Secrecy, Transparency and Proportionality

Reviewing Part 5.6 of the *Criminal Code 1995* (Cth) in recognition of the importance of transparency, whistleblowing and press freedom

Submission to the Independent National Security Legislation Monitor

Human Rights Law Centre

March 2024

Melbourne Office
Human Rights Law Centre
Level 17, 461 Bourke Street
Melbourne VIC 3000

Sydney Office
Human Rights Law Centre
Level 5, 175 Liverpool Street
Sydney NSW 2000

admin@hrlc.org.au
(03) 8636 4450
(03) 8636 4455
www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses strategic legal action, policy solutions and advocacy to support people and communities to eliminate inequality and injustice and build a fairer, more compassionate Australia.

In 2023, we launched the Whistleblower Project, Australia's first dedicated legal service to protect and empower whistleblowers who want to speak up about wrongdoing. We provide legal advice and representation to whistleblowers, as well as continuing our longstanding tradition of advocating for stronger legal protections and an end to the prosecution of whistleblowers. We are also a member of the Whistleblowing International Network.

We advise and act for clients under relevant state and commonwealth public interest disclosure legislation and sector-specific protections. This often requires advising on the application of secrecy offences, including those in the *Criminal Code 1995* (Cth) (***Criminal Code***). As a consequence of whistleblower protection exclusions in the national security context, uncertainty around the scope of outsider offences and 'dealing with' provisions in the *Criminal Code* directly impact our work on an ongoing basis.

Whistleblower protection is an essential part of the wider human rights framework in this country, underpinned by Australia's international obligations and provides vital checks and balances on Australia's national security institutions. The ability of whistleblowers to speak up, and the public's right to know, is protected under the right to freedom of opinion and expression in international human rights law. This is particularly important for intelligence and national security whistleblowers, who raise critical issues of international importance, but who are afforded significantly narrower whistleblower protections.

In recent decades whistleblowers have proven critical to exposing human rights abuses around the world – without robust whistleblowers protections and public interest journalism, too often human rights violations go unchecked. Whistleblower protections have emerged as an important aspect of the obligations of state parties, including Australia, to fight corruption under the *United Nations Convention Against Corruption*. Whistleblowers also play an important role in upholding Australia's transparent, accountable democracy, ensuring governments respect and uphold human rights and build a fairer, more compassionate country.

The Human Rights Law Centre acknowledges the people of the Kulin and Eora Nations, the traditional owners of the unceded land on which our offices sit, and the ongoing work of Aboriginal and Torres Strait Islander peoples, communities and organisations to unravel the injustices imposed on First Nations people since colonisation. We support the self-determination of Aboriginal and Torres Strait Islander peoples.

Introduction

Australia's secrecy regime is one of the harshest in the liberal democratic world. With over 800 secrecy offences, we also have one of the most extensive.[1] In 2019, the *New York Times* declared that Australia "may well be … the most secretive democracy" in the world, following police raids on journalists.[2]

Prior to 2018, Australia's general secrecy offences dated back to the First World War, and reform was overdue. But the reform as enacted through Part 5.6 of the *Criminal Code* went beyond what was necessary or proportionate. The amendments created broad categories of offences related to vague definitions, each with severe penalties, that have a chilling effect on whistleblowers, journalists and the civil society organisations that support them.

This submission responds to most, though not all, of the 35 issues identified by the INLSM's Issues Paper on the review of Part 5.6 of the *Criminal Code* and issues discussed at the civil society roundtable discussion in early February 2024. Our submission reflects a need to underpin general secrecy offences with principles of proportionality and necessity, and appropriate safeguards and oversight.

As a signatory to the *International Covenant on Civil and Political Rights* (***ICCPR***), Australia must uphold the right to freedom of expression under Article 19(2), which includes the "freedom to seek, receive and import information and ideas of all kinds." Part 5.6 of the *Criminal Code* risks breaching the rights of public servants, whistleblowers, journalists and civil society advocates by limiting their freedom of expression. That, in turn, has constitutional implications in light of the implied freedom of political communication.

