and transparent government and broader public accountability.

1.85 Where a criminal law does not protect a public interest of this character, or where a criminal law response is disproportionate and inappropriate to any harm caused, the broader public interest suffers. This happens in one of three ways:

(a) Fundamentally, trust and confidence in government suffers. Obvious government overreach is enough to damage public confidence in government and public administration. “David vs Goliath” struggles between the Commonwealth and individual members of the community such as lawyers, journalists, or whistleblowing public servants are repellant and offensive to basic concepts of fair play and treatment.

(b) The administration of justice also suffers when already limited policing, prosecutorial and court resources are misdirected from dealing with ‘core’ business like the detection and prosecution of violent and other serious offences into marginal and seemingly political prosecutions of journalists, public servants or members of society.

(c) Public administration also suffers when a broad swathe of conduct of public servants is criminalised. This is because internal disciplinary inquiries should properly be put on

hold pending the resolution of any parallel criminal investigation by police, which may take months or years.[25] To do otherwise could compromise a police investigation or trial by interfering with the chain of custody of key evidence and records and by compromising testamentary evidence through lines of questioning that are inappropriate in a criminal context and which may "contaminate" testimony.[26] In any case, proceeding with a disciplinary inquiry into the same subject area covered by an offense risks compromising a subsequent criminal investigation and trial and undermines the very point of having an offense in the first place. This means that public servants who have in fact committed disciplinary violations which have a criminal element either remain in positions of trust for extended periods of time, or will be placed on suspension, often at full pay, with government having no ability to permanently back-fill the position while police inquiries are ongoing. The proper operations of government is placed into extended limbo. The broader the scope of potential criminal liability, the worse this problem becomes.

1.86 In the context of disclosure offences, trust in government suffers in particular where inappropriately broad secrecy laws are then selectively and inconsistently applied, particularly where the reasons for investigation are seen as politically motivated and directed to the punishment of perceived critics of government or the discovery, at all costs, of anonymous critics expressing criticisms through the media. These practices suggest a "weaponisation" of secrecy laws as a tool to suppress criticism by intimidation. Ultimately it is government, including law enforcement, that lose public standing and public trust through this behaviour, and with that, the ability to carry out its functions in the public interest.

1.87 While such an approach undermines the standing and authority of government domestically, the apparent focus on punishing critics of government also undermines Australia internationally, particularly in forums where Australia seeks a leadership role to promote an international rules-based order so as to promote its national interests.

---

[25] Indeed, there is the potential for potential criminal accused to seek injunctions staying an internal disciplinary proceeding undertaken under public service legislation – see *Bannister & Ors v DG Department of Corrective Services* [2002] QSC 469. See also Australian Public Service Commission, *Handling Misconduct – A human resource manager's guide* (Circulars, Guidance, and Advice, 1 February 2022), [10.11].

[26] The issue crystalises most clearly where the earlier compulsive process exercises compulsive powers or effective powers of compulsion, but is not limited to those cases – for example, cases of contamination of testimony. The issue is rarely litigated because, axiomatically, a trial cannot proceed because of the compromised state of the evidence, and is usually litigated in the context of seeking stays to disciplinary action – see, as examples, *Herron v McGregor* (1986) 6 NSWLR 246 at 266, *Bannister & Ors v DG Department of Corrective Services* [2002] QSC 469, *Hurley v Newton* [2020] QDC 49.

1.88 Threatening to jail journalists and others who highlight government wrongdoing is bad diplomacy for a liberal democracy. It undermines the trust of liberal democratic allies and needlessly gives ammunition to foreign critics. Indeed, the use of secrecy laws to suppress or withhold information of legitimate public interest that does not harm national security, or to prosecute journalists, researchers, environmental activists, human rights defenders or others for disseminating such information, has already been recognised by the United Nations as a breach of the right to freedom of expression guaranteed by article 19 of the International Covenant of the Civil and Political Rights.[27] This means that the continued failure to address overbroad secrecy laws needlessly exposes Australia to being brought before an international human rights body by an aggrieved citizen, or by an unfriendly state actor seeking to undermine the nation's standing internationally.

1.89 For all these reasons, the creation and enforcement – selective or otherwise – of inappropriately broad secrecy laws is itself damaging and does real harm to the community and national interest.

1.90 Once these principles are accepted, certain things follow for the current disclosure offences and the information categories they are said to protect.

Personal information

1.91 The nature of the personal information that is subject to criminal protections across the Commonwealth statute book will vary between statutory contexts. In most statutory contexts, the information is likely to be broadly innocuous. Nor is the threat that unauthorised disclosure will impede the future supply of information to government likely to be either material, or otherwise sufficiently serious to justify criminal penalties as a proportional and appropriate response.

1.92 In these cases, it is very difficult to see why a framework for the management of personal information under a *Privacy Act 1988* (Cth) (**Privacy Act**) style framework is not the appropriate and sole form of regulation.

1.93 Even in more serious cases, where more tangible damage results to an individual from a disclosure, a Privacy Act regime seems more appropriate to dealing with disclosures. This is because by far the largest number of disclosures are likely to be inadvertent: principally through data breaches that result from poor cybersecurity management. The real issue in these cases is whether the entity holding the targeted information (government or private sector) has put in place appropriate systems

[27] Human Rights Committee, *General Comment No 34: Article 19: Freedoms of opinion and expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011), [30].

for the safe management of its information assets, which is already dealt with in the Privacy Act.[28] An overlapping criminal offence adds nothing.

1.94 It appears that many earlier secrecy offences that pre-dated the introduction of the Privacy Act (or which post-date the Privacy Act, but which uncritically and reflexively adopted pre-Privacy Act legislative templates) were intended to protect personal information and business information collected by government.[29] Such offences should have been repealed (or should never have been introduced – if passed after the Privacy Act) once the Privacy Act introduced a bespoke and better targeted regime to address the same policy concerns.

1.95 In fact, the existence of overlapping criminal offenses covering disclosures that are already regulated by the Privacy Act in fact undermines the administration of the Privacy Act. This is because the conduct of investigations into Privacy Act contraventions that focus on internal systems and processes will be complicated and potentially compromised when a parallel criminal investigation by police investigates the same conduct, as the police investigation must take precedence to any Privacy Act inquiry for the reasons discussed at paragraph 1.87(c) above.

1.96 Finally, a criminalised prohibition on the disclosure of personal information does not stop the misuse of personal information: only the unauthorised disclosure of personal information. This is because most criminal offences contain exceptions for disclosures authorised by the Agency concerned in purported pursuance of its statutory roles and functions.[30] So where a senior government official wishes to disclose personal information for reasons which include malice, the desire to inflict retribution on internal or external critics, or to discourage future critics with the implied threat of similar retribution in future, that senior official may do so with apparent impunity. This is because no apparent offence would be committed because that officer would be making an authorised disclosure apparently carried out in accordance with the statute (therefore receiving, for example, the benefit of the "*defence*" in s 122.5(1)(a) of the Criminal Code which provides that it is a defence where a person makes the disclosure, when "*exercising a power, or performing a duty, in the person's capacity as a public official*"). It is not credible to suggest that any prosecutor would proceed in a case where a person is apparently exercising a power or performing a duty but where the existence of bad faith may render that exercise of power or function a legal nullity.

[28] *Privacy Act 1988* (Cth), Australian Privacy Principle 11.
[29] John McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 Federal Law Review 49, 49.
[30] See for example Criminal Code s 122.5(1)(a); *Australian Security Intelligence Organisation Act 1979* (Cth), s 18(1)(d); *Intelligence Services Act 2001* (Cth) ss 39(1)(c), 39A(1)(c), 40(1)(c); *Surveillance Devices Act 2004* (Cth), s 45(4).

