AUSTRALIA'S RIGHT TO KNOW SUBMISSION TO THE SENATE LEGAL AND CONSTITUTIONAL AFFAIRS LEGISLATION COMMITTEE INQUIRY INTO THE *SECRECY PROVISIONS AMENDMENT (REPEALING OFFENCES) BILL 2026*

14 MAY 2026

Australia's Right to Know coalition of media organisations (**ARTK**) welcomes the opportunity to make a submission to the Senate Legal and Constitutional Affairs Legislation Committee inquiry into the Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (**the Bill**).

On 4 June 2019 the AFP raided the home of then News Corp Australia journalist Annika Smethurst, and on 5 June 2019 the AFP raided the ABC offices in Sydney.

These raids, and the laws that underpinned them, put a spotlight on the serious impact of secrecy laws on journalists and news reporting, the rule of law, and the vital role of the fourth estate in Australia's democracy.

Reform of Australia's secrecy laws is one of our top priorities.

To that end ARTK has made substantive forensic submissions to inquiries about Commonwealth secrecy laws. The most thorough inquiry being the Independent National Security Legislation Monitor's (INSLM) 2024 *Secrecy Offences – Review of Part 5.6 of the Criminal Code Act 1995.* ARTK also submitted to the Attorney-General's Department 2023 *Review of Commonwealth Secrecy Laws – Consultation Paper*.

Our submissions and recommendations[1] reflected principles developed by the Australian Law Reform Commission, and most recently endorsed by the INSLM:

[1] For example, submissions to the AGD Review of Secrecy Provisions review – see https://consultations.ag.gov.au/crime/review-secrecy-provisions; submissions to the INSLM Part 5.6 Secrecy Offences Review – see www.inslm.gov.au/publications/secrecy-submissions

1. Clear limiting principles in respect of secrecy provisions must be 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. Liability should only be imposed where there is some clear public interest harmed by disclosure. Disclosures of many types of information (commercial information, etc.) will not meet this threshold; and
4. One essential public interest, the public interest in being informed about activities of government, must also be adequately protected. This justifies disclosures which may cause some harm because a broader set of public interests (revealing wrongdoing, etc.) are served by the disclosure.

Unfortunately, the Bill does not meet those principles and fundamental rule of law principles discussed below.

EXECUTIVE SUMMARY

The Bill fails to meet the four principles above including by:

- Only repealing about 29 secrecy offences – leaving more than 520 on the statute books. No explanation has been given for why it is appropriate to maintain any or all the secrecy offences not repealed by the Bill; and
- Creating a new secrecy offence at s122.4 of the Criminal Code.

This submission sets out the following issues arising from the bill:

1. The new secrecy offence at s122.4 of the Criminal Code is broad and unworkable

The proposed new s122.4 offence is far too broad and is inconsistent with rule of law principles and the specific principles for the drafting of secrecy offences carefully adopted by a number of previous inquiries.

It criminalises legitimately motivated public interest disclosures, and the journalist that facilitates them, that are essential to ensuring a free and independent media can hold power to account. Rather than being clear, certain and properly targeted to disclosures of government information which cause serious harm to essential public interests, the offence uses fundamentally indeterminate criteria (criminalising "*improper*" disclosures). This makes assessing whether or not a given disclosure of information is criminalised ahead of time impossible and so fundamentally undermines the rule of law and free speech. In particular, the new offence:

a) Criminalises dealings with innocuous information and is not confined to cases where disclosure causes actual or likely harm to any clearly identifiable public interest;

b) Criminalises the use or communication of information when "*improper*", which is unacceptably vague for a serious criminal offence; and

c) Criminalises behaviour without an accused demonstrating any degree of moral culpability. A person may be convicted of the offence when there is no dishonestly, no intention to cause harm, no

recklessness as to causing harm, and where the person's subjective motives were otherwise proper and motivated by considerations of the public interest.

2. The Bill fails to extend journalist defences and fails to correct defects in existing journalist defence

The Bill does not extend the current journalist defence in Criminal Code s122.5(6) (or any other defence now contained in Part 5.6) to apply to the more than 520 offences that will remain in statutes nor any of the converted secrecy offences. More succinctly, the more than 520 secrecy offences that will remain after passage of the Bill will not have a journalist defence.

ARTK strongly holds that the existing journalist defence should be extended across the statute book. The public being informed about activities of government is an essential public interest that must also be adequately protected by any secrecy law framework through – at a minimum – the availability of appropriate defences.

There is an obvious perversity in providing, under the current law, for a journalist defence to the general secrecy offences in Part 5.6 but failing to also provide a journalist defence in relation to other standalone secrecy offences which overlap with the existing Part 5.6 offences and/or criminalise less serious offending.

Additionally, as ARTK has put previously, the evidential burden of that defence should not rest on the journalist.

3. Failure to repeal more than 520 secrecy offences

No explanation has been given for why it is appropriate to maintain the remaining 520 plus secrecy offences which are not repealed by the Bill. The Committee is therefore unable to assess whether the Bill has *gone far enough* in removing existing secrecy offences, nor judge whether further modifications to any remaining standalone secrecy offence are needed. This should be remedied.

4. Criminalising existing non-disclosure duties

The current Criminal Code s122.4 makes all existing statutory non-disclosure duties in Commonwealth legislation subject to criminal sanction if those non-disclosure duties are breached. This was a transitional measure and never intended to be permanent. The Bill proposes to maintain the application of that current version of s122.4 to 11 discrete non-disclosure duties. This is inappropriate. These non-disclosure duties attach wholly or partly to innocuous information that should not be subject to criminal protections.

5. Failure to address perverse applications of extended criminal liability principles

A journalist may be found liable under the *insider* offence applicable to public officials under the principles of extended criminal liability in Criminal Code ss11.2, 11.2A, 11.3, 11.4 and 11.5. This should be modified to ensure that journalists, academics, lawyers and other members of civil society are not made liable as accessories to "insider" offences which are designed to operate only to nominated categories of government insider.

6. Amendments in relation to ABC and SBS staff

ARTK supports the policy of excluding ABC and SBS staff from the insider offences at Criminal Code ss 122.1(1),(2),(4); 122.2(1),(2),(4). However, this should be retrospective in operation.

7. Commentary around the continued relevance of security markings to prosecutions for secrecy offences

References in the EM at [257] – [261] and [307] – [310] that purport to describe the continued relevance of security classifications to prosecutions for Part 5.6 offences are legally incorrect and wrongly misstate the ongoing legal effect of security classification markings in prosecutions for secrecy offences. Those references should either be removed or substantively revised to accurately reflect the correct legal position.

8. "Security" in the "outsider" offence in Criminal Code s122.4A must be defined within the Act itself

The current offence in s122.4A applies to "outsiders" to government such as journalists, academics and civil society groups. As amended by the Bill, that offence will criminalise certain disclosures where disclosure causes serious harm to "*security (within the meaning of the Australian Security Intelligence Organisation Act 1979)*."

This is problematic. "*Security*" should instead be defined within the Criminal Code itself. This will ensure the offense remains clearly confined and will reduce the risk that external legislative changes will inadvertently expand the scope of these serious criminal offences. Any properly formulated definition of "security" must also be confined to protecting the security of Australia and no other nation.

9. Amendments to "insider" offences in Criminal Code ss 122.1 and 122.2

Various changes are required:

- The offences should not apply to the disclosure of harmless information simply because it relates to a foreign or domestic intelligence agency. Disclosing information which relates to such agencies does not harm those agencies;

- If the offences are to continue to apply to information that relates to the "*functions*" of an agency, basic rule of law principles require those functions be set by law – otherwise the scope of a serious criminal offence will be set by the policy decisions of public servants and not by Parliament;

- The offences should not apply to "*information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency*". Disclosure of information which relates to law enforcement does not compromise law enforcement;

- These offences relate to disclosures which may prejudice *"security (within the meaning of the Australian Security Intelligence Organisation Act 1979)".* This is problematic. "Security" should instead be defined within the Criminal Code itself. This will ensure the offense remains clearly confined and will reduce the risk that external legislative changes will inadvertently expand the scope of these serious criminal offences. Any properly formulated definition of "security" must also be confined to protecting the security of Australia and no other nation.

- The proposed changes to the harm threshold that determines whether a disclosure is criminalised (deleting reference to harm and maintaining reference to prejudice) are meaningless; and

- The proposed amendments to the concept of "*dealing*" with information are not effective in removing mere passive receipt of information from criminalisation.

Each of these is expanded below.

1. THE PROPOSED NEW s122.4 INSIDER OFFENCE SHOULD BE REMOVED

Bill: Schedule 1, Item 1

1.1 The new offence is open to abuse and is inconsistent with fundamental rule of law principles

The proposed new s122.4 offence is far too broad. It criminalises legitimately motivated public interest disclosures, and the journalist that facilitates them, that are essential to ensuring a free and independent media can hold power to account.

Rather than being clear, certain and properly targeted to disclosures of government information which cause serious harm to essential public interests, the proposed new secrecy offence uses fundamentally indeterminate and values-driven criteria (criminalising "*improper*" disclosures) and does not identify the harm justifying a penal response. This makes assessing whether or not a given disclosure of information is criminalised ahead of time impossible and therefore undermines the rule of law. The new offence also adopts fault elements which will lead to the conviction of the morally blameless. While ostensibly directed to dealing with the facts of the PWC tax scandal, the proposed offence applies far too broadly and criminalises disclosures where the only apparent harm is that the disclosure might cause embarrassment to government.