Article 19(3) of the *ICCPR* allows for some restriction to these rights "for the protection of national security or of public order, or of public health morals." The Human Rights Law Centre recognises the importance of protecting information that is genuinely likely to threaten Australia's national security, and in other situations where secrecy serves a legitimate and compelling public interest. We are not transparency absolutists. However, national security has too often been over-utilised as a justification for the secrecy offences, keeping public interest information secret, despite there being no demonstrable threat to national security. As Justice Finn famously said in *Bennett v President, Human Rights and Equal Opportunity Commission*, "[o]fficial secrecy has a necessary and proper province in our system of government. A surfeit of secrecy does not."[3]

In his October 2023 National Press Club address, eminent journalist and press freedom advocate Peter Greste warned against the use of national security rhetoric as a tool to shut down efforts for transparency.[4] As it stands, the secrecy provisions in the *Criminal Code* encroach beyond what is reasonable for the protection of national security.

---

[1] Attorney-General's Department, *Review of Secrecy Provisions,* (Consultation Paper, March 2023) https://consultations.ag.gov.au/crime/review-secrecy-provisions/user_uploads/review-secrecy-provisions-consultation-paper.pdf (*AGD Secrecy Provisions Consultation Paper)*; Peter Greste, 'Australia's secrecy laws include 875 offences. Reforms are welcome, but don't go far enough for press freedom,' *The Conversation* (online, 21 November, 2023) <https://theconversation.com/australias-secrecy-laws-include-875-offences-reforms-are-welcome-but-dont-go-far-enough-for-press-freedom-218234>.

[2] Damian Cave, 'Australia May Well Be the World's Most Secretive Democracy', *The New York Times* (online, 5 June 2019) <https://www.nytimes.com/2019/06/05/world/australia/journalist-raids.html>.

[3] [2003] FCA 1433 [98].

[4] Peter Greste, 'Protecting Whistleblowers and Press Freedom in the Digital Era' *National Press Club Australia* (17 October 2023).

Any changes to the *Criminal Code* that follow this review should substantially improve the circumstances of former and current Commonwealth officers ('insiders'), as well as third party 'outsiders' engaging with official information, who see wrongdoing in government and seek to speak up. In doing so, we can shift the needle towards transparency, accountability and good governance – in a way which addresses the false binary that transparency and national security are in tension, not mutually-reinforcing. Through properly calibrated frameworks, core democratic values of transparency and accountability, so often achieved through whistleblowing and public interest journalism, strengthen rather than undermine our national security.

We welcome the INSLM's review of the *Criminal Code* in line with the principles of effectiveness, protection, proportionality, appropriateness and alignment with Australia's international human rights obligations,[5] and urge robust recommendations for reform. Through our responses to the Issues Paper, we make the following recommendations:

> **Recommendation 1:** Administrative sanctions should be preferred over criminal sanctions for minor breaches of secrecy obligations by public servants and contractors. This preference should be reflected by the repeal of lower-level secrecy offences.
>
> **Recommendation 2:** The *Criminal Code* should not reflect the 'mosaic effect' in any form. Alternatively, it should only be utilised in relation to special categories of insiders – such as intelligence officers, who might reasonably be aware of the mosaic effect and the derivative risk of the publication of otherwise non-sensitive information.
>
> **Recommendation 3:** The penalties in Part 5.6 of the *Criminal Code* should be reduced, to levels that are necessary and proportionate.
>
> **Recommendation 4:** 'Dealing with' offences should be significantly narrowed to only apply to 'insider-insider' contexts and meet a threshold of causing risk of serious harm.
>
> **Recommendation 5:** Secrecy offences applying to third-party, non-Commonwealth officers should be repealed. Alternatively, communicative secrecy offences should only apply to non-Commonwealth officers in extremely narrow circumstances, and 'dealing with' offences should have no application to non-Commonwealth officers.
>
> **Recommendation 6:** The Attorney-General should issue the Commonwealth Director of Public Prosecutions with guidance on considering the public interest test when deciding whether to prosecute whistleblowers and journalists.
>
> **Recommendation 7:** The Commonwealth Director of Public Prosecutions should issue explanations of its decisions to prosecute under Part 5.6 of the *Criminal Code*.
>
> **Recommendation 8:** For serious offences by Commonwealth officers with a harm element, there should be a requirement for 'serious harm.'