1.97 This means that secrecy provisions provide largely illusory protections to individual members of the public because, ultimately, all it takes is a senior person in government to purportedly authorise a disclosure of a person's personal information, regardless of whether that authorisation is a misuse of that information or otherwise an abuse of power.

Commercial information

1.98 In these cases, it cannot be assumed that any commercial interests would actually be compromised by disclosure, so no actual harm may ever eventuate. Where no harm results to either business in the community or the Commonwealth from a disclosure, criminal sanction can never be justified.

1.99 Nor, even in those rarer cases where commercial harm results to the Commonwealth or a third party, or the Commonwealth's interests are more indirectly affected because the disclosure may compromise the future flow of commercial information to government, could criminal sanction ever be the appropriate means to deal with disclosures that simply relate to business or commercial matters. No meaningful impact to the community that may legitimately engage a criminal law response – such as threats to life, health, or community safety – arise. The law does not otherwise criminalise behaviour which may simply damage business interests. That role is performed by the civil law. That is the appropriate forum for dealing with unauthorised disclosures of business information, coupled with internal disciplinary proceedings for any public servants at fault.

Confidential and other information

1.100 The fact that information either is, or once was, confidential, says nothing about whether its disclosure would compromise essential public interests. There is no public interest in the protection of information said to be "*confidential*" that warrants criminal sanction, particularly where, applying circular logic, the statute in question effectively deems information confidential and therefore 'bootstraps' the apparent public policy need to protect that information through criminal sanction.

1.101 Nor is it clear, even in cases where some form of specific kind of confidentiality breach may compromise some form of recognisable public interest, that criminal sanction could ever be appropriate and proportionate to addressing such harm. That is particularly so when there are other more targeted ways to enforce the confidence or to compensate for a breach of confidence, particularly civil law remedies for actionable breach of confidence or breach of contract. These remedies will actually restore the person adversely affected financially – which is a more suitable vindication for that person than a criminal prosecution of the public servant involved – and will place a greater incentive on agencies to appropriately manage their information holdings because of the

financial sanction borne by the Agency when its officers mishandle the business information of third parties.

Law enforcement information

1.102 Disclosure of information which is about law enforcement does not compromise law enforcement. Therefore, any disclosure of material that simply relates to the activities of a law enforcement body, no matter how innocuous that information is and no matter how unrelated it may to actual criminal investigations, cannot by and of itself damage any recognisable public interest.

1.103 It may be argued that the need to maintain internal discipline within a police force justifies criminal penalties for breaches of internal police confidentiality. That argument does not hold. There is no principled reason to say why internal duties of confidentiality and not other duties imposed on police by the internal disciplinary framework should be the subject of criminal and not simply disciplinary sanction. Under the policing internal disciplinary framework, police are instructed not to discriminate, not to abuse their position, and to declare and manage conflicts of interest between their personal position and professional duties.[31] None of these critical duties imposed by the disciplinary framework are criminalised. There is no logical reason to single out confidentiality and treat a breakdown of police discipline in that limited area as so serious a risk to police force integrity as to justify criminal sanction, and yet at the same time ignore, from a criminal law perspective, disciplinary breaches that have a far greater impact on the police's ability to discharge its functions and build and hold public trust and acceptance.

1.104 The Casey report into the Metropolitan Police gives a stark illustration of the kinds of behaviours that lead to the "*breaking*" of public consent in a police force.[32] The disclosure of information with a view to bringing misconduct to light is <u>not</u> one of those behaviours.

National security information

Similar considerations apply to national security information.

It is contrary to the rule of law for criminal convictions to depend on security classifications set under policy

[31] Australian Federal Police, *AFP Code of Conduct* (undated), accessible at https://www.afp.gov.au/about-us/our-organisation/professional-standards/afp-code-conduct. See further the *AFP National Guideline on conflicts of interest*, accessible at https://www.afp.gov.au/sites/default/files/PDF/IPS/AFP%20National%20Guideline%20on%20Conflicts%20of%20interest%2027AUG2012.pdf.

[32] Baroness Casey of Blackstock DBE CB, 'An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service' (Final Report, March 2023).

1.105 A problematic aspect of the current law is the criminalisation of disclosures which involve material that bears particular security markings.

1.106 Some critical points can be made about the current framework in "*Policy 8: Sensitive and classified information*".

1.107 The first is that there is no statutory framework which is applied in making decisions to classify documents. Instead, there seems to be an amorphous mass of agency policy where it could not be credibly contended that in respect of *each* classification decision there could ever be full compliance.

1.108 As policy materials, there has been no proper Parliamentary oversight of this material under the scrutiny principles that would be applied to the scrutiny of regulations.[33] As far as ARTK is aware, this means the current classification framework itself has not been credibly and independently assessed to ensure its compliance with basic democratic norms or to assess whether it achieves an appropriate balance between the public interest in transparency and any identifiable public interests favoring non-disclosure.

1.109 Further, under the policy framework, there is no recorded decision-maker (the duty to attach the classification rests with an unspecified "*originator*", which is in any case a meaningless concept where the material is first generated externally to government). There are no recorded reasons for decision. And there is no merits review and no judicial review.

1.110 This last issue has special importance in criminal trials.

1.111 In some cases (and potentially all), there does not appear to be any opportunity in a criminal trial to "*collaterally review*" the lawfulness of the original security classification decision made in relation to a stamped document. This is because there is no actual recorded "*decision-maker*" for that decision, because the reasons for decision are not recorded, and because the framework is wholly policy based – meaning there is no legal standard to apply. This means that the original classification may simply have been factually wrong, may have been demonstrably unreasonable, or may have proceeded on a fundamental misunderstanding of the relevant policy requirements, and none of that can be taken into account during a criminal trial where the mere fact that a document has been stamped must be taken as the relevant integer for establishing criminal guilt.[34]

1.112 It is inappropriate for criminal liability to attach in these cases. In no other context would it be suggested that the unreviewable, non-statutory decisions of unknown public servants – which could

[33] See Order 23 of Senate Standing Orders.
[34] See, for example, Criminal Code s 122.3(1).

be wrong in fact, misinterpret the policy that was purportedly applied, or which may no longer be current – could be used as the key integer to establish whether a person should be jailed. It is repellant to basic concepts of the rule of law and basic justice. It also compromises the existence of an independent judiciary which can command public trust and acceptance, which is conscripted into an exercise which simply serves simply to imprison people based on unreviewable executive fiat.

1.113 There are certain other offenses, such as those dealing with the disclosure of "*inherently harmful information*" in Criminal Code s 122.1, which suggest that whether or not a security classification "*has been applied in accordance with the policy framework*" is a matter that can be agitated in criminal trials. However:

(a) While the question for the court may be whether the document was correctly classified under a relevant policy, that is not clear on the face of the relevant s 90.5 of the Criminal Code. That is the more rights-protective reading and it is a matter of construction rather than being dealt with through clear drafting. The Commonwealth may, now or in the future, take the position that all that s 90.5 requires is proof that there was some mechanistic purported application of a relevant policy to the document in order to establish that a security classification was "*applied in accordance with the policy framework*", and that a broader role for the tribunal of fact to assess whether the policy was correctly applied based on the facts and circumstances known to the putative (but probably unknown) classifier is not contemplated by the legislation. This may even be the better argument. If this view is ever upheld, then the law is unacceptable from a rule of law and judicial independence perspective for the reasons just given.