In doing so, the proposed new offence ignores the carefully developed body of principles developed over multiple reviews and inquires to guide the drafting of secrecy offences. The most comprehensive of these was the Australian Law Reform Commission's 2010 *Secrecy Laws and Open Government* report, which concluded that secrecy offences should only operate where:

- There is actual or likely harm to specified public interests from disclosure of government information;[2]
- There is an intentional disclosure, with either knowledge, recklessness or intention as to the harm caused by that disclosure;[3] and
- There are clear and defined categories of permitted disclosure.[4]

This set of principles was broadly endorsed as recently as 2024 by the Independent National Security Monitor (**INSLM**) in his comprehensive recent report on the Part 5.6 secrecy offences (**INSLM Review**).[5] These principles are however just an application of broader established principles that guide the coherent and just development of the criminal law. Those broader principles are:

2 ALRC Report at [4.2], [4.19] – [4.20], [4.77], [4.12], [4.20], [8.16]-[8.18], [10.33]
3 ALRC Report at [6.96] – [6.127]
4 ALRC Report at [7.55] – [7.60]
5 www.inslm.gov.au/reviews/secrecy-review

- Criminalised conduct must involve, or have the potential to cause, considerable harm to society or individuals, environment or Australia's national interests, including security interests;[6]
- The scope of offences and defences must be clear so that those subject to the laws can know in advance what is and is not criminalised with reasonable certainty;
- That proof of fault is fundamental, [7] and that fault elements should operate to identify those with a genuinely "guilty mind" who engage in genuinely blameworthy conduct;

As we now explain, the proposed Criminal Code s122.4 offence satisfies none of these principles and will have a chilling effect on free speech.

1.2 The new offence criminalises dealings with innocuous information and is not confined to cases where disclosure causes actual or likely harm to any clearly identifiable public interest

Criminal laws should only apply to conduct which involves, or has the potential to cause, considerable harm to society or individuals, environment or Australia's national interests, including security interests.[8] Even in these limited cases, countervailing public interests – in particular the need to maintain a free and independent media – may ultimately excuse an accused from liability.

The new offence does not adhere to this principle. It applies where a person:

a) Uses or communicates information with the intention of obtaining a benefit (for themselves or a third party) or with the intention of causing a detriment (to the Commonwealth or another person); and

b) "*It would be reasonable to conclude that the use or communication of that information is improper*".

This offence therefore has no express harm element. There is no need for the prosecution to establish that either a benefit was in fact obtained or a detriment was in fact caused. Nor do the elements of the offence confine it to cases where any other actual or potential damage to any governmental interest or any person or group in wider society could be caused by the relevant dealing with information. The information dealt with does not even need to be governmental in nature and could be innocuous, trivial or already public domain.[9]

Simply dealing with information in way deemed "*improper*" within the meaning of the new proposed offence does not, in itself, result in any "*considerable harm*" either to Australia's national interests or to any

---

6 www.ag.gov.au/legal-system/publications/guide-framing-commonwealth-offences-infringement-notices-and-enforcement-powers (Guide to Framing Commonwealth Offences) at [2.11]. The need for a "harm based" approach to preparing the current proposed offence based on the ALRC's guiding principles was dealt with extensively by the INSLM at INSLM Report [7.53] – [7.62]

7 Guide to Framing Commonwealth Offences at [2.2.6]

8 Guide to Framing Commonwealth Offences at [2.11]. The need for a "harm based" approach to preparing the current proposed offence based on the ALRC's guiding principles was dealt with extensively by the INSLM at INSLM Report [7.53] – [7.62].

9 The offence applies to information "*obtained*" by reason (for example) of being, or having been, a Commonwealth officer. A public servant whose duties involve reviewing public domain information (like reading a newspaper) is therefore subject to the offence if they subsequently use or communicate any information they acquire. This is regardless of how innocuous or public domain the information is.

member of the public.[10] The information disclosed may be completely innocuous. The new offence is therefore insufficiently targeted to protecting the categories of information that, if disclosed, could cause "*considerable harm*" to Australia's national interests or to the legitimate interests of any person outside government. The conduct it covers is simply inappropriate to criminalise.

1.3 The new offence creates a chilling effect on public interest communications because it does not impose clear standards of conduct sufficiently knowable in advance to guide the conduct of individuals who are subject to the law

A fundamental aspect of the rule of law is that "*the criminal law should be certain and its reach should be able to be ascertained by those who are subject to it."*[11] This means criminal laws must set reasonably clear standards of conduct knowable in advance so that persons may order their affairs knowing what will and will not be subject to criminal sanction.

The proposed offence applies, in contrast, where "*it would be reasonable to conclude that the use or communication of the information is improper*". This is unacceptably vague.

In the context of journalism, the impacts are particularly stark. A journalist and their publisher cannot know whether a person will or not be breaching the law when reporting government information in the public interest. Nor will their source know this when deciding whether or not to cooperate with a journalist. This will lead to an inevitable chilling effect.

The new offence is unacceptably vague for two reasons.

1.3.1 While supposedly operating as an objective test, an assessment of whether conduct is "improper" requires an assessment of the purposes of each accused, which are endlessly variable and intrinsically contestable

The proposed offence applies where "*it would be reasonable to conclude that the use or communication of the information is improper*". The standard purports to be objective. That *appears* to be the point of requiring a jury conclude that "*it would be reasonable to conclude that the use or communication of the information is improper*".

However, objective standards in the criminal law are usually applied in light of the circumstances known to the accused and other relevant characteristics of the accused.[12] Contrary to what is asserted in the EM at [25] – [26], a fair and just assessment of whether conduct by an accused can objectively be regarded as "*improper*" would still need to take into account the motivations, knowledge and beliefs of the accused. A court cannot credibly and fairly assess the *propriety* of a person's actions if it cannot assess their *purpose*

10 As noted recently by the INSLM, the essential governmental interests likely to warrant protection by the criminal law include: security, national defence, international relations, and law enforcement. Criminal secrecy offences are warranted only to protect these and similar classes of information.

11 *DPP v Poniatowska* (2011) 244 CLR 408 at [44] per French CJ, Gummow, Kiefel, Bell

12 For example, as in the defences of self-defence (see *R v Hawes* (1993) 69 A Crim R 92 at 98-99 per Hunt CJ, Simpson and Bruce JJ) and provocation (see *Masciantonia v R* (1995) 183 CLR 58 at [27] – [28] per Brennan, Deane, Dawson and Gaudron JJ)

when acting. An accused's purpose in dealing with the information will therefore be relevant (but not determinative) when a jury assesses whether their conduct was "*improper*".[13]

This means evaluating whether an offence will or has been committed will require a broader contextual assessment of the defendant's situation which considers the factors that motivated them, the immediate operational context and the nature of the information they were dealing with. The offence would therefore operate *differently* to *different people* who disclose the *similar information* based on highly contextual (and contestable) facts about the circumstances of the alleged offending and offender.

Whether or not the offence actually applies in a given circumstances will therefore be highly uncertain and impossible to judge in advance before a person chooses to deal with information.

1.3.2 An assessment of whether conduct is "*improper*" involves a weighing of indeterminate factors without any guidance on *how* to weigh such factors

As above, the proposed offence applies where "*it would be reasonable to conclude that the use or communication of the information is improper*". However, the concept of an "*improper*" dealing with information is highly defuse, morals and values driven. The jury[14] would need to consider the *competing* legal, ethical and moral duties that bear on a public servant's decision-making.[15] Those duties would cover:

- Statutory non-disclosure duties;
- Duties imposed by internal policies and practices;
- Ethical duties (ethical duty to avoid misuse of information for personal gain, etc); and
- Public interest considerations (public's right to know of the operations of its own government, particularly where there is misconduct within government).

When the jury is tasked with making a judgement about the weighing of these conflicting duties to assess whether given conduct was "*improper*", the focus is no longer the *neutral evaluation of provable facts*.[16] Instead, the inquiry would become a *normative evaluation* that involves the jury making *ex post facto* moral judgments about contestable matters of personal conduct based on hindsight reasoning, without a clear set of objective standards which would allow them to identify, rank and prioritise the factors which may favour disclosure versus the factors which may favour non-disclosure.

---

13 If we are wrong, and subjective purpose is in fact to be disregarded for assessing whether an accused has engaged in "*improper*" conduct", this would be another major flaw in the offence. You cannot with fairness and logic determine a person has acted improperly while ignoring their reasons or purpose in acting.

14 The proposed offence carries a standard 2 year penalty. It is an indictable offence – see *Crimes Act 1914* (Cth) (**Crimes Act**) s4J. Indictable offences are tried in either the District or Supreme Court depending on the jurisdiction – see for example, *Supreme Court Act 1933* (ACT) ss20, 68-68G. There is a mechanism for the proposed offence to be tried summarily in a Local or Magistrates Court without a jury, provided there is consent from both the prosecution and accused – see Crimes Act s4J. These submissions assume that prosecutions under the new s122.4A offence will proceed on indictment before a jury – however broadly the same problems we discuss in relation to jury trials will exist in any trial by a Magistrate sitting as the tribunal of fact.

15 This fact is ignored by the EM (at [25] – [27]). It however is necessary when assessing whether conduct is "*improper*" to assess all legal and ethical standards that may bear on the decision to engage in that conduct. The fact that the EM ignores a whole range of considerations related to whether or not disclosure would be *"improper"* and thereby seeks to delegitimate factors which may favour disclosure underscores the unacceptable indeterminacy of the proposed test.

16 An example of such a neutral evaluation would be: did disclosure harm some clearly defined, essential public interest (e.g. national security)? Did the defendant *intend* that harm or was *reckless* to that harm resulting because they appreciated a substantial risk of that harm resulting and proceeded regardless without justification?

This imports an unacceptable degree of subjectivity into the offence. The outcome of the assessment will also be impossible to predict in advance. People subject to the offence will simply not be able to tell whether any proposed disclosure is or is not criminalised. This will inevitably have a chilling effect on public interest disclosures, including to journalists, who themselves may be liable under the offence as accessories.[17] Rational actors will necessarily err on the side of non-disclosure of information which is in the public interest to disclose when criminal liability is imposed on an arbitrary, after-the-fact basis without the application of objective standards.