[5] Independent National Security Monitor, 'Secrecy Offences in Part 5.6 of the Criminal Code 1995', *Secrecy Review* (Web page) <https://www.inslm.gov.au/node/268#:~:text=In%20January%202024%20the%20INSLM,public%20hearings%20will%20be%20held>.

Recommendation 9: Aggravated offences in section 122.3 of the *Criminal Code* should be abolished. Alternatively:

1. For an offence in section 122.1 to be an aggravated offence, there must be an element of 'serious harm' introduced; and
2. For an offence in section 122.2 to be an aggravated offence, the current threshold must be upgraded to 'serious harm.'

Recommendation 10: There should not be a new offence inserted into Part 5.6 that applies to disclosure of information that is prejudicial to the effective working of government.

Recommendation 11: 'Classified information' should be defined in more narrow and specific terms.

Recommendation 12: The journalist defence in section 122.5(6) should be framed as an exemption, and a fail-safe general public interest defence made available.

Recommendation 13: Additional avenues for disclosure of intelligence information should be established in Australia, including through parliament and external disclosures.

In addition to what follows, we note our recent submissions to the Attorney-General's Department's review of secrecy offences,[6] and to the same Department's ongoing consultation over reform to federal public sector whistleblowing provisions.[7] It is our firm belief that reform on these issues must be achieved in tandem, to ensure secrecy provisions are appropriately calibrated through robust, effective whistleblowing pathways. Otherwise, as was said in response to the prior reform, expanding secrecy offences without fixing inadequate whistleblowing laws is to put the cart before the horse.

[6] Human Rights Law Centre, Transparency International Australia and Griffith University's Centre for Governance and Public Policy, Submission to the Secrecy Provisions review by the Attorney-General's Department, 12 May 2023 ('*Joint Submission to the Secrecy Provisions Review*').

[7] Human Rights Law Centre, 'Pathway to Protection: Reforming the *Public Interest Disclosure Act 2013* (Cth) on the Road Towards Comprehensive, Best-Practice Federal Whistleblower Protections', Submission to the Attorney-General's Department review of the Public Interest Disclosure Act, January 2024 ('*HRLC PID Act Review Submission*').

2. Responses to the Issues Paper

We respond to the issues identified in the Issues Paper as follows.

Administrative sanctions for secrecy offences should be favoured over criminal sanctions

Addressing Question 1 in the Issues Paper

Administrative mechanisms are useful tools to address minor breaches of secrecy obligations by staff and contractors. Disciplinary action and the loss of security clearance, among other administrative tools, should be preferred over criminal sanctions for lower-level breaches. We support the Australian Law Reform Commission's position that "administrative and disciplinary frameworks play a central role in ensuring government information is handled appropriately."[8] Such arrangements have a major deterrent effect on misuse of government information, given the significant impact disciplinary action, or loss of security clearance, can have on the career of a public servant.

Criminal sanctions should be a last resort, with administrative sanctions deployed in most cases. With broader use of administrative sanctions, the requirement for criminal offences for lower-level secrecy breaches becomes unnecessary. As the Issues Paper notes, there have been no prosecutions under Part 5.6 of the *Criminal Code,* although it should be noted that the chilling effect of Part 5.6 on whistleblowers is real and significant – whether or not prosecutions have taken place.

> **Recommendation 1:** Administrative sanctions should be preferred over criminal sanctions for minor breaches of secrecy obligations by public servants and contractors. This preference should be reflected by the repeal of lower-level secrecy offences.

Transparency is not a threat to national security

Addressing Question 4 in the Issues Paper

Transparency and national security do not exist in a binary, as rhetoric, legislation and recent prosecutions of high-profile whistleblowers might suggest.[9] Peter Greste, in his October 2023 National Press Club address, warned against the use of national security as a rhetorical and nebulous theme to shut down "uncomfortable journalism" and efforts for transparency.[10]

---

[8] Australian Law Reform Commission, Secrecy Laws and Open Government in Australia: Report (Report No 112,
December 2009) <https://www.alrc.gov.au/wp-content/uploads/2019/08/ALRC112.pdf> ('*ALRC Secrecy Laws Report*').