(b) Even if some degree of review of the underlying classification decision was permitted, the Court is not permitted to evaluate for itself whether the relevant security classifications under the policy correctly identify real and not perceived national security threats. The role of the court is confined to only looking at whether the document has been applied in accordance with whatever formula is set by policy from time to time.

(c) Even if some degree of effective review of the underlying classification decision was permitted, the fact that the original administrative decision to classify a document is based on national security information would make any attempt to collaterally review the underlying classification decision practically impossible. In any prosecution alleging the disclosure of a classified document, the Commonwealth would refuse to divulge the material relied on in making the original classification decision (assuming that material could be found), leading to further and seemingly insoluble issues of how to maintain a fair hearing that is credible and transparent

when the prosecution attempts to keep critical evidence away from the defendant.[35] It is hard to see how, in these circumstances, a fair hearing could ever be given to the accused.

(d) Even if some degree of effective review of the underlying classification decision was permitted, the apparent statutory question is whether the classification was correctly applied at the time it was applied, not whether it remained *correctly applied at the time of disclosure or other form of relevant dealing*. Nor are there any firm requirements under the policy regarding the "*declassification*", "*reclassification*" (to a lower security classification) or "*sanitising*" of documents, and no guarantee that these seemingly aspirational requirements are met in practice. There is no assurance that even if the original marking was correctly applied, the marking remains appropriate at the time a document is disclosed and that any actual harm may have resulted from the dealing or disclosure. The document may have become purely innocuous, noting the offence could potentially apply to the air defence plans for Darwin from 1942.

(e) There are no means for a criminal defendant to know, in advance of a relevant "*dealing*" or "*disclosure*", whether any security marking was in fact applied "*in accordance with the policy framework*". A person, when confronted with a document marked "*secret*" or "*top secret*" must assume that disclosure will result in criminal liability even if the mark was not correctly applied. That impermissibly chills speech and effectively broadens the offence to the disclosure of any document that happens to bear a purported marking.

1.114 Underscoring these difficulties is the fact that the Australian public can have little confidence about security marking decisions being reasonable and appropriate.

1.115 As one key example, the security classified material alleged to have been published by Annika Smethurst in the matter that led to the subsequent unlawful police raids and abandoned criminal investigation was alleged to contain "*secret*" and "*top secret*" marks. Under the policy framework, a "*top secret*" marking is only appropriate where there is "*catastrophic business impact, or exceptionally grave damage to the national interest, organisations or individuals*", and a "*secret*" marking is only appropriate where there is "*extreme business impact"* or *"serious damage to the national interest, organisations, or individuals*".[36]

[35] See, generally, NSI (CCPA) Act.
[36] Attorney-General's Department, *Protective Security and Policy Framework, Policy 8: Sensitive and classified information* (28 September 2018) accessible at https://www.protectivesecurity.gov.au/system/files/2023-01/pspf-policy-08-sensitive-and-classified-information.pdf, 2; 7-8.

1.116 Ms Smethurst's article related to a law reform proposal within government and ultimately suggested a power play between competing factions within the security establishment. The fact that the information was allegedly leaked was embarrassing to the senior figures involved may have given rise to a suggestion that the story, if it was in fact leaked, was leaked to further the position of a group involved in those same disputes within government who opposed the measures.[37] But on no rational basis could the information contained in Ms Smethurst's article justify a "*secret*" or "*top secret*" marking under the existing policy. In no way could disclosure of this information be said to have a "*catastrophic*" impact or cause "*serious damage to the national interest*".

1.117 If nothing else, this exposes the ultimate vice behind such schemes, namely that it is inherent human nature to conflate personal and institutional interest with the national interest.

Need for some meaningful damage to a recognisable public interest

1.118 The bare fact that information has some connection to national security does not mean that disclosure of information compromises national security. Disclosure offences should not cover every piece of information held by a national security organisation. Such information may be wholly innocuous, may be completely unrelated to actual intelligence gathering or operational activities, or may otherwise be incapable of harming investigations if disclosed publicly.

1.119 Specifically, it is not appropriate to criminalise disclosures that simply reveal "*operations, capabilities or technologies of, or methods or sources used by*" security or law enforcement.[38] None of these matters, if disclosed, have any necessary impact on the conduct of investigations.

Innocuous disclosures do not compromise future intelligence sharing

1.120 Nor is there any reason to suggest that criminalising the disclosure of innocuous material from security agencies would compromise intelligence sharing between governments.

1.121 The other Five Eyes security partners do not have secrecy laws such as those currently in Australia. Such laws are not possible in the United States given constitutional protections concerning free speech and a free press. Such laws are also highly problematic in the United Kingdom, Canada and New Zealand because of statutory human rights instruments which entrench similar human rights standards. The failure of Australia to maintain secrecy laws of a type which do not exist and which

[37] Annika Smethurst, 'Spying shock: Shades of Big Brother as cyber-security vision comes to light', *The Daily Telegraph* (online, 29 April 2018) <https://www.dailytelegraph.com.au/news/nsw/spying-shock-shades-of-big-brother-as-cybersecurity-vision-comes-to-light/news-story/bc02f35f23fa104b139160906f2ae709>.
[38] Criminal Code ss 122.1(1), 121.1 definition of "*inherently harmful information*".

could never exist in these partner countries could therefore have no bearing on Australia's perceived status as a "*reliable*" intelligence partner.

1.122 Rather than be concerned by a failure to prosecute a journalist or junior public servant whose disclosures do not in any way risk compromising intelligence activities, the likely expectation of security partners instead would be that Australia focus efforts and resources on the protection of operationally sensitive information of actual significance to intelligence activities.

1.123 Foreign security partners are more likely to have been alarmed, for example, by the "*Cabinet files*" scandal where – for which no person has ever been held publicly to account, and for which no public explanation has ever been given – highly sensitive security documents relating to the national security deliberations of Cabinet and operational intelligence matters were left in a locked filing cabinet which was then sold by the Department of Premier and Cabinet to a used furniture shop. A further irony was that the abandoned files disclosed that, between 2008 and 2013, the Australian Federal Police alone "*lost*" nearly 400 national security files, and that the security practices of the Cabinet Secretariat were so lax that its general practice was to *"give up searching and write off lost documents*" if they could not be located after repeated attempts.[39]

1.124 Ultimately, the system failures illustrated by this incident are likely to be of greater concern to foreign partners because it spoke to a broader failure of systems and processes for the effective management of security information. The point may be as simple as this: if the government wants to protect its national security information and is concerned that a failure to do so could jeopardise intelligence sharing, government should protect its information by making the right investments in information protection systems and training. The focus on the criminal law is, at best, a distraction from the real issue.

Overly broad criminal secrecy laws do not provide meaningful deterrence for the most common forms of disclosure

1.125 As the "*Cabinet files*" incident shows, by far the greatest threat to the security of national security information is simple human error. But the fact is that the criminal law is not an apt tool for changing negligent behaviour. A criminal law simply cannot create general or specific deterrence for an

[39] Ashlynne McGhee and Michael McKinnon, 'The Cabinet Files reveal national security breaches, NBN negotiations, welfare reform plans', *ABC News* (online, 31 January 2018, last updated 10 February 2018) <https://www.abc.net.au/news/2018-01-31/cabinet-files-reveal-inner-government-decisions/9168442>; Paul Karp, 'Cabinet documents: ABC reveals top secret files found in old filing cabinets', *The Guardian* (online, 31 January 2018) https://www.theguardian.com/media/2018/jan/31/cabinet-documents-abc-reveals-top-secret-files-found-in-old-filing-cabinets.

individual whose own inattention and lack of awareness means that they do not appreciate that they are doing anything wrong or are in fact committing a crime.