How the prosecution would actually go about proving whether conduct is "*improper*" is also unclear.

On the one hand, the EM appears to treat the issue as one of fact to be put to the jury. However, unlike other factual questions that may be put to a jury (e.g. was conduct dishonest by the standards of ordinary people, was the use of force reasonable, was the publication obscene), the question of whether or not the conduct of a public servant was "*improper*" in light of complex and competing ethical and legal obligations does not appear, on one reasonable view, suitable for resolution by a jury based on their own commonsense, everyday understandings.

Instead, the matter may need to be resolved based on expert evidence.

However, whether there is in fact a pool of credible "experts" able to give admissible or reliable evidence on whether conduct by public servants is "*improper*" is extremely doubtful. There is no recognised body of relevant "*specialised knowledge*" to be applied.[18] The subject area of expertise is *not* public administration as a general discipline, but rather public sector *ethics.* Nor could any person asserting such knowledge usually represent themselves as *independent* of the prosecution, given such knowledge is likely derived from extensive service in government. Expert evidence led by the prosecution is unlikely to be based on any coherent set of principles that deal with the proper *balancing* of the various legal, policy and ethical duties that would sit at the heart of the court's assessment of whether conduct was "*improper*". The evidence will instead likely be dismissed as the biased assertions of government "insiders".

To illustrate some of these problems.

A public servant uncovers evidence that the head of their agency is engaged in serious misconduct involving improper attempts to influence political decisions. That public servant has no objective standard to assess whether a disclosure to a journalist or other agency outsider would or would not be regarded as "*improper*". The public servant is subject to a range of conflicting legal, ethical and moral duties. The public servant's conundrum in weighing those duties would be strongly informed by the fact that any internal agency disclosure would be highly risky given the very misconduct by their superior that would be the subject of the disclosure. The public servant's own subjective purpose in bringing misconduct to light would *on the better view* be taken into account in assessing whether their conduct is viewed as "*improper*", but it would not be treated as decisive in any future criminal prosecution or trial.

As this scenario illustrates, what the offence provision does and does not authorise will rarely be clear before a person engages in conduct, at least in cases where there is some legitimate, public interest consideration motivating the accused. That is offensive to the rule of law per se, and in the context of public

17 We discuss this further below

18 As an example, see *Evidence Act 2011* (ACT) ss76 – 80 and associated expert witness codes of conduct.

interest disclosures causes particular concern due to the chilling effect caused on legitimate public interest reporting.

1.4 The mental elements of the new offence are triggered without an accused showing the degree of moral culpability that justifies criminal punishment

The need to prove fault is fundamental to creating fair criminal offences that have broad social acceptance.[19]

Without appropriate fault elements in offences, people will be unjustly convicted for accidents, justifiable or excusable risk-taking, or for actions over which they had no reasonable control. The perceived injustice of this would undermine the legitimacy of the criminal law. When structuring criminal offences, it is therefore essential for mental fault elements to identify only those defendants who are sufficiently morally culpable.

While each element of the proposed offence in the new s122.4 offence does contain a fault element,[20] for the reasons we explain, these fault elements do not operate to identify a state of mind of an accused which is sufficiently morally culpable to justify a person being imprisoned.

1.4.1 The mental element of intending a "*benefit*" for another person applies to conduct carried out for wholly legitimate purposes

Under s122.4(1)(c) of the proposed new offence, one of the main fault elements of the offence is satisfied where a person either intends to obtain a "*benefit*" to any person, or intends to cause "*detriment*" to either the Commonwealth or any other person. A person has intention with respect to these results "*if he or she means to bring it about or is aware that it will occur in the ordinary course of events*".[21]

The concept of a "*benefit*" which must be intended by the person is undefined. The EM asserts an operation of this aspect of the new offence which is extremely broad (see EM at [22]). What is clear is that the ordinary meaning of intending a "*benefit*" goes beyond *dishonest or improper* attempts to benefit and also includes circumstances where an accused intends to benefit a person for wholly proper purposes.

Consider this illustration.

A public servant discloses information about a major chemical spill. Their concern regards the agency giving timely or accurate warnings to the public may lead to injuries or deaths amongst the public. They provide the information to the journalist. The public servant in making this disclosure is acting with a proper purpose. However they have also acted with the intention of providing a "*benefit*" to the journalist, in so far as the information is intended to be of assistance to the journalist in publishing a story in the public interest.

---

19 Guide to Framing Commonwealth Offences at [2.2.3]. Creating a fault element in an offence means placing a requirement on the prosecutor to establish a particular state of mind (usually knowledge, intention or recklessness) about the existence of the physical elements of the offence. For example, in the traditional form of the offence of murder, the accused must cause the death of another human being (the physical element) and must *intend* to cause death or *intend* to cause grievous bodily harm (the mental / fault element).

20 This occurs by operation of Criminal Code s5.6 and the specific fault element imposed by proposed Criminal Code s122.4(c).

21 Criminal Code s5.2(3)

This means that the mental element associated with proposed s122.4(1)(c) may be satisfied without any personal impropriety at all on the part of an accused. The disclosure may be for an unquestionably proper purpose.

1.4.2 The mental element associated with needing to appreciate a "*substantial risk*" that conduct is "*improper*" is also satisfied by conduct carried out for wholly legitimate purposes

The other key mental fault element is at Criminal Code s122.4(1)(d).

Under s122.4(1)(d), the proposed offence applies where "*it would be reasonable to conclude that the use or communication of the information is improper*". The associated mental element is recklessness. The prosecution must prove that the accused had:

a) A subjective appreciation that there was a "*substantial risk*" that the relevant circumstance exists or will exist; and

b) That "*having regard to the circumstances known to him or her, it would be unjustifiable to take that risk*".[22]

The first requirement in (a) is problematic. The test for whether a person is reckless is subjective. It involves assessing what the accused had a subjective appreciation of it being "*reasonable to conclude that the use or communication of the information is improper*". This means the jury will be asked to decide whether the accused was subjectively aware that *someone else may conclude that an objective standard that the third party may formulate may be breached by their conduct.* This would be as tortured as it sounds.

The requirement also gives prosecutors an effective benefit of the doubt. So long as the accused appreciates that disclosure may *plausibly* breach the objective standard, this element of the fault element is satisfied – because the accused would appreciate a "*substantial risk*" that the objective standard of "*proper*" conduct might be breached. The accused will satisfy this even when subjectively convinced that their conduct is, on balance, carried out in accordance with the objective standards of "*proper*" conduct.

This is unfair.

It also stands in direct contrast with how the Criminal Code now evaluates whether conduct can be treated as "*dishonest*". Under Criminal Code s130.3, conduct of an accused is dishonest if it is judged to be dishonest by the standards of ordinary people and it is known by the defendant to be dishonest according to the standards of ordinary people. This stricter formulation based on an accused knowing their conduct falls short of an objective standard ensures that people are not convicted when they believe that *on balance* their behaviour conforms to an objective standard.

Due to these flaws, this fault element of the offence will also be satisfied without any personal impropriety at all on the part of an accused. The disclosure may be for an unquestionably proper purpose.

The other relevant aspect of the recklessness test does not meaningfully help. As just discussed, in addition to having to establish that there was a "*substantial risk*" that the relevant circumstance exists or will exist

[22] Criminal Code s 5.6(2), 5.4(1)

the prosecution must also prove that "*having regard to the circumstances known to [the accused], it would be unjustifiable to take that risk*".[23]

The test to assess whether conduct is "*justified*" is: "*whether taking a risk was unjustifiable calls for assessment of the likelihood of the risk eventuating according to its nature and in the circumstances, if the act is done, and whether the risk is one which should have been taken. Whether taking the risk was unjustifiable "requires the jury to make a moral or value judgment concerning the accused's advertent disregard of the risk.*"[24]

Contrary to what is asserted in the EM at [27], this means that the jury would be required to assess whether the accused's reasons for dealing with information were altruistic or for some otherwise proper purpose. That goes to the heart of the "*moral or value judgment*" that must be made about whether their risk-taking was "*justified*".

However, the way this would operate is problematic. The inquiry would be completely uncertain. It would involve the jury making *ex post facto* moral judgments about contestable matters of personal conduct based on hindsight reasoning. This exercise would be unacceptably indeterminate. An accused becomes criminally liable for accepting those "*unjustifiable*" risks that *a jury determine they should not have taken, after those people have deliberated after-the-fact and with the benefit of hindsight, in the highly artificial forum of a jury trial, several months or years after the events in question.* One jury *today* is likely to take a different approach to one jury *tomorrow*. The jury in *Courtroom 1* is likely to take a different approach to the jury in *Courtroom 2.* This is offensive to the rule of law.

This means that while there may be *some limited capacity* for the defendant to argue that they should be exonerated from liability because they held a proper purpose, the mechanism for establishing this is completely unsatisfactory. This means there will remain a very clear risk that the morally blameless will be convicted.

1.4.3 Conclusions on fault elements

It is wrong to send a person to jail for two (2) years for breach of contestable moral standards when there is no dishonestly, no intention to cause harm, no recklessness as to causing harm, and where the person's subjective motives were otherwise proper and motivated by considerations of the public interest. Such an offence falls so short of received standards of fairness and justice that its adoption would bring public administration and the administration of criminal justice into serious disrepute.

To be clear, ARTK's position is not that an accused who has a proper, legitimate purpose when dealing with information should automatically be shielded from criminal liability. The position is more nuanced.