[9] See generally Alliance for Journalists' Freedom, Submission to the Attorney-General's Department, Review of Secrecy Provisions (May 2023) 17; Australia's Right to Know, Submission to the Attorney-General's Department, Review of Secrecy Provisions (5 May 2023) 25.

[10] Peter Greste, 'Protecting Whistleblowers and Press Freedom in the Digital Era' *National Press Club Australia* (17 October 2023).

We submit that it is, in fact, oppressive secrecy which undermines national security. Transparency is a vehicle for national security, and good and accountable government. We would encourage the INSLM to reflect this proposition in this review of the *Criminal Code*, by ensuring any limitations on transparency and accountability are no more than what is necessary and proportionate, having regard to the democratic significance of these values.

The mosaic effect is inconsistent with the principles of criminal responsibility

Addressing Question 6 in the Issues Paper

It is our view that the mosaic effect or method of 'mosaic analysis', as referred to in the Issues Paper, does not align with the principles of criminal responsibility set out in the *Criminal Code*, or the rule of law more broadly.

Section 5.1(1) of the *Criminal Code* sets out that there must be a fault element of an offence which could be intention, knowledge, recklessness or negligence. The scope of 'intention' or ' knowledge' is too broad when applied to the disclosure of information by one person, where that information *could* be used by a third party, in conjunction with other information, to deduce some other broader information. The discloser cannot intend or know the actions of an unknown hypothetical third party, and they should not be responsible for the third parties' actions. As the Issues Paper sets out at [1.49], "the individual making one disclosure may not know what other information has been, or may be in future be disclosed, by others." We agree with the Issues Paper that this is of greater concern for non-Commonwealth officers.

Section 10.1 of the *Criminal Code* outlines the principle that a person cannot be held criminally responsible if there is intervening conduct or an event brought about by a third party, which the person has no control over. This seems to be contrary to the use of the mosaic effect in relation to secrecy offences. Where the principle is retained, its use should be limited to special categories of insiders, such as intelligence officers, who might be considered to be 'insider-insiders', given the acute nature of the information in their possession, and their special knowledge of the risks attaching to unauthorised disclosure of that information, including via mosaic analysis.

> **Recommendation 2:** The mosaic effect should not be reflected in the *Criminal Code* in any form. Alternatively, it should only be utilised in relation to special categories of insiders – such as intelligence officers, who might reasonably be aware of the mosaic effect and the derivative risk of the publication of otherwise non-sensitive information.

Part 5.6 of the *Criminal Code* has negative impacts on whistleblowers, journalists and civil society groups

Addressing Question 7 in the Issues Paper

The existence of Part 5.6 of the *Criminal Code* has had a significant impact on civil society groups, whistleblowers, journalists and legal practitioners.

<u>Whistleblowers: current and former Commonwealth officers</u>

The secrecy provisions in Part 5.6 of the *Criminal Code* encroach on freedom of expression. The effect of this encroachment is to silence and create a chilling effect on whistleblowers, and the journalists seeking to support their disclosures.

The broad scope of secrecy offences in Part 5.6 that apply to potential whistleblowers, coupled with the severe criminal liability that attaches, significantly limits public sector whistleblowing. If an aggravating factor in section 122.3 applies, offences with a three-year imprisonment term increase to five, and offences with a seven-year imprisonment term increase to 10. These penalties, which were significantly increased from prior levels when the *Criminal Code* reform was introduced, are disproportionate and draconian. They should be reduced.

These provisions significantly hinder Commonwealth officers or former officers who fear gathering, engaging with or coming forward with any evidence of wrongdoing in the public sector. We see this frequently in practice, where our clients have grave concerns about secrecy offences. We commonly hear comments to the effect of: "I want to blow the whistle, but I don't want to go to jail." The fear is exacerbated by the limited, technical offences in Part 5.6, and the unsatisfactory state of Australia's present whistleblower protection framework (which might otherwise ameliorate the worst of the secrecy provision's excesses).