1.126 Ultimately, criminal secrecy laws, by failing to address the main area of risk when it comes to disclosure of security information, do little to make the community safer or more secure.

1.127 To the extent that disclosures are motivated by less than laudable goals, in particular the desire to assist a foreign government, then espionage charges are and should remain available. There is, however, nothing to suggest that those who deal with the media have such intentions.

1.128 Nor has any plausible justification been given to the assertion that journalists might become the targets of foreign powers and unwittingly used as some kind of 'fifth column' or 'trojan horse' to collect intelligence on its behalf.[40] If there is such a threat, the solution is for the intelligence services to do their jobs (and address what is claimed to be known), rather than demand that journalists cease doing their jobs.

Criminalising overly broad confidentiality duties undermines the disciplinary framework within security services and creates irresolvable problems for the administration of justice

1.129 Confidentiality is a critical part of the role of those who work in national security. It does not follow however that any duties of confidentiality imposed by an internal disciplinary framework should be criminalised.

1.130 Indeed, it is the pressing need for confidentiality which in fact suggests that such disclosures should not be criminalised. Where confidentiality and trustworthiness are inherent parts of a person's role within a national security agency, the national interest favors the speedy, prompt and immediate removal of a person from their position if they have violated a confidentiality duty. That can only be effected through a speedy disciplinary inquiry, which cannot occur if there are parallel police investigations which must proceed at a slower pace so as to maintain the integrity of evidence for a future criminal trial, as outlined at paragraph 1.85(c) above.

1.131 And assuming a police investigation is able to come to a conclusion, government then faces the vexing – and in no way satisfactorily resolved issue – of how to conduct a criminal trial which is fair and transparent while at the same time using national security evidence that must be kept secret.[41] This raises the specter, already realised in at least one case (the "*Witness J / Alan Johns*" prosecution) of

[40] Fergus Hunter, 'Foreign spies use journalism as cover, ASIO warns in press freedom inquiry', *Sydney Morning Herald* (online, 14 August 2019) https://www.smh.com.au/politics/federal/afp-commissioner-declines-to-rule-out-charges-for-news-corp-journalist-20190814-p52gw4.html.
[41] See, generally, *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) (**NSI (CCPA) Act**).

"*secret trials*" and "*secret prisoners*".[42] Cases like this bring the administration of justice as a whole into disrepute by violating key concepts of "*open justice*", which require the law be administered openly, fairly, and subject to public scrutiny. These "*open justice*" principles are the only effective means to avoid abuses of power within the judicial system and to maintain broader public trust and confidence in the administration of justice. Ultimately, "*secret prisoners*" and "*secret trials*" risks jeopardising the community's trust and confidence in the justice system itself, which is the bedrock upon which the community's acceptance of the laws is based and vital to maintaining social cohesion and order.

[42] Grant Donaldson, *Review into the operation of Part 3, Division 1 of the National Security Information (Criminal and Civil Proceedings) Act 2004 as it applies in the Alan Johns matter* (4th Independent National Security Legislation Monitor, 17 June 2022), accessible at https://www.inslm.gov.au/sites/default/files/2022-07/nsi-report-4thinslm-17june-2022.pdf.

Question Two: Having regard to these principles, are there any general or specific offences that should be amended or repealed?

Yes.

NECESSARY AMENDMENTS TO DIVISION 122 OF THE CRIMINAL CODE

Offences for various dealings with "inherently harmful material": Expression too broad – Criminal Code ss 122.1(1), (2),(3),(4)

2.1 All offences relate to disclosure or use of "*inherently harmful material*". This expression, as defined under s 121.1(1), is too broad:

(a) The definition covers "*security information*", defined ultimately under s 90.5 to mean material with "*a classification of secret or top secret that is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes which include the purpose) of identifying information (i) for a classification of secret …. (ii) for a classification of top secret ….; or (b) any equivalent classification or markings prescribed by the regulations".* Under this definition, the only matter which may be tested in a prosecution is whether the classification was applied under the policy, not whether its retention was consistent with the policy at the time of disclosure, and not whether the policy being applied is actually directed to identifying specific instances of specific actual harm to national security interests. As such, this offence is not actually targeted to identifying cases where meaningful and actual harm to national defence or security is caused or threatened by disclosure. The material in fact may be completely innocuous, but remain the subject of an out of date classification. Alternatively, the policy may not in fact target the classification decision sufficiently to areas or issues where an actual, appreciable risk to the national interest actually arises.

(b) The definition covers "*information that was obtained by, or made on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions*". This simply covers all information held by such organisations, including wholly innocuous information of no operational significance. Indeed, in relation to foreign intelligence organisations, the release of such information may well be permitted under their own domestic laws. Again, the offence is not actually targeted to identifying instances of specific, actual harm to national security interests from disclosure. Nor, for the reasons given at paragraphs 1.120 to 1.124, can the disclosure of wholly innocuous material from a domestic intelligence agency create a meaningful risk to intelligence sharing or compromise internal agency discipline to a degree that warrants the imposition of criminal sanction.

(c) The definition covers "*information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency*". No actual damage necessarily results from disclosure of any of this information: the information may be so general as to in no way risk actual operational activities or otherwise cause meaningful harm. There is a compelling public interest in the Australian public having at least a general awareness of these matters, particularly in relation to domestic law enforcement agencies, as that is relevant to collective judgments to be made about the appropriateness of current law enforcement arrangements.

Amend the fault element from recklessness to intention

2.2 The fault element for whether information is in fact "*inherently harmful information"* is recklessness.[43] For the reasons given in relation to Principle Two, the fault element should be intention, noting in particular the current 'no comment' policies by Commonwealth agencies in relation to most of the matters dealt with in the definition of "*inherently harmful material".*[44]

Conduct causing harm to Australia's interests: Expression too broad – Criminal Code ss 122.2(1) – (4)

2.3 All offences relate to disclosure or use of information that will "*cause harm to Australia's interests*". This includes cases under the relevant definition in s 121.1 where disclosure may "*harm or prejudice the security or defence of Australia*." The concept of the "*security or defence of Australia*" is defined to include "*the operations, capabilities or technologies, or methods or sources used by, domestic or foreign intelligence agencies*". That definition is overbroad and in the nature of a deeming provision: disclosure of these matters, particularly at a high level of generality, does not necessarily lead to any meaningful or actual harm to national defence or security is caused or threatened by disclosure. The material in fact may be completely innocuous, and in fact the Australian public has a clear right to know many of these matters at a higher level of generality. As such, by use of this deeming provision, there will be occasions where no real and meaningful harm from disclosure will eventuate from criminalised activity.

2.4 The fault element for causing such harm appears to be recklessness, although legislatives notes do not make that clear.[45] For the reasons given in relation to Principle Two, the fault element should be intention, noting in particular the current 'no comment' policies by Commonwealth agencies in relation to most of the matters dealt with in the definition of "*cause harm to Australia's interests*".