In a properly structured offence where harm to some essential public interest forms a key physical element of the offence, it *might* be appropriate for criminal liability to be imposed when a person has an *intention* to

---

23 Criminal Code s 5.6(2), 5.4(1)

24 *Lustig v Regina* (2009) 195 A Crim R 310 at [74] (Gils JA), Grove J (at [80]), Hall J (at [81], endorsing the earlier decision of the NSW Court of Appeal in *R v Saengsi-Or* (2004) 61 NSWLR 135at [70] (Bell J), Wood CJ at CL agreeing at [1], Simpson J agreeing at [2]. See also *R v Chalabrian (No 13)* [2022] NSWSC470 at [58]; *R v Nozhat (No 2)* [2019] ACTSC 81 at [12]; *FairWork Ombudsman v Ecoway* [2016] FCA 296 at [193]; *ASIC v Mariner Corporation* [2015] FCA 589 at [369] – [374].

cause harm or is *recklessness* in causing that harm *even if their purpose when acting was altruistic or otherwise proper.*

However, this is not the situation with the proposed new offence. The proposed offence lacks any harm element. So the normal fault element that would be appropriate – being either an *intention* to cause that harm or *recklessness* in causing that harm – cannot be used as a component of this offence.

The proposed offence instead makes compliance with a supposedly objective (but in truth indeterminate) moral standard (an "*improper*" dealing with information) the key physical element. Therefore, for the reasons just given, none of the mental elements in the offence are triggered by a sufficiently blameworthy state of mind. The person may in fact be acting with the best of motives. A blameless mind and breach of an indeterminate and contestable moral standard is a fundamentally unsound basis to impose criminal liability.

1.5 The new s122.4 offence does not give effect to its stated policy justifications

The EM justifies the introduction of the new s122.4 offence at [10]:

> *The new offence is intended to protect sensitive information held by the Commonwealth and ensure that Commonwealth officers and others with confidentiality obligations can be held to account when they use information inconsistently with the standards expected of them. The new offence has also been designed to address issues raised by the alleged disclosure of Treasury information by a then partner at a consulting firm in breach of confidentiality obligations.*

The Statement of Compatibility gives a different policy justification (at [44]):

> *The new offence is necessary as it … protects information that, if improperly used or disclosed by Commonwealth officers and persons who work for the Commonwealth, would harm the trust individuals and organisations place in government to appropriately handle their information.*

The proposed offence is not coherent with either statement of policy intent. It *is not*:

- confined to prohibiting the disclosure of sensitive information;
- confined to prohibiting the disclosure of information by persons under specific confidentiality obligations;
- confined to protecting the information which individuals and groups have "entrusted" to government (nor confined to cases where the disclosure of "entrusted" information, if disclosed, is likely to harm trust by those providing that information to government – a much narrower category);
- Nor is there any meaningful articulation in the legislation of any of the "*standard expected*" of public servants that the EM asserts the new offence is designed to safeguard.

These stated rationales do not support the offence in the form introduced.

One additional policy rationale is given. The EM states the new offence is needed to *"address issues raised by the alleged disclosure of Treasury information by a then partner at a consulting firm in breach of*

confidentiality obligations." What ARTK can say about this issue is limited.[25] It can say that *if* a government service provider obtained sensitive information through the performance of an advisory engagement and used that information to obtain a benefit for themselves or a third party, that person has potentially committed the offence of Abuse of Public Office.

Criminal Code s142.2(1) relevantly provides:

> *A Commonwealth public official[26] commits an offence if:*
>
> *(a) the official:*
>
> *….*
>
> *(iii) uses any information that the official has obtained in the official's capacity as a Commonwealth public official; and*
>
> *(b) the official does so with the intention of:*
>
> *(i) dishonestly obtaining a benefit for himself or herself or for another person; or*
>
> *(ii) dishonestly causing a detriment to another person.*

There is no reference to s142.2(1) in the EM and no explanation as to why the existing criminal prohibition on the dishonest use of information is inadequate in capturing the "*issues raised*" by the alleged incident referred to in the EM. However, this provision appears to cover the conduct of the type referred to in the EM.

The far more wide-reaching offence proposed in new Criminal Code s122.4 is, therefore, wholly unnecessary.

RECOMMENDATION

The proposed new s122.4 offence be removed from the Bill.

2. THE CURRENT JOURNALIST DEFENCE IN CRIMINAL CODE s122.5(6) SHOULD BE REFRAMED AND EXTENDED TO APPLY TO ALL SECRECY OFFENCES

Defences to the offences found in Criminal Code Part 5.6 are set out at Criminal Code s122.5. Civil society has had longstanding concerns with the operation of these defences. Despite the current Bill being directed to the overall reform of secrecy offences (and their cognate defences), no attempts have been made by the Bill to address these issues.

---

25 While an individual is not named in the EM, the identity of a specific individual can still be readily inferred. Reporting suggests that the identifiable individual remains the subject of an ongoing criminal investigation. What can be said in public statements about that individual is therefore constrained by the need to ensure this individual receives a fair trial.

26 Third party service providers to government are covered as "commonwealth officials" under (p) and (q) of the Criminal Code Dictionary definition of "commonwealth official".

ARTK seeks two changes to the current defence in Criminal Code s122.5(6). Specifically, the current journalist defence in s122.5(6) of the Criminal Code should be:

- Extended to apply to all secrecy offences; and
- Reframed to correctly place to onus of proof on the prosecution, as per scrutiny principles and current practice in criminal prosecutions.

2.1 The journalist defence in Part 5.6 should extend across the statute book

The current general secrecy offences found in Part 5.6 of the Criminal Code are subject to several defences set out in s122.5.

One of those defences is a defence for journalists and other media workers in s122.5(6).

This defence (and the other defences in Criminal Code s122.5) apply only to the offences in Part 5.6. They will not apply to the approximately 520 criminal secrecy offences that will remain on the statute book after the passage of the Bill (see [3] below).

This is a serious policy error.

The Statement of Compatibility explains the decision not to extend the existing journalist defence this way at [8]:

> *Consideration was also given to whether there were other secrecy offences to which a public interest journalism defence could appropriately be applied. It was determined that the majority of secrecy offences did not apply to journalists. For the remaining offences that could apply to journalists, these protect sensitive information such as law enforcement, national security, sensitive health and commercial-in-confidence information, and it would rarely be appropriate for such information to be disclosed outside of established whistleblower frameworks.*

These assertions are neither correct nor consistent with the general findings of the inquiries referred to at [1.1] above.

Dealing specifically with the claims made in the Statement of Compatibility – in relation to all primary secrecy offences, it is irrelevant if the offence is confined on its face to a particular class of public servant in a way that excludes journalists. Principles of accessorial liability, joint commission, incitement and conspiracy that apply under Criminal Code ss 11.2, 11.2A, 11.4 and 11.5 all apply. They will operate to make journalists liable under all primary secrecy offences even when the offence, on its face, excludes journalists. This issue is very real, as it inheres in the very nature of a journalist obtaining information from a source that the journalist will be accused of facilitating or encouraging the commission of a secrecy offence by persons subject to the relevant secrecy offence. The assertion that these offences do not require a journalist defence because the offences "*do not apply to journalists*" is therefore incorrect.

The assertion that the more than 520 remaining offences "*protect sensitive information such as law enforcement, national security, sensitive health and commercial-in-confidence information"* is also inaccurate based on the limited review ARTK has undertaken – for reasons including that the offences cover information relating to the internal operations of government where the only consequence of disclosure is embarrassment for public officials. We discuss this below at [3.0].

Also, these are not categories of information which necessarily warrant criminal protections per se because their disclosure will cause "*serious harm*" – we have outlined these scenarios already at [1.2] above. They are not categories which warrant criminalisation where the accused is acting as a journalist in the public interest. That is underscored by the fact that a journalist defence is *already* provided in respect of similar disclosures when those disclosures are dealt with under the offences in Part 5.6 of the Criminal Code.

The reasons for the public's right to know about the activities of its own government should be uncontroversial. The free flow of information about the activities of politicians and public servants is the only effective safeguard against government abuse, excess and mismanagement. Government itself can never be the sole investigator of itself.

If secrecy laws can be used to prevent the public seeing maladministration, misconduct or corruption within government, the democratic system risks breaking down. 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 voting decisions about its government and the direction of its country. This public interest, subject to confined exceptions, outweighs the short term harm caused by the disclosure of particular information.

The need to protect this vital public interest has already been recognised by the Parliament when it adopted the current journalist defence in Part 5.6.

That public interest will simply not be protected if journalism remains subject to over 520 secrecy offences which prohibit legitimate reporting in the public and national interest if no equivalent journalist defence is introduced. There is an obvious perversity in providing, under the current law, a journalist defence for the general secrecy offences in Part 5.6 but failing to also provide a journalist defence in relation to other standalone secrecy offences which either overlap with the Part 5.6 offences or criminalise less serious offending.

RECOMMENDATION

The existing defence in Criminal Code s122.5(6) be extended to all other secrecy offences, with an appropriate mechanism developed to identify relevant offences based on Sched 3 item 1 of the Bill.

2.3 An evidential burden for establishing the journalist defence in s122.5(6) should not sit on an accused

There is an existing defence for journalists and media workers at s122.5(6), but its protection is limited.

Normally, the prosecution must establish all matters relevant to establishing criminal guilt beyond a reasonable doubt. This usually means the prosecutor needs to present a case that seeks to establish the existence of all the elements of the offence and seeks to pre-empt and deal with any "reasonable doubts" about whether those elements in fact exist.[27]

[27] For example, in the traditional form of the offence of murder, the prosecution must prove that the accused caused the death of another person with the intention of causing that death or causing grievous bodily harm. If there is a possible reasonable doubt about the existence of any of those elements (for example, a reasonable doubt that the death might have been through natural causes and not caused by the defendant), the prosecution must deal with that issue in their case in chief and try to dispel any reasonable doubt about a natural cause of death.