The ongoing prosecution of tax office whistleblower Richard Boyle, although not charged under these offences (as the alleged offending predates the reformed provisions), is indicative of these issues. Boyle argued that he was immune from prosecution as his whistleblowing – internally at first, then to oversight bodies, then to the media as a last resort – was pursuant to the *Public Interest Disclosure Act 2013* (Cth) (***PID Act***).[11] However, most of the charges related not to Boyle's whistleblowing per se, but anterior conduct – taking documents, recording conversations and so on – in preparation for making an internal disclosure.[12] At first instance, Kudelka J of the District Court of South Australia held that this prior conduct was not protected by the *PID Act*'s immunity, even where it was reasonably necessary for the whistleblowing.[13] That judgment is subject to appeal, and the Court of Appeal of South Australia is presently reserved (the Human Rights Law Centre participated in the appeal as a friend of the court).

The *Boyle* case underscores the risks posed by the overbreadth of the *Criminal Code*'s secrecy provisions, given the current inadequacies of federal whistleblowing law. It is readily imaginable that a public servant who otherwise blows the whistle properly and consistently with the *PID Act* could be prosecuted under dealing with offences in relation to prior conduct (such as photocopying and then taking home a document, to provide to an oversight body, or a journalist, in situations otherwise permitted under the *PID Act*). Current 'dealing with' offences should be significantly narrowed and limited to only what might be described as 'insider-insider' contexts – those in the public service, such as intelligence operatives, who are dealing with intelligence or national security information that is likely to have a significant impact on the public interest if disclosed. Administrative sanctions are otherwise sufficient to respond to these circumstances.

> **Recommendation 3**: The penalties in Part 5.6 of the *Criminal Code* should be reduced, to levels that are necessary and proportionate.

[11] *Boyle v Commonwealth Director of Public Prosecutions* [2023] SADC 27 [1].
[12] Ibid [2]-[5].
[13] Ibid.

Recommendation 4: 'Dealing with' offences should be significantly narrowed to only apply to 'insider-insider' contexts, and meet a threshold of causing risk of serious harm.

Legal practitioners: non-Commonwealth officers

Part 5.6 of the *Criminal Code* has had a significant negative impact on access to justice by impeding whistleblowers' avenues for legal representation and imposing the spectre of liability on lawyers approached by potential clients in the national security context.

The Human Rights Law Centre has previously submitted that section 122.4A of the *Criminal Code,* which covers communication and dealing with information by non-Commonwealth officers, should be abolished entirely.[14] We reiterate this position. Section 124.4A extends to non-Commonwealth officers, which includes everyone, including journalists who might receive public interest disclosures, lawyers who seek to provide advice to potential clients and civil society organisations who may receive whistleblowing complaints.

The provisions in 122.4A for communicating and dealing with information by non-Commonwealth officers have caused ongoing concern for us in relation to our ability to advise and represent clients. The *PID Act* enables public servants to make protected disclosures to legal practitioners for the purposes of seeking advice or representation. However, it entirely excludes such disclosures where the information is intelligence information, and partially excludes such disclosures where the information has a "national security or other protective security classification" (unless the lawyer holds a suitable security clearance). This means that the Project cannot advise whistleblowers in relation to such matters. The intake guidelines on our website outline that we are unable to receive intelligence information or information with a national security or other protective security classification. We outline to prospective clients that sending us any material in these circumstances may be a criminal offence.

However, given the breadth of the *Criminal Code* third party provisions, there is a possibility that mere receipt of such information – even in circumstances where we are actively discouraging such disclosures – could leave our staff criminally liable. This risk is heightened in situations where the immunity provided by the *PID Act* uses undefined language without clear content – preventing disclosure to legal practitioners (without appropriate security clearances) where the matter involves information with 'national security or other protective security classification.' The third party offences in the *Criminal Code* have posed serious, ongoing concerns for us in the operation of our legal services to clients. The imposition of potential liability in these circumstances is not necessary or proportionate and the law should be amended to remove or significantly reduce application to lawyers and other third parties who are not actively soliciting receipt.