[43] See Criminal Code ss 122.1(1) Note 2, 122.1(2) Note 2, 122.1(3) Note 2
[44] Criminal Code s 121.1.
[45] See Criminal Code s 5.6(2)

Dealings with information subject to a "duty not to disclose" – Criminal Code s 122.4

2.5 This offence applies whenever there is a "*duty not to disclose the information*" which "*arises under Commonwealth law*". This offence is impermissibly broad, as it coverers information of the sort where no meaningful risk to a public interest of sufficient importance to warrant criminal sanction, for the reasons outlined in relation to Principle Three above.

2.6 This section should not be reenacted after it sunsets.

Communications and dealings with information by non-Commonwealth officers – Criminal Code s 122.4A

2.7 This offence requires a third party to government to communicate material obtained from a Commonwealth officer or who was otherwise engaged to perform work for the Commonwealth, in one of five circumstances, including where the information "*has a security classification of secret or top secret*".[46]

2.8 The definition covers "*security classified information*", defined ultimately under s 90.5 to mean material with "*a classification of secret or top secret that is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes which include the purpose) of identifying information (i) for a classification of secret …. (ii) for a classification of top secret ….; or (b) any equivalent classification or markings prescribed by the regulations".* Under this definition, the only matter which may be tested in a prosecution is whether the classification was applied under the policy, not whether its retention was consistent with the policy at the time of disclosure, and not whether the policy being applied is actually directed to identifying specific instances of specific actual harm to national security interests.

2.9 As such, this offence is not actually targeted to identifying cases where meaningful and actual harm to national defence or security is caused or threatened by disclosure. The material in fact may be completely innocuous but remain the subject of an out of date classification. Or the policy may not in fact target the classification decision sufficiently to areas or issues where an actual, appreciable risk to the national interest actually arises. As such, this offence is not directed to dealing with disclosures that cause real harm to any identified public interest. Indeed, if the information actually causes damage to security or defence of the country, that is already covered by the separate limb of this offence in s 122.4A(d)(ii).

2.10 If there is any policy justification for criminalising disclosure of documents bearing security classifications at all (which ARTK submits is not the case – see paragraphs 1.105 to 1.117), such a

[46] See Criminal Code s 122.4A(d)(ii)

policy does not apply to disclosures by third parties to government, such as the persons subject to liability under this offence. For these reasons, and reflecting the general principles outlined at 1.105 to 1.117 and 2.1 above, reliance on a document bearing a security classification should not be an integer of this offence.

2.11 The fault element for causing the harms set out in s 122.4A(d) is recklessness.[47] For the reasons given in relation to Principle Two, the fault element should be intention, noting in particular the current 'no comment' policies by Commonwealth agencies in relation to most of the matters dealt with in the list of matters set out in s 122.4A(1)(d), in particular in relation to defence and national security.

DEFENCES UNDER DIVISION 122

Journalist defence – s 122.5(6)

2.12 For the reasons given at paragraphs 1.37 to 1.67 above and below, there should be no evidential onus on the defendant. This protection should instead be framed as a "*negative element*" of the offence.

2.13 For the reasons given at paragraphs 1.20 to 1.23 above and below, the defendant should only be required to establish a bone fide belief by the journalist in question that engaging in the conduct in question was in the public interest, not "*reasonable grounds*" for that belief.

2.14 The existing limits on this defence set out in s 122.5(7) are appropriate.

Legal advice defence, public interest disclosure defence – ss 122.5(4)(a), (5A)

2.15 For the reasons given at paragraphs 1.37 to 1.67 above and below, there should be no evidential onus on the defendant. This protection should instead be framed as a "*negative element*" of the offence.

Accessorial liability under Division 122 of the Criminal Code

2.16 Div 122 of the Criminal Code creates a distinction between offences where the offender is or was a "*commonwealth officer*" or is "*otherwise engaged to perform work for a commonwealth entity*" (ss 122.1, 122.2, 122.3) and offences which are engaged in more limited circumstances committed by persons who have obtained information from such persons (s 122.4A).

2.17 That intentional delineation and limitation of criminal liability is rendered superfluous when a journalist who obtains information from a person alleged to have engaged in an offence under s 122.1, 122.2, 122.3 is tried as an accessory to that person's offending, which requires the court to establish the existence of the primary, broader offences with certain additional elements.[48] As the

[47] See s 122.4A Note 2
[48] See Criminal Code s 11.2

very nature of offending under s 122.3 is to procure an offence under ss 122.1, 122.2 and 122.3, the existence of accessorial liability for these offences exists in all cases and renders illusory the specific limits on criminal liability imposed on journalists and others under s 122.4A. For these reasons, accessorial liability should not be available.

NECESSARY AMENDMENTS TO OTHER COMMONWEALTH LEGISLATION

The following pieces of legislation raise particular issues:

***Australian Border Force Act 1997* – s 42**

2.18 The concept of protected "*immigration and border protection information*" is too broad and extends to commercial and business information. The balance of this material should be able to be disclosed to further legitimate journalism and journalist protections are appropriate in relation to any potential accessorial liability, noting in particular the overlap between the matters protected by the concept of "*immigration and border protection information*" and the matters now dealt with in Criminal Code ss 122.2(1), (2), (3) and (4) and the concept of *"causes harm to Australian interests",* which are all subject to the current journalist protection in s 122.5(6).

Australian Crime Commission Act 2002

2.19 Offences are generally overbroad in that secrecy in relation to notices and hearings may not be necessary to ensure the integrity of hearings or to protect other vital interests such as the safety of witnesses (non-publication can be directed to protect reputation, for example). Offences which criminalise any disclosures from law enforcement per se are bad in principle – see paragraphs 1.102 to 1.104 above.

2.20 In any case, the material should be able to be disclosed to further legitimate journalism. Journalist protections are appropriate in relation to any potential accessorial liability, noting in particular the conceptual overlap between the information covered by these offences and sub-paragraph (e) of the definition of "*inherently harmful information*" used in the offences at ss 122.1(1), (2), (3) and (4) of the Criminal Code, which are subject to the current journalist protection in s 122.5(6).

***Australian Federal Police Act* – ss 40ZA, 60A**

2.21 The offences are overbroad as they criminalise disclosure of any information in relation to certain investigations (for non-officers) and any disclosures from others (officers), regardless of the operational effect or other concrete damage that disclosure may have. This breadth is unacceptable for the reasons given previously in this submission.

2.22 Further, offences which criminalise any disclosures from law enforcement per se are bad in principle – see paragraphs 1.102 to 1.104 above.

2.23 In any case, the material should be able to be disclosed to further legitimate journalism and journalist protections are appropriate in relation to any potential accessorial liability, noting in particular the conceptual overlap between the information covered by these offences and sub-paragraph (e) of the definition of "*inherently harmful information*" used in the offences at ss 122.1(1), (2), (3) and (4) of the Criminal Code, which are subject to the current journalist protection in s 122.5(6).

***Australian Security Intelligence Organisation Act 1979* – ss 18(2), 18A, 18B, 81, 35P esp 35P(2) & 35P (2A)**

2.24 These offences are overbroad. Sections 18(2), 18A, 18B, 81 all relate to all information held by the organisation, regardless of whether disclosure or other use may compromise investigations or operations. For the reasons given above at paragraphs 1.102 to 1.104 it is wrong in principle to criminalise the disclosure of all information that simply relates to a law enforcement or intelligence agency.

2.25 Section 35P, in particular ss 35P(2) and (2A), are too broad. They criminalise, on a recklessness standard only, disclosures of information "*relating*" to a "*special intelligence operation*" where certain other conditions are met. For the reasons set out in relation to Principle Two, the intention element should be intention and not recklessness. The recklessness standard in this particular application is problematic for public interest journalism given the inherent risk that reporting, in good faith, matters of public importance may be said to be "*reckless*" in causing prejudice to the effective conduct of a special intelligence operation.