This is an essential part of the right to be presumed innocent and the right to silence.

Sometimes the Courts have regarded it as *unfair* to require the prosecutor to have to preempt and deal with a particular issue in its case. This may be because the prosector cannot reasonably be expected know anything about that issue. This will normally be because the issue is "*peculiarly within the knowledge of the accused*".[28]

Sometimes it may be regarded as *unreasonable* to make prosecutor try to preempt and deal with a particular issue in its case because of questions of cost or expense.[29] This is often addressed by asking: would it be significantly more difficulty and costly to force the prosecution to have to disprove the issue compared to making the accused prove the issue.

In these two *limited* cases when it is neither *fair* nor *reasonable* to require the prosecutor pre-empt and deal with an issue, the common law may instead place either an evidentiary or a legal onus on the accused.

A legal onus usually requires the accused to prove the issue on the balance of probabilities. An evidentiary onus only requires the defendant be able to point to evidence that suggests a reasonable possibility that the issue exists.[30] If they do that, the burden shifts and prosecution must then prove beyond a reasonable doubt that the issue does not exist.

Currently, the journalist defence in s122.5(6) places an evidential burden on the accused.

The placement of this evidential onus is not justified by the principles just discussed, which have since been adopted as legislative scrutiny principles used to review all criminal legislation.[31]

Under the current journalist defence in s122.5(6), whether or not a person *subjectively held* a belief that their actions were 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. This is instead a matter which the prosecution can and should readily establish by inference from objective facts. So this is not a case where it is *unfair* to make a prosecutor deal with this issue in the normal way.

Nor is dealing with a journalist defence "*significantly more difficult and costly for the prosecution to disprove … than for the defendant to establish*". There are no obvious barriers faced by a prosecution in having to disprove the existence of a journalist defence in its case in chief. So this is not a case where it is *unreasonable* to make a prosecutor deal with this issue in the normal way.

In fact, it appears that the prosecution may need to deal with the absence of a journalist defence in its case in chief due to other procedural requirements regardless of where the evidentiary onus sits.[32] So nothing

---

28 An example of this is the common law defence of insanity. A prosecutor is generally not expected to deal with whether the accused is sane because the information about that issue rests solely with the accused and what is occurring in their own mind. The prosecutor has no access to that information.

29 An example would again be the common law defence of insanity. A prosecutor would be put to pointless difficulty in having to prove beyond a reasonable doubt in every trial that the defendant was sane. Sanity will simply not be an issue in most trials so this would be wasted effort.

30 Criminal Code s13.3

31 *Senate Standing Committee for Scrutiny of Bills Guidelines (Second Edition)* at p. 7

32 An established principle of criminal practice is that the Crown must usually run its case before the defendant and must usually lead the whole of its evidence "*fully and fairly*" before the defendant opens his or her case - *R v Soma* (2003) 212 CLR 299 . Prosecutors are generally not allowed to reopen their case after a defendant's case to address matters raised in the

actually seems to be achieved by seeking to place the evidentiary onus on the accused. In those circumstances it should be removed.

RECOMMENDATION

The reverse evidentiary onus on defendants under the defence in s122.5(6) be removed.

3. SIGNIFICANTLY MORE SECRECY OFFENCES SHOULD BE REPEALED – MORE THAN 520 STANDALONE SECRECY OFFENCES WILL REMAIN IN FORCE

Bill reference: Schedule 2, Items 1-41

The Bill appears to repeal approximately 29 existing secrecy offences (a small number are converted to non-criminalised non-disclosure duties). This leaves approximately over 520 secrecy provisions on the Commonwealth statute book and about 295 existing statutory non-disclosure duties[33].

Many of the remaining secrecy offences that are not repealed by the Bill are problematic because:

- They are overly broad and criminalise the communication of information where there is no clear policy justification (this justifying either repeal of these offences or amendment to appropriately confine their operation);

- They substantively overlap with the secrecy offences in Part 5.6. Basic rule of law and fairness considerations favour repealing any specific offences where there is substantive overlap. Minor differences, including differences regarding penalty, should be dealt with as circumstances of aggravation attaching to the general Part 5.6 secrecy offences;[34] and

defendant's case. This is for reasons of fairness. The Crown should not have the advantage of both the first *and* last word before a jury. Defendants should also not be forced to speculate on what the prosecution *might* do *after* the accused has made forensic decisions about the questions to be put in cross-examination, the evidence they may wish to call, and the objections, if any, they may wish to make in relation to the prosecutor's evidence – see *R v Killick* (1981) 147 CLR 565 at 569-571 per Gibbs CJ, Murphy and Aicken, 576-577 per Wilson and Brennan JJ; *R v Chin* (1985) 157 CLR 671 at 685-6. It is only in *"very special or exceptional"* circumstances that the prosecution will be allowed to adduce evidence after a defendant's case. While defences where a defendant carries a legal burden (e.g. insanity) *may* permit a Crown case in rebuttal, it appears that reasonably foreseeable defences which must be raised only to an evidentiary standard by the accused must generally be dealt with by the prosecutor in their case in chief – see *R v Goode* [2004] QCA 211 at [39], [44]; *Shaw* at 379-380; *Killick* at 572; *Chin* at 676-677; *Soma* at [104]. This means that if reliance on a particular defence subject to a reverse evidential onus is reasonably foreseeable by the prosecution, the prosecution must attempt to deal with that offence in its case in chief *regardless of where the evidentiary onus sits*. It goes without saying that when a proceeding is brought under Part 5.6 against a journalist, it will be "*reasonably foreseeable*" that the accused will rely on the journalist defence. So the prosecution will need to deal with that issue in its case in chief.

33 AGD Secrecy Review at p. 10

34 It is not appropriate to leave substantively overlapping offences on the statute book. The assertion may be made that maintaining a specific offence to deal with a specific topic will lead to better deterrence. This is not an acceptable reason for ongoing incoherence across the statute book. Any remaining offences that overlap with the existing Part 5.6 offences will generally not be subject to the same defences as the current Part 5.6 defences – which means that public servants dealt with under any remaining standalone secrecy offences will be substantively disadvantaged than if they were prosecuted under the overlapping Part 5.6 offence. This is fundamentally unfair to accused persons. Leaving offending conduct outside the operation of the current Criminal Code Part 5.6 to be dealt with by a standalone criminal offence also means that the

- They are often framed in archaic language that does not cohere with the provisions of the Criminal Code dealing with facilitation of proof, ascertaining fault elements or the operation of defences and excuses. Invariably, the remaining standalone secrecy offences do not contain the specialist defences or facilitation of proof mechanisms now contained in Part 5.6 of the Criminal Code that have already been judged as appropriate by Parliament for the existing general secrecy offences. Even if a case for retaining a standalone secrecy offence could be made, there is an overwhelming case to *modernise* the remaining standalone defences offences and align their operation with both the broader Criminal Code regime and the specific principles regarding defences and facilitation of proof now set out in Criminal Code Part 5. One obvious example of this is the need to provide consistent journalist defences across the statute book (dealt with above at [2.1]).

Some of the retained secrecy offences of most concern include:

- *Australian Border Force Act 1997* (Cth) s42
  the concept of protected "*immigration and border protection information*" is too broad and extends to commercial and business information;

- *Australian Crime Commission Act 2002* (Cth) s5
  the protection extended to information "*acquired … in the course of … the performance of duties under the Act*" is too broad as it extends to any information (commercial procurement, etc) regardless of sensitivity or impact on law enforcement functions;

- *Australian Federal Police Act* (Cth) ss40ZA, 60A
  these offences are overbroad as they criminalise disclosure of any information in relation to certain investigations (s40ZA) and any *disclosures* of information obtained in the course of carrying out functions or duties (s60A), regardless of the operational effect or other damage that disclosure may have;

- *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) ss 18(2), 18A, 18B, 81, 35P esp 35P(2) & 35P (2A)
  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. It is wrong in principle to criminalise the disclosure of all information that simply relates to a law enforcement or intelligence agency. Section 35P, in particular ss35P(2) and (2A), are too broad. They criminalise disclosures of information "*relating*" to a "*special intelligence operation*" where certain other conditions are met;

- *Crimes Act 1914* (Cth) ss 15HK, 15JQ,15JR
  the offences relating to disclosure of information relating to "*controlled operations*" are overbroad and raise the same issues as the similar s 35P of the ASIO Act. As with s 35P, disclosure of information pertaining to a controlled operation – which involves an authorisation to commit otherwise illegal conduct – is not the same thing as disclosing information which *harms or compromises* a controlled operation;

---

standardised approaches adopted in Part 5.6 to facilitating proof and facilitating the provision of relevant information to a Court for the purposes of effectively prosecuting offences do not apply to the standalone offence.

- *Defence Act* (Cth) ss 73A
  criminalising disclosure all information under s 73A "*relating to any fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or air force aerodrome or establishment or any other naval, military or air force information*" is self-evidently too broad;

- *Inspector-general of Intelligence and Security Act 1986* (Cth) s34
  criminalising disclosure of all information "*acquired*" in connection with IGIS service is too broad as it extends to any information (commercial procurement, etc) regardless of sensitivity or impact on intelligence functions; and

- *Intelligence Services Act 2001* (Cth) ss 39-41B
  the criminalising all information "*acquired*" in connection with ASIS, AGIO, DIO or ASD functions is too broad as it extends to any information (commercial procurement, etc) regardless of sensitivity or impact on intelligence functions.

No explanation has been given for why it is appropriate to maintain each of the more than 520 secrecy offences which are not repealed by the Bill.[35] This gives rise to a risk that, in attempting to defend a prosecution under one of the existing or proposed Part 5.6 offences, an accused will find themselves in breach of one or more of these 520 offences.[36] As no list of those offences has been provided, the Committee will find it difficult to be satisfied that an accused will not be placed in this situation. A defendant being stopped by a secrecy offence from disclosing information to facilitate their own criminal defence would be an injustice.

35 Only a limited, provisional list of provisions deemed appropriate for removal was contained at Appendix E. Those limited recommendations do not appear to have fully been put into effect by the Bill.

36 The defence of providing information to a Court or Tribunal in s122.5(5) would not apply to information provided to a Court or Tribunal in breach of a criminal offence found outside Part 5.6 of the Criminal Code.

RECOMMENDATION

AGD be requested to provide a comprehensive explanation:

1. Outlining the statutory secrecy offences identified in its earlier review that will not be repealed or converted to a non-disclosure duty under the Bill;

2. In relation to each remaining criminal secrecy offence identified:

    a) comprehensively explaining the information which is covered by the offence and the persons primarily subject to the offence;

    b) comprehensively explaining why it is appropriate to criminalise disclosure of all of the information covered by the offence;

    c) comprehensively explaining why, if appropriate to criminalise disclosure, it is appropriate to criminalise disclosure of that information outside the framework of the existing secrecy offences in Criminal Code Part 5.6; and

    d) confirming that, for each retained criminal secrecy offence, a defendant seeking to defend a Part 5.6 prosecution would not be legally precluded from adducing evidence by reason of the standalone secrecy offence (explaining the mechanism for how such disclosures would be authorised).

4. CRIMINAL LIABILITY SHOULD NOT CONTINUE TO ATTACH TO BREACHES OF 11 EXISTING STATUTORY NON-DISCLOSURE DUTIES

Bill reference: Schedule 1, Items 2, 16, 17, 18, 19, 20, 21, 24, 25, 26, 27, 28, 32, 33

The current s122.4 makes all existing statutory non-disclosure duties imposed by Commonwealth law subject to criminal sanction if they are breached. That provision was transitional in nature and designed to sunset after a period initially set aside for review of the statute book to identify any existing non-disclosure duties that warranted being criminalised. This period was originally set at 5 years but has since been extended to 7 years.

The Bill proposes to maintain the application of that version of s122.4 to 11 discrete non-disclosure duties.

The EM does not substantively justify why each of these specific non-disclosure duties should be criminalised. The EM instead asserts at [33] that: *"The protection offered by the offence at existing section 122.4 has been determined to be of continued necessity for this small number of duties, which relate to sensitive healthcare, personal and commercial information, and are unable to be sufficiently protected by offences in their specific legislation or other non-criminal sanctions."*

Ongoing criminalisation of information subject to many of these duties is inappropriate. For example:

- *Information subject to s67 of the Australian Hearing Services Act 1991 (Cth)* – being all information concerning the operations of the (defunct) Hearing Services Authority (such information not being limited to, or seemingly necessarily even including, personal medical information);

- *Information subject to s15AAA of the Competition and Consumer Act 2010 (Cth)* – being information falling within an unacceptably wide concept of "*protected information*" including information "*given in confidence*" to the ACCC; and

- *Information subject to s98E of the National Health Act 1953 (Cth)* – being certain information subject to evidentiary certificates disclosed to the Pharmaceutical Benefits Remuneration Tribunal – a long defunct body concerned with adjudicating disputes concerning the pay of pharmacists (it may never have actually sat or may have only rarely sat).

ARTK has serious concerns about the extension of criminal liability under this item of the Bill to cover what appears to be the disclosure of commercial information or information that relates only to the internal operation of agencies. There is no justification for criminalising the disclosure of these types of information per se.

While some of the categories of information dealt with in this item of the Bill *might* contain sensitive personal or health information of individuals which *might* conceivably be protected through an *appropriately targeted* criminal offence[37], this item of the Bill will extend criminal liability to a far wider pool of information.

The EM contains no explanation of what information is *specifically* covered through the criminalisation of each *specific* statutory non-disclosure duty covered by the Bill, nor does the EM explain why that information should be subject to criminal protections. This means that it is impossible to properly assess whether the Bill is appropriately extending criminal liability. This should be remedied so that the Parliament can make an informed assessment on whether to extend criminal liability under these items of the Bill.

[37] Noting that even this conceivable type of criminal protection is highly contestable from a policy standpoint – protection of such information is already protected by privacy and health records legislation.

Recommendation

AGD be requested, in relation to each non-disclosure duty which the Bill seeks to criminalise, to:

a) comprehensively explain the information which is covered by the duty and the persons primarily subject to the offence;

b) comprehensively explain why it is appropriate to criminalise disclosure of all of information covered by the duty;

c) comprehensively explain why, if appropriate to criminalise disclosure, it is appropriate to criminalise disclosure of that information outside the framework of the existing secrecy offences in Criminal Code Part 5.6; and

d) confirm that, for each duty that has been criminalised, that a defendant seeking to defend a Part 5.6 prosecution would not be legally precluded from adducing evidence by reason of the now criminalised non-disclosure duty (explaining the mechanism for how such disclosures would be authorised).

5. PRINCIPLES OF EXTENDED CRIMINAL LIABITY SHOULD BE MODIFIED IN THEIR APPLICATION TO PART 5.6 OFFENCES

The current secrecy offences in Part 5.6 are divided between "insider" offences applicable to government officials and government service providers, and the one "outsider" offence at s122.4A applicable to government "outsiders" such as journalists, academics and other members of civil society.

The very point of currently having different insider and outsider offences is to reflect the different degrees of criminal culpability for those "insiders" subject to the offences in ss122.1, 122.2, 122.3 and 122.4 and the "outsiders" subject to s122.4A. The current law reflects the recognition that an "outsider" such a journalist, an academic, or other interested member of civil society should only be criminally liable in a much more limited set of circumstances than public servants and other "insiders". This is for a range of reasons including that they are not employed by the Commonwealth, have not made commitments of confidentiality to it or agreed to abide by its policies.

However, it is inherent in the very act of journalism that a journalist may be taken to be a person who procures the commission of an insider offence. This will likely make that journalist liable under the *insider* offence under the principles of extended criminal liability in Criminal Code ss 11.2, 11.2A, 11.3, 11.4 and 11.5. Under these principles, the journalist will be taken to have committed the *insider* offence and be punished accordingly, provided certain intention and other requirements for accessorial liability are met.

To permit the operation of an insider offence to an outsider renders pointless the attempt to create two separate legal regimes for insiders and outsiders in Part 5.6. The effect is that a much broader range of conduct by journalists, academics and other civil society participants who have engaged with government insiders will be investigated and tried as "insiders". This is not appropriate.

As already discussed at [2.1], a similar issue arises in relation to the operation of the remaining standalone offences. Even when those offences are on their face limited to applying to named classes of government insiders, any outsider who participates in receiving information for them is also potentially criminal liable under the principles of extended criminal liability.

RECOMMENDATION

That the principles of extended criminal liability be modified to ensure that journalists, academics, lawyers and other members of civil society are not made liable as accessories to "insider" offences in Part 5.6 and elsewhere which are designed to operate only to nominated categories of government insider.

6. THE REMOVAL OF ABC AND SBS STAFF FROM THE OPERATION OF THE "INSIDER" SECRECY OFFENCES SHOULD BE BACKDATED TO THE COMMENCEMENT OF THE "INSIDER" OFFENCES

Bill reference: Schedule 1, Items 3-8

ARTK supports the policy of excluding ABC and SBS staff from the insider offences at Criminal Code ss122.1(1),(2),(4); 122.2(1),(2),(4).

These insider offences were designed to deal with government officers and other government "insiders". The unique position of public broadcasters makes the inclusion of ABC and SBS staff within such offences inappropriate. This was recognised by the INSLM report.[38]

It is clear that the current application of these offences to ABC and SBS staff was an inadvertent drafting oversight.[39] As it was never the intention to subject ABC and SBS staff to these offences, it is appropriate for these beneficial amendments designed to exclude ABC and SBS staff from the operation of these offences to operate retrospectively from the commencement of the operative offence provisions on 29 December 2018.

RECOMMENDATION

The Committee recommend that Sched 1 item 15 be amended to provide for retrospective operation of the amendments at Sched 1 items 3 – 8 from 29 December 2018.

38 INSLM Report at [8.91]

39 It arose this way. The offences apply where a person is a "Commonwealth officer" (which under s121.1 is specifically defined to exclude ABC and SBS staff). However the offences also apply where a person is "otherwise engaged to perform work for a Commonwealth entity". The Dictionary definition of "Commonwealth entity" (with its linked definition of "Commonwealth Authority") covers the SBS and ABC as "bodies established by or under" laws of the Commonwealth, subject to the operation of any regulation being made removing these bodies from the definition. It is clear from this that the apparent intention to exclude the ABC and SBS evidenced from the drafting of "commonwealth officer" miscarried because of a failure to either appropriately amend the definition of "commonwealth entity" to reflect the same limitation found in the definition of "public official", or introduce a Part specific definition applicable only to the Part 5.6 offences that reflected the same limitation.

7. THE EFFECT OF REMOVING SECURITY CLASSIFICATIONS AS AN ELEMENT OF THE PART 5.6 SECRECY OFFENCES SHOULD BE ACCURATELY DESCRIBED IN THE EXPLANATORY MEMORANDUM

Bill reference: Schedule 4, Items 6, 9, 10 and 22

While ARTK welcomes this change we have concerns with the way that the EM describes the ongoing effect of security markings in prosecutions under Part 5.6 of the Criminal Code, particularly the EM's discussion of relevance of security marking to establishing the "outsider" offence targeted to non-government officials in s122.4A of the Criminal Code.