2.26 These provisions all potentially relate to newsworthy information where publication serves an essential public interest, and journalist protections are appropriate for any direct and accessorial liability under these offences, noting in particular:

(a) the conceptual overlap between the matters covered by these offenses and the matters dealt with in the Criminal Code concepts covered in Criminal Code s 122.4A(1)(c) and the concepts at

subparagraphs (c) and (e) of the definition of "*inherently harmful information*", where the relevant offences are already the subject of the journalist protection in s 122.5(6); and

(b) the existing journalist protection already is drafted to accommodates offence under s 92 of this legislation, which is an appropriate limitation on the existing journalist defence and which ARTK supports.

***Australian Transport Security Act* – s 74**

2.27 The offence provision itself appears appropriate, however the communication of threats to aviation security is a matter that is legitimately newsworthy and a journalist protection is appropriate to address any accessorial liability of a journalist engaging in bone fide reporting in the public interest (a test which will not be made out if the journalist reported in way which was demonstrably unreasonable and in a manner that could compromise aircraft security). A range of matters are criminalised by the regulations. A corresponding journalist protection is appropriate there also.

***Crimes Act 1914* – ss 15HK, 15JQ,15JR**

2.28 The offence relating to disclosure of information relating to controlled operations is overbroad and raises the same issues as the similar s 35P of the *Australian Security Intelligence Organisation Act 1979,* particularly were a journalist to be charged as an accessory to the primary "*entrusted person*" offences, where prejudice to the operation or risks to the health and safety of any person do not need to be established. As with s 35P, information pertaining to a controlled operation – which involves an authorisation to commit otherwise illegal conduct – is inherently newsworthy, and this too is a case where journalist protections are appropriate noting in particular the broad reach of the primary offences to journalists under principles of accessorial liability. Similar issues apply to integrity testing operations (s 15JQ and s 15JR).

***Criminal Code 1995* – Sched 1 s 91.1(2)**

2.29 The offence of being "*reckless*" as to national security is overbroad and has the capacity to apply to instances of legitimate good faith journalism, or to create a chilling effect in such cases, because the possibility of prejudice to national security will be known, raising the real prospect of criminal investigation, for much the same reasons as outlined in relation to Principle Two above in relation to the fault element for the s 122 secrecy offences. Information caught by this very broad provision may be intrinsically newsworthy and a journalist protection is required. There is little point in the current journalist protection in Division 122 if many of the same disclosures, to the extent they extend to security classified information, could be dealt with as espionage offences without a journalist protection. This renders the current protections largely illusory.

***Defence Act* – ss 73A, 90**

2.30 The offence in s 73A is overbroad. No damage to any national security interest may result from disclosure. No justification exists for the wholesale suppression of information relating to a particular government activity. That is particularly true where third parties such as journalists may be tried as accessories to the primary offending of defence force members and public servants. A journalist protection is warranted given the inherently newsworthy nature of the information captured: e.g. "*any document…relating to any defence work, or to any defences of the Commonwealth*".

2.31 Similar issues arise with s 90. It is wrong in principle to jail any person for breach of a confidentiality direction given by a court martial, particularly where none of the institutional protections to ensure open justice that apply in a court apply in a court martial and where information about the proceedings is intrinsically newsworthy. The offence should be repealed or at the least be the subject of a journalist protection.

***Defence Force Discipline Act 1982* – ss 58, 16**

2.32 While the offence in s 58 appears broadly appropriate in so far as it requires a disclosure likely to be prejudicial to the security or defence of Australia, a journalist protection is warranted to the extent that the offence may apply to journalist and other third parties on an accessorial basis, and the imposition of a legal onus on the defendant to make out the existing defence is also inappropriate.

2.33 Further, s 16 ("*communicating with the enemy*") is too broad in that it could theoretically apply to a service person communicating with a journalist to relay newsworthy information, which would then be relayed to "*the enemy*".

***Inspector-General of Intelligence and Security Act 1986* – s 34**

2.34 Section 34 is overbroad: for the reasons given above, it is improper to criminalise disclosure of all information relating to a particular law enforcement or similar entity, particularly where the offence could extend to journalists and other third parties under accessorial liability principles. A journalist protection is, again, appropriate.

***Intelligence Services Act 2001* – ss 39-41B**

2.35 The offences ins ss 39-41B and Sched 1 item 9 are overbroad. For the reasons given above, it is wrong in principle to criminalise the disclosure of any information that simply relates to a law enforcement or national security organisation, particularly where a journalist or third party may be criminally liable as an accessory said to "*procure*" the primary offence. A journalist protection in respect to any potential accessorial liability is appropriate, noting the overlap between the matters dealt with in these

offences and the criminalised disclosure under Division 122 of the Criminal Code of the material covered in (c) and (e) of the definition of "*inherently harmful information*", which is already the subject of journalist protections.

National Anti-Corruption Commission Act 2022

2.36 The offences in this Act are overbroad. They extend to criminalising the disclosure of information that includes substantiated findings of misconduct against government officials and contracted service providers who are to remain in office or otherwise engaged by the Commonwealth, and are otherwise directed to the suppression of information that merely embarrasses or has reputational consequences for the public servants or politicians in question. The legislation does not confine criminal secrecy requirements to disclosures that could genuinely prejudice an ongoing investigation and maintains criminalised secrecy duties after an investigation has concluded in an apparent attempt to maintain the reputations of those subject to adverse corruption findings. At the least, the disclosure of information about the operations of the NACC and any substantiated adverse findings are intrinsically newsworthy and should be the subject of journalist protections in respect to any accessorial or direct liability that may arise.

***Office of National Intelligence Act 2018* – ss 42, 44**

2.37 The offences in ss 42 and 44 are overbroad. For the reasons given above, it is wrong in principle to criminalise the disclosure of any information that simply relates to a law enforcement or national security organisation, particularly where a journalist or third party may be criminally liable as an accessory said to "*procure*" the primary offence. A journalist protection in respect to any potential accessorial liability is appropriate, noting the overlap between the matters dealt with in these offences and the criminalised disclosure under Division 122 of the Criminal Code of the material covered in (c) and (e) of the definition of "*inherently harmful information*", which is already the subject of journalist protections.

Question Three: Are there circumstances in which it is appropriate for a specific secrecy offence to prohibit conduct that is also prohibited by a general secrecy offence?

None identified. The question proceeds on the currently misplaced and patchwork approach to secrecy offences. If a principled approach of the type outlined above is adopted then the need for specific offences is largely eliminated.

3.1 ARTK notes that no public policy reason has been raised, and none exists, for why a statutory journalist protection should not apply to each and every Commonwealth criminalised disclosure prohibition. Provided this essential protection applies in relation to each and every Commonwealth non-disclosure offence, then the public interest in ensuring the Australian people are meaningfully informed of the conduct of its own government is protected. It would not centrally be to the point if the primary disclosure offences were contained in three provisions or over 800, as is currently so.

3.2 The current confused and incoherent patchwork of criminal laws is unworkable and demonstrates the caution required prior to adopting or continuing a legislative model based on specific circumstances. This absence of clarity about what a particular disclosure is in fact criminalised under a primary non-disclosure offence compromises public interest journalism.