The EM states at [307] – [310] that:

> *Subsection 122.4A(1) establishes an offence for communication of certain sensitive information by non-officials.*
>
> *Existing subparagraph 122.4A(1)(d)(i) provides a circumstance element of the offence, requiring that the information has a security classification of Secret or Top Secret.*
>
> *The effect of the repeal of this subparagraph is that communication of information would not trigger the secrecy offence at section 122.4A merely because the information was classified Secret or Top Secret.*
>
> *An individual's knowledge that a document was classified Secret or Top Secret, as well as any knowledge of the Australian Government security classification framework in force from time to time, would nevertheless continue to be an indicator of, and relevant to, the assessment of recklessness for the purposes of establishing the fault element for the circumstances at paragraph 122.4A(1)(d) as amended by the Bill. Section 5.4 of the Criminal Code provides that a person is reckless with respect to a circumstance if they are aware of a substantial risk that the circumstance exists or will exist, and, having regard to the circumstance, it is unjustifiable to take the risk.*
>
> *A non-official's knowledge that the information was classified Secret or Top Secret would be a relevant matter pointing to their understanding of the nature of the information and the consequence if the information was communicated. For example, a journalist that has come into possession of a document marked Top Secret would likely be aware of a substantial risk that the document includes information that, if communicated to the public, could cause serious damage to national security. (emphasis added)*

This assertion is inaccurate. Overzealous security marking is endemic within Government. This is inconsistent with the public interest in open government and damaging to the overall public interest. The INSLM's recent report dealt extensively with current agency practice as it relates to the security classification of information. The INSLM report identifies matters that point to serious, sustained and widespread deficiencies including:

- Systemic risks of over-classification, particularly in email traffic;[40]

[40] INSLM Report at [4.54] – [4.55], Annex E p. 289

- Inconsistent application of security markings across different agencies in relation to similar information;[41]

- Markings being applied inaccurately and without a rigorous, evidence based and objective assessment of the real risks of disclosure; [42]

- Inadequate accountability systems for recording the person who makes a classification decision and their reasons, and inadequate mechanisms to review the application of markings;[43]

- Inadequate mechanisms for downgrading markings when the initial sensitivity of the information has changed or been lost because of the passage of time or supervening events;[44]

- Inadequate training and guidance material to assist officers to consistently and appropriately apply classification rules.[45]

Given these matters, an "outsider" to government such as a journalist is unlikely to subjectively appreciate a "substantial risk" that disclosure of classified information would cause serious damage to national security (or defence)[46] simply because a "Secret" or "Top Secret" marking has been applied. Instead, all that would be apparent to the "outsider" from the existence of a "Secret" or "Top Secret" marking is that:

- Some unspecified person (or some unspecified automated system);
- At some unspecified point in time; and
- Has applied a marking to a document in a purported attempt to comply with a complex, vague and highly discretionary internal policy framework, for reasons which may be mistaken, misguided or improper.

The identified deficiencies with the administration of that framework mean that this itself gives no assurance to any "outsider" dealing with the information that disclosure could cause any harm at all, let alone cause the specific kind of "serious damage" to "national security" or "defence" made relevant by the offence.

This means that the existence of a "Secret" or "Top Secret" marking could not credibly be used to establish that a defendant was aware that the communication of particular security classified information would cause serious damage to national security or defence. The existence of a security marking will therefore not be decisive to establishing the fault element of the amended "outsider" offence at s122.4A(1)(d)(i),(ii) which require this state of mind. What is now stated in the EM is incorrect and likely to mislead law enforcement and prosecutors.

Similar misstatements exist in other areas of the EM.[47] These should all be corrected.

---

41 INSLM Report at Annex D p. 281
42 INSLM Report at [4.45] – [4.51]
43 INSLM Report at [4.47]
44 INSLM Report [4.63]
45 INSLM Report at [4.47]
46 Serious damage to security and serious damage to defence will be the criteria that apply under the amended s122.4A(1)(d)(i),(ii) element of the s122.4A(1) "outsider" secrecy offence – see Bill Sched 4 item 22.
47 Paras [257] - [261] of the Explanatory Memorandum assert that the existence of a security classification would also be relevant to establishing fault elements under the "insider" offence at ss122.1(1) and 122.1(2). The offences at s122.1(1) and 122.1(2) require information that is dealt with or communicated by the defendant being either (a) "obtained by, or made by,

RECOMMENDATION

References in the EM at [257] – [261] and [307] – [310] that purport to describe the continued relevance of security classifications to prosecutions for Part 5.6 offences either be removed or substantively revised to accurately reflect the correct legal position.

8. THE "OUTSIDER" OFFENCE IN s122.4A SHOULD BE MEANINGFULLY CONFINED THROUGH WORKABLE DEFINITIONS OF "SECURITY" THAT DO NOT INCORPORATE CONTENT BY REFERENCE AND WHICH ARE APPROPRIATELY CONFINED TO ACTIONS WHICH DAMAGE AUSTRALIA'S SECURITY

Bill reference: Schedule 4, Items 11 and 22

The current offence in Criminal Code s122.4A applies to government "outsiders" (i.e. non-officials).

Following amendments proposed by the Bill, an offence will relevantly be committed where:

a) The communication of the information causes serious damage to security (within the meaning of the *Australian Security Intelligence Organisation Act 1979* (Cth));

b) The communication of the information causes serious damage to the defence of Australia;

c) The communication of the information causes serious damage to the operations, capabilities or technologies of, or methods or sources used by, a domestic intelligence agency or foreign intelligence agency;

d) The communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

In relation to (a) above – ARTK supports the amendment which seeks to remove a problematic deeming element of the current definition of "*security*" (Bill Sched 4 item 11). However, in terms of the new proposed definition of "*security*", it is inappropriate for the elements of a serious criminal offence to be incorporated by reference from a definition found in other legislation (in this case, the definition of "*security*" in s4 of the

or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions"; or (b) "information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency" (see s122.1 definition of "inherently harmful information"). To satisfy the recklessness fault element associated with these physical elements, the prosecution must prove the defendant appreciated a "substantial risk" of either of these two matters and that the taking of that risk was "unjustified" – see Criminal Code s5.4. Contrary to what is asserted in the EM, the mere fact that a document is marked with a higher classification such as "Top Secret" is not probative as to the whether the defendant appreciated a "substantial risk" of either matter. As made clear in the INSLM's report at [4.42], the higher security classifications cover a vast range of information – far broader than the specific types of information that are covered by the offences in ss122.1(2) and 122.1(2). It is specious to suggest, for example, that the attachment of a "Top Secret" marking because disclosure could cause "catastrophic business impact" would imply or suggest to a person dealing with or communicating the information that the information subject to that marking was either (a) obtained by, or made by, or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions"; or was (b) "information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency".

ASIO Act). Changes may inadvertently be made to the scope of the offence through future amendments to the ASIO Act.

The incorporated definition is also ambiguous when read as an element of a criminal offence. In particular, the extension of the ASIO Act s4 definition of "*security*" to matters associated with "*the carrying out of Australia's responsibilities [for example, in respect to espionage] to any foreign country*" introduces indeterminacy as to the scope of the offence and the offence's application to protecting the security interests of foreign countries rather than Australia. Any offence must clearly be confined to protecting *Australia's* security interests.

In relation to (c) above – there is no policy justification for an Australian offence to operate where disclosure damages a foreign intelligence agency as proposed by this amendment. To the extent that a disclosure may harm a foreign intelligence body but still have a meaningful impact on *Australian government interests,* this can separately be dealt with under (a) above (serious damage to security) or (b) above (serious damage to defence).

RECOMMENDATIONS

1. That the proposed new definition of "security" in the existing s 122.4A offence be reconsidered to ensure it applies only to protecting the legitimate security interests of Australia and not any foreign jurisdiction;

2. That any definition of "*security*" (whether or not reformulated) for the purposes of this offence be inserted in Criminal Code Part 5.6 rather than be incorporated by reference from the ASIO Act; and

3. That the requirement that the communication of information cause damage to the operations, capabilities or technologies of, or methods or sources used by, a domestic intelligence agency or foreign intelligence agency be confined to impacts on domestic intelligence agencies only.

9. VARIOUS OTHER CHANGES ARE NEEDED TO "INSIDER" OFFENCES

9.1 THE CONCEPT OF "INHERENTLY HARMFUL INFORMATION" IN THE "DEEMED HARM" INSIDER OFFENCES AT s122.1 SHOULD NOT CRIMINALISE THE DISCLOSURE OF HARMLESS INFORMATION THAT SIMPLY RELATES TO A DOMESTIC OR FOREIGN INTELLIGENCE AGENCY

Bill reference: Schedule 4, Item 6

The current offences in Criminal 122.1 apply to government "insiders" (i.e. officials and certain government contractors).

The offences apply where this is disclosure or other dealing involves "*inherently harmful information*". These are designed to be categories which identify cases where the simple act of disclosing information of

the specified type can be safely assumed to cause harm to national security interests which is sufficiently serious to warrant criminal sanction.[48] This means these categories must be carefully confined.

Following amendments proposed by the Bill, "*inherently harmful information*" will be defined in Criminal Code s121.1 to mean:

a) Information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's function;

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

These remain unchanged from the existing legislation.

In relation to (a) above – it is improper to criminalise the disclosure of information that simply *relates* to the operation operations of a domestic intelligence agency. 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. As the INSLM recommended (Recommendation 2), such an offence should be properly confined to instances where disclosure will cause actual harm to intelligence related activities.

In its response to the INSLM report, the Government noted that "*it will undertake further work to assess the feasibility of legislating an alterative, narrower definition*" and that "*the Government acknowledges that not all information held by intelligence agencies is inherently sensitive".*[49] An appropriately confined definition has not been introduced by the Bill and is needed.

RECOMMENDATION

That the existing definition of "*inherently harmful information*" be narrowed to only cover classes of information that, if disclosed likely are to compromise core intelligence gathering and related national security activities of domestic or foreign intelligence services.

48 Distinguishing the offences in s122.2, where harm to the national interest from the disclosure of information must be proven by the prosecution on the facts.

49 Australian Government response to the Independent National Security Legislation Monitor report (Government Response to INSLM Review) at p. 3

9.2 IF THE CONCEPT OF "INHERENTLY HARMFUL INFORMATION" IN THE s122.1 INSIDER OFFENSES CONTINUES TO APPLY TO INFORMATION RELATING TO AN AGENCY'S "FUNCTIONS", THOSE FUNCTIONS MUST BE SET OUT IN LEGISLATION OR A DISALLOWABLE LEGISLATIVE INSTRUMENT

Bill reference: Schedule 4, Item 46

The offences in Criminal Code s122.1 criminalise the disclosure of "*inherently harmful information*". The definition in s121 applies to "*information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions*".

One key intelligence agency (the Defence Intelligence Organisation (**DIO**) operates without functions set out in either primary or subordinate legislation (this is in and off itself a rule of law concern). As DIO has no statutory functions, it is impossible to now properly assess whether information has the relevant connection with DIO's "*functions*" when applying this limb of the definition of "*inherently harmful information*".

The INSLM therefore recommended (Recommendation 5) that the "*functions*" of the DIO should be set out in legislation or a disallowable legislative instrument. In this way, *Parliament* would have the power to set the parameters of DIO's functions and through that, set the limits of the offences in Criminal Code s122.1 which refer back to those functions. The INSLM recommendation is uncontroversial and based on basic rule of law and Parliamentary supremacy principles: the parameters of serious criminal offences must be clearly set by law and not by the policy decisions of public servants.

The Bill has failed to implement this recommendation. Instead, the Bill provides, in an amendment to the *Intelligence Services Act 2001* (Cth) that:

> *The Director of the DIO must make publicly available the document known as the Defence Intelligence Organisation Mandate, as in effect from time to time.*

This amendment fails in two respects:

i. There is no statutory requirement for the "*Defence Organisation Mandate"* to even set out the functions of the DIO in this document. Publishing a blank document with the title "*Defence Organisation Mandate"* satisfies the provision; and

ii. This ignores the very rule of law problem that needs to be solved. If the parameters of an offence are to be set by reference to the "*functions*" of an agency, those functions must be set by law and not by the policy actions of public servants. In this case, such policy would be expressed through a document, which will invariably fail the standards of clarity required for legislation and subordinate legislation, published on the internet.

RECOMMENDATION

That *either* the functions of the DIO are to be set by legislation or disallowable instrument *or* the DIO should be excluded from the concept of a "*domestic intelligence agency*" for the purposes of the definition of "*inherently harmful information*".

9.3 THE CONCEPT OF "INHERENTLY HARMFUL INFORMATION" IN THE "DEEMED HARM" INSIDER OFFENCES AT s122.1 SHOULD BE NARROWED TO PROTECTING A MORE LIMITED RANGE OF LAW ENFORCEMENT FUNCTIONS WHERE DISCLOSURE WILL CAUSE ACTUAL DAMAGE TO LAW ENFORCEMENT ACTIVITIES

Bill reference: Schedule 4, Item 6

The offences in Criminal Code s122.1 criminalise the disclosure of "*inherently harmful information*". The definition in s121 applies to "*information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency*" (our emphasis).

This limb of definition is too broad. Disclosure of information which relates to law enforcement does not compromise law enforcement. 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 be to actual investigations or the performance of investigatory functions, cannot by and of itself damage any recognisable public interest.

This was recognised by the INSLM report (Recommendation 3) and acknowledged by Government in its response to the INSLM report which stated: *"The Government will develop legislation to confine the categories of law enforcement information covered by section 122.1 to information in which there is an essential public interest that needs to be protected by the application of criminal sanctions. This includes essential public interests in the integrity of criminal justice processes and protection of sensitive law enforcement capabilities, methodologies and sources."*[50]

This has not occurred.

RECOMMENDATION

That *either* a more appropriately confined approach be taken to the law enforcement limb of the definition to reflect the commitments made in the Government's response to the INSLM report, *or* the INSLM's preferred reformulation of this limb of the definition be adopted.

9.4 THE CONCEPT OF CAUSING "HARM TO AUSTRALIA'S INTERESTS" IN THE INSIDER OFFENCES AT s122.2 SHOULD BE MEANINGFULLY CONFINED THROUGH WORKABLE DEFINITIONS OF "SECURITY" AND "PREJUDICE" THAT DO NOT INCORPORATE CONTENT BY REFERENCE

Bill reference: Schedule 4, Items 4 and 11

The current offences in Criminal Code s122.2 "insiders" offences apply where a dealing or disclosure of information where this may "*cause harm to Australia's interests*". "*Caus[ing] harm to Australia's interests*" is defined in s121.1. The definition covers categories designed to identify circumstances where the disclosure of specific types of information *might* cause harm to national interests sufficiently serious to warrant criminal sanction if sufficient harm thresholds are met.

[50] Government Response to INSLM Review at p. 3

As amended by the Bill (with changes in markup), the relevant definition of "*cause harm to Australia's interests*" will cover activities which:

> *(a) interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth; or*
>
> *(b) ~~interfere with or~~ prejudice the performance of functions of the Australian Federal Police under:*
>
> > *(i) paragraph 8(1)(be) of the Australian Federal Police Act 1979 (protective and custodial functions); or*
> >
> > *(ii) the Proceeds of Crime Act 2002 ; or*
>
> *(c) ~~harm or~~ prejudice Australia's international relations in relation to information that was communicated in confidence:*
>
> > *(i) by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and*
> >
> > *(ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; or*
>
> *(f) harm or prejudice the health or safety of the Australian public or a section of the Australian public; or*
>
> *(g) ~~harm or prejudice the security or defence of Australia.~~ prejudice security (within the meaning of the Australian Security Intelligence Organisation Act 1979); or*
>
> *(h) prejudice the defence of Australia*

In relation to (b), (c), (f) and (g) above – the removal of references to "*harm*" from the existing categories of the "*cause harm to Australia's interests*" definition has no obvious legal effect. There is no substantive difference between "*harm*" (the deleted expression) and "*prejudice*" (the expression that is retained). Prejudice is an archaic synonym of harm. There seems no reason to make this change.

More concerningly, the EM seeks to give a broader explanation of "*prejudice*" than is warranted by the actual statutory language and context (see EM at [234]). In the context of criminal offence, what does and does not amount to "*harm*" would usually be left to the jury to determine applying ordinary standards and understandings. Why the EM opines on this topic is unclear. The term "*prejudice*" is existing statutory language. It is not contained in the Bill. An EM should not seek to explain the effect of existing legislation unless there is something in the Bill which modifies the effect of that existing legislation.

In relation to (g) above – this raises the same issues as the related amendment to Criminal Code s122.4A discussed above at [10]. As discussed, ARTK supports the amendment which seek to remove a problematic deeming element of the current definition of "*security*" (Bill Sched 4 item 11). However, in terms of the new proposed definition of "*security*", it is inappropriate for the elements of a serious criminal offence to be

incorporated by reference from a definition found in other legislation (in this case, the definition of "*security*" in s 4 of the ASIO Act). Changes may inadvertently be made to the scope of the offence through future amendments to the ASIO Act.

The incorporated definition is also ambiguous when read as an element of a criminal offence. In particular, the extension of the ASIO Act s 4 definition of "*security*" to matters associated with "*the carrying out of Australia's responsibilities [for example, in respect to espionage] to any foreign country*" introduces indeterminacy as to the scope of the offence and the offence's application to protecting the security interests of foreign countries rather than Australia. Any offence must clearly be confined to protecting *Australia's* security interests.

RECOMMENDATIONS

1. That the proposed new definition of "security" in the existing definition of "cause harm to Australia's interests" offence be reconsidered to ensure it applies only to protecting the legitimate security interests of Australia and not any foreign jurisdiction; and

2. That any definition of "*security*" (whether or not reformulated) for the purposes of this offence be inserted in Criminal Code Part 5.6 rather than be incorporated by reference from the ASIO Act

9.5 PROPOSED AMENDMENTS TO THE INSIDER OFFENCES IN ss 122.1(2) and 122.2(2) THROUGH AMENDING THE CONCEPT OF "DEALING" DO NOT ACHIEVE THEIR AIM OF REMOVING CRIMINAL LIABILITY FOR THE MERE PASSIVE RECEIPT OF GOVERNMENT INFORMATION

Bill reference: Schedule 4, Item 5

The "insider" offences at Criminal Code ss 122.1(2) and 122.2(2) apply where an accused "*deals with*" information rather than "*communicates*" information.

A dealing for the purposes of the offences at ss 122.1(2) and 122.2(2) is currently defined in Criminal Code s90.1(1) and (2) (see Criminal Code s121.1 definition of "*deal*"). The INSLM was concerned that these definitions could have the effect of criminalising the mere passive receipt of information and recommended that the definition be amended so as exclude initial receipt.

The proposed replacement definition of deal includes when a person "*possesses"* information or an article. "*Possess*" is not defined for the purposes of the Criminal Code or Part 5.6. There is no reason to think "possess" would be read in a limited way – i.e. to read the term "*possess*" in a limited way so that to "*possess*" information or an article would be read as requiring information or an article to be *knowingly* possessed or be *taken into possession* through some positive act of the accused. To "possess" is instead likely to be taken to mean *in a person's possession,* which includes cases of mere passive receipt. For this reason, ARTK doubts that the amendments are effective to achieve its stated purpose.

RECOMMENDATION

Effective drafting be provided to ensure passive receipt is not a “dealing” for the purposes of the offences at ss 122.1(2) and 122.2(2).