3.3 One key difficulty arises because the existence of different criminal laws covering the same subject matter, all with different penalties, creates legal confusion as to which offence is legally operative given the principles that govern the implied repeal of older criminal offences by more recent offences relating to the same conduct, and related principles of double jeopardy.[49] This means that, confronted with the current statute book, no person – whether police, prosecutors, journalist sources, or the lawyers giving pre-publication advice to journalists – can have any confidence about whether what purports to be the law in fact is the law.

3.4 This problem underscores the unworkable complexity of the existing statute book arising from the existence of over 800 offences, where it is absurd to suggest that any lawyer – let alone a layperson – could be capable of making a legally informed assessment of whether proposed action is or is not actually criminalised. The incoherence, confusion, and needless technicality of the current statute book places a pall of risk and uncertainty over the disclosure of any government information and

[49] *See Hoffman v Chief of Army* (2004) 137 FCR 520 at [7] – [15] per Black CJ, Wilcox and Gyles JJ. Or as Issacs J put it in *Clyde Engineering v Cowburn* (1926) 37 CLR 466: *'If an Act of Parliament, for instance, prescribed 25 lashes for robbery under arms and a later Act prescribed that such an offender should be punished with 20 lashes, it could, of course, ... be said that both provisions **could** be obeyed, and therefore, applying the suggested test* [as to whether the two provisions were inconsistent]*, the offender must receive 45 lashes. But surely the vital question would be: Was the second Act on its true construction intended to cover the whole ground and, therefore, to supersede the first?'.*

makes definitive pre-publication legal advice to journalists very difficult if not impossible, which in turn has an obvious chilling effect on journalism.

3.5 Radical simplification, an across-the-board journalist, whistleblower and legal advice protection, and a clear, legislated hierarchy between any remaining criminal offence provisions to create a statute book which is clear and simple to administer and advise on are minimum requirements and should be the subject of urgent reform.

Question Four: Are there current defences for general secrecy offences available under section 122.5 of the Criminal Code appropriately framed? Are there any amendments or additions to these defences that should be considered?

No, the current defences are not appropriately framed and yes, amendments are necessary.

4.1 ARTK's views in relation to the journalist defence in s 122.5(6) are set out above in relation to Question One (as to high level principles) and Question Two above (as to amendments specifically required).

4.1 Section 122.5(4) provides a defence where relevant information is dealt with for the purposes of communicating it in accordance with the *Public Interest Disclosure Act 2013* (Cth) (**PID Act**).

4.2 It is unclear how this defence interacts with the immunity from criminal liability for the makers of "*public interest disclosures*" under s 10 of the PID Act. Both provisions purport to excuse behavior made in conformity with the PID Act for the purposes of the offences contained in Division 122 of the Criminal Code. But their respective ambits and operation – and whether the later s 122.5(4), by covering the same field covered by the earlier s 10 of the PID Act, actually effects an implied repeal of the PID Act – remain undetermined.

4.3 This again highlights an unacceptable level of internal inconsistency in the statute book, which makes providing clear pre-publication legal advice to journalists and their sources very difficult if not impossible.

4.4 More fundamentally, the PID Act regime does not work. The reasons for which are numerous and are matters that ARTK requests be explored and addressed in the second phase of the PID Act review and amendments foreshadowed by the Government. ARTK considers it preferable that the question of public interest disclosures to journalists be dealt with in the context of PID reform, where amendments which properly reflect the public interest in the Australian public being informed about the conduct of its own government are urgently needed.

4.5 Otherwise, the current defence concerning disclosures for the purpose of taking legal advice in s 122.5(5A) requires the following amendments:

(a) The protection must apply to all disclosure offences, not just contained in Part 122 of the Criminal Code. No justification has been given, and none exists, for why the disclosure of information to obtain legal advice should be protected in some contexts but not others.

(b) The onus of proof needs to rest on the prosecution, with no evidential onus sitting on the defendant. This is for broadly the same reasons outlined at paragraphs 1.37 to 1.67 above.

4.6 Apart from the matters identified above ARTK does not otherwise express any view on whether the existing Division 122 defences are or are not appropriate, but should not be taken to endorse the drafting of the existing provisions. In particular, the changes requested in relation to onus of proof questions in s 122.5(5A) and s 122.5(6) of the Criminal Code may logically require other amendments to the balance of the other defences.

Question Five: Are there any defences that should generally be available for specific secrecy offences? Are there any amendments or additions to defences for specific defences that should be considered?

5.1 The general defence with the amendments proposed above should be applied across the statute book. They should be included in Chapter 2 of the Criminal Code such that they are applicable to all Commonwealth laws, as per s 2.2, and should make clear their application to primary and secondary offending by journalists, the corporations that employ them and employees, servants and agents of those corporations who support and assist journalists in preparing news reports. Thus, subject to the proposed revisions to those defences set out above including in answer to Question 4, the defences now found in s 122.5(6) (journalists), s 122.5(4)(a) (public interest disclosures), and s 122.5(4A) (disclosures to lawyers) should be applied across the statute book to any remaining disclosure offences.

5.2 No policy reason has been given, and none exists, for why these protections should not be available wherever disclosures of government information are criminalised.

5.3 The Consultation Paper does not identify, explain or evaluate the over 800 offences on the current statute book, other than to list them. Most of these provisions should be repealed in full, leaving nothing to amend. It is otherwise unreasonable to expect any party participating in a six week consultation to have identify the discrete policy purposes of the over 800 criminal offences and to positively justify why each offence should contain protections of type currently set out in Division 122 of the Criminal Code. Further, it is unreasonable to seek to speculatively preempt the arguments that may be raised by those inside government in relation to any of those over 800 criminal offences that could be deployed to assert that those offences should not be the subject of journalist, whistleblower and legal advice protections, and for ARTK to have to deal with such in this submission preemptively.

5.4 Ultimately, there can be no policy justification for the maintenance of criminal offences where the essential public interest in ensuring an informed Australian public is not protected by suitable journalist, whistleblower and legal advice protections. That is why ARTK has identified a principled basis underpinning legislation as being the foundation for any proposed offences.

5.5 To similar effect, it is not reasonable to expect stakeholders including ARTK to review over 800 criminal offences, identify any statutory or common law defences or qualifications on liability which may currently apply, and either justify their retention or explain why the protections now found in Division 122 are more suitable. If the Department has a particular view about particular existing

defences relating to offences it proposes be retained, that view should be put forward so that stakeholders can meaningfully engage with the issues raised.

Question Six: What principles should determine how the public interest journalism defence to the general secrecy provisions in Part 5.6 of the Criminal Code is framed?

These principles are set out in relation to Question One and Question Two above.

6.1 Throughout this submission, ARTK has used the neutral expression "*journalist protection*" rather than "*defence*" or "*exception*". This is because the characterisation of the protection as a "*defence*" or "*exception*" has proven controversial in the past. To be absolutely clear on this matter: provided no evidential onus sits on an accused because the statute makes the matters dealt with by the protection part of the scope of the primary offence, ARTK is broadly indifferent to whether the legislation itself refers to the protection as a "*defence*" or "*exception*" because in circumstances where the correct onus of proof has been determined by legislation, the particular terminology used does not dictate essential questions of procedure or onus of proof.

6.2 There are some unfortunate aspects of the Consultation Paper ARTK must draw attention to.

6.3 The Consultation Paper states that: "*The public interest journalism defence in in Part 5.6 of the Criminal Code is the only public interest journalism defence in Commonwealth legislation. There are no equivalent defences in relation to specific secrecy laws*".

6.4 It is true that there are no other journalist *"defences".* There are, however, as discussed at above, "*journalist protections"* where the substantive protection for journalists is framed as a "*negative element*" of the primary offence, in the very form that ARTK contends should be adopted for all disclosure offences. That provision is found in the more recent s 474.47 of the Criminal Code. Amendments in this form have been sought by the media for several years for the reasons broadly canvassed in this submission. Those arguments were accepted when s 474.47 was legislated.

6.5 It is a missed opportunity that when seeking public comment in the Consultation Paper, neither the availability of this most recent legislative model, nor the reasons for or against the use of that legislative model, were presented for public comment. Instead, the impression left when reading the Consultation Paper is that the current Division 122 journalist "*defence*" is an outlier, rather than being a model of protections that are evolving as the public interest they protect is better understood over time.

6.6 It is noteworthy that the Consultation Paper is also silent on the operation of the privilege relating to the disclosure of journalist sources in s 126K of the *Evidence Act 1995* (Cth), even though the operation of this privilege is crucial to understanding the practical operation of the journalist "*defence*" in s 122.5(6) of the Criminal Code.

6.7 The Consultation Paper then makes conclusive – and incorrect – statements which preempts ultimate findings of the review. It states: "*recognising that unauthorised communication or other dealings with national security information could be expected to cause serious or grave damage to Australia's national interest, there are a range of specific secrecy offences in Commonwealth legislation that apply to unauthorised dealings with national security information* …" For the reasons given in relation to Principle Three, that is not correct. The disclosure or use of information about national security does not necessarily compromise national security. That is particularly so where the concept of "*national security information*" remains undefined and appears to extend to any information pertaining to the activities of national security organisations. Nor does it follow that any "*dealing*" with information, which may fall well short of the disclosure of information, would have these damaging effects.

6.8 At the very least, the question of whether "*unauthorised communication or other dealings with national security information"* could "*be expected to cause serious or grave damage to Australia's national interest"* is a matter for reasoned discussion. It is not appropriate for the outcome of that debate to have been preemptively stated as a conclusion in a document designed to facilitate public consultation.

6.9 The Consultation Paper then refers to the "*appropriate oversight and accountability mechanisms in the area of national security including for wrongdoing, corruption or maladministration. The department notes the role of oversight mechanisms such as the Inspector-General of Intelligence and Security and the National Anti-Corruption Commission*".

6.10 The point of "*noting*" these matters is unstated and unclear. The apparent purpose is to suggest that continued government secrecy is appropriate because problems can be addressed 'in house' without public scrutiny by these bodies. The reasons for why that is not the case is explained at length in relation to Principle One.

6.11 Finally, the Consultation Paper refers to the 2019 Richardson Review. It states that this review "*found the current mechanism for public interest disclosures of information obtained by, or relating to, National Intelligence Community agencies (NIC Agencies*) *remained appropriate. Further, it recommended that neither general nor specific secrecy offences applying to NIC agencies should be amended*".

6.12 The Richardson Review – i.e. the *Comprehensive Review of the Legal Framework of the National Intelligence Community* – is not referred to in the terms of reference; nor is it summarised in Attachment C to the Consultation Paper, which is surprising given the central role it plays in the Consultation Paper. What is clear from a cursory review is that this report was primarily prepared by

senior Department of Attorney-General officers leading a team of seconded officers from the Department of Attorney-General and other Commonwealth agencies. Mr Richardson states, in respect to two key Departmental officers, that: "*my role was part time, theirs full time. Throughout the report I refer to 'we' and 'our', recognising the team effort involved. However, the responsibility for the recommendations and views expressed herein, is mine alone*."

6.13 Mr Richardson also notes: "*The review did not undertake detailed consideration of issues that were the subject of recent or ongoing parliamentary or other inquiries, including freedom of the press ….*".

6.14 This report was therefore neither independent nor actually directed to the questions before the current review. Its use as apparent support of the current legislative status quo is not compelling nor appropriate.

Question Seven: Having regard to those principles, is the current public interest journalism defence Part 5.6 of the Criminal Code appropriately framed? If not, what amendments should be considered?

7.1 No, the "defence" is not appropriately framed. The necessary amendments are outlined in answer to Question Two at paragraphs 2.12 to 2.14 above.

Question Eight: Should the public interest journalism defence to the general secrecy offences in Part 5.6 of the Criminal Code identify factors that may be considered for the purposes of determining whether the communication or other dealings with the information may be in the public interest?

No.

8.1 No explanation has been given for this suggestion in the Consultation Paper. When an amendment to this effect was proposed by the Law Council of Australia during the passage of the legislation that introduced the current Division 122, the Attorney-General's Department rejected that proposal.[50] In those circumstances, it would assist if the Department could now explain why such a change is now considered potentially appropriate.

8.2 In any case, such an amendment would only exacerbate the existing problems identified in relation to Principle Two above. Relevantly, it would draw the magistrate or other tribunal of fact into an improper examination of the merits of the journalist's reporting, which is wrong as a matter of principle and creates an unacceptable chilling effect on public interest journalist for the reasons outlined above. In that sense, this question assumes a premise that ARTK does not accept: a magistrate or other tribunal of fact should not be assessing whether a journalist holds "*reasonable grounds*" that use of particular information is in the "*public interest*" in the first place, irrespective of whether that exercise is guided by a list of factors that purport to guide that exercise of discretion.

[50] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (June 2018), [5.38]-[5.39].

Question Nine: Should a public interest journalism defence modelled on subsection 122.5(6) of the Criminal Code be considered for specific secrecy offences, and for which offences would it be an appropriate defence?

Yes. A journalist protection modelled on s 122.5(6), with the modifications proposed in answer to Question Two, should be adopted for all disclosure offences that are to remain on the statute book.

9.1 The framing of the question suggests that it falls to consulted parties to identify each specific criminal offence provision and justify why a journalist protection is appropriate in each case.

9.2 That is not feasible and it is not appropriate.

9.3 As noted in answer to question 5, no policy reason has been given, and none exists, for why this and the related whistleblower and legal advice protections should not be available wherever disclosures of government information are criminalised. ARTK is otherwise unable to comment further. The Consultation Paper does not identify, explain or evaluate the over 800 offences on the current statute book, other than to list them. The unreasonableness of expecting to review over 800 criminal offences in a six week consultation period has already been expounded in paragraph 5.3.

Question Ten: Should the requirement for the Attorney-General's consent to prosecute a journalist for certain offences, which is currently imposed by a ministerial direction, be maintained? If so, should this requirement be legislated?

Yes, the Attorney-General's consent should be a requirement, and yes it should be legislated.

10.1 ARTK notes, however, that such a measure is simply an additional protection that is dependent on the fiat of a senior member of government.

10.2 An after the fact power to grant '*permission*' to publish newsworthy information will vest in the Attorney-General. Irrespective of the personal propriety of the Attorney-General in question, as a structural matter that creates the same form of chilling effect on public interest journalism as where a similar discretion is vested in a magistrate or tribunal. Indeed, the effect is exacerbated because the power is vested in a member of the very government whose actions may be being held up to scrutiny.

10.3 A discretionary power vested in the Attorney-General that concerns prosecutions only will make no difference to the conduct of police investigations investigating overbroad disclosure offences, which as outlined cause their own significant chilling effect on public interest journalism.

10.4 Another problem with this proposal is delay: an Attorney-General may simply fail to grant consent, rather than actively making a positive decision not to grant consent. This places investigations and affected parties in a state of indefinite limbo.

10.5 These factors mean that this measure is at best a complement to proper reforms of the type outlined in the balance of this submission. It cannot be a substitute.