To consider a readily-imaginable hypothetical. The Human Rights Law Centre actively promotes the availability of our Whistleblower Project to provide legal advice to potential whistleblowers. Say an intelligence officer was concerned about corruption within their agency, and wanted to speak up through appropriate channels. They contacted our Whistleblower Project through our intake portal, failing to observe our warnings that we cannot assist intelligence whistleblowers. Or, they may think, wrongly, that intelligence information is limited to actual sensitive information, not the much wider scope of the relevant definitions in section 41 of the *PID Act*. A junior lawyer at the Project receives the intake submission, and grows concerned that the information contained therein is

[14] *Joint Submission to the Secrecy Provisions Review* (n 6) 6-7.

intelligence information. There is, first, a very real possibility that this lawyer's mere receipt of the information could constitute an offence under the 'dealing with' offence in s 122.4A(2), with ss 90(1) and 121.1 together defining 'deal' as including to receive or obtain information. Seemingly, all the other elements of the s 122.4A(2) offence are satisfied. The s 122.5(4) defence in relation to the *PID Act* would not be available, given the blanket exclusions for intelligence whistleblowing in that law. Nor would the s 122.5(5A) defence arise, given the dealing with was not for the purpose of legal advice in relation to the operation of the *Criminal Code* itself, but in relation to reporting wrongdoing.

The Human Rights Law Centre has processes and procedures governing what our staff are to do if, contrary to our instructions to the contrary, we are contacted by people seeking legal advice in relation to intelligence or national security matters. These processes and procedures have been informed by expert advice by pre-eminent senior counsel, to minimise the risk of any liability.

However, say that, contrary to those procedures, in a fit of panic, troubled by the receipt of this information, the lawyer copies the details from our intake portal into an email, to send to a supervising lawyer in our practice alerting them to their concerns. That lawyer may now be in further breach of s 122.4A(2) – with 'deal' also encompassing making a record of something, or copying something, at s 90(1) – and then, if they went ahead and sent the email, s 122.4A(1), for now communicating that information.

In our view, this potential criminal liability, for mere receipt and internal practice management of information that we take active steps to avoid, is disproportionate and unnecessary. In its recent *Review of Secrecy Provisions: Final Report*, the Attorney-General's Department concluded: "unsolicited receipt or other unwitting dealings will not be sufficient to reach the threshold of intention required."[15] As such, the Department concluded amendments were not required. We acknowledge that the need to demonstrate intention (as the fault element for s 122.4A(2)(a) limits the risk of liability. However, the expanded approach to intention in s 5.2 means that it is not certain that 'mere receipt' could never give rise to liability. Additionally, in circumstances where there was subsequent internal communication, the fault elements would be satisfied.

To all of this it might be said that (a) it is extremely unlikely such a matter would be prosecuted; this is particularly so where, (b) the Whistleblower Project has taken steps to actively disclaim receipt of such information. That may be so. But we use this not-farfetched example to demonstrate the sweeping breadth of s 122(4A) as presently framed, and its significant impact on organisations such as ours. We were fortunate to receive extensive, pro bono advice in assessing how to mitigate these risks and comply with the *Criminal Code*. Not all organisations are so fortunate. That there is significant uncertainty about the scope of liability of third parties for mere receipt points to defects in the law. It should not be up to third parties to take active steps to avoid liability for merely receiving, unsolicited, information.

> **Recommendation 5:** Secrecy offences applying to third-party, non-Commonwealth officers should be repealed. Alternatively, communicative secrecy offences should only apply to non-Commonwealth officers in extremely narrow circumstances, and 'dealing with' offences should have no application to non-Commonwealth officers.

[15] Attorney-General's Department, *Review of Secrecy Provisions* (Final Report, 2023) 38 < https://www.ag.gov.au/sites/default/files/2023-11/secrecy-provisions-review-final-report.pdf>.

Low priority should be given to investigations where no evidence of harm involving journalists

Addressing Question 8 in the Issues Paper

We generally support the practice of giving low, or no, priority to investigations where: (i) there is no evidence of harm; and (ii) it involves journalists or media organisations. However, reliance on selective enforcement of investigations is not a comprehensive solution or an answer to the issue of overcriminalisation of non-Commonwealth officers within the *Criminal Code*.

Further, reliance on the Operational Prioritisation Model referenced in the Issues Paper, a model subject to change, does not provide journalists or whistleblowers with any certainty that they will or will not be prosecuted, based on the Australian Federal Police's assessment of harm. It is not sufficient for the Issues Paper at [1.31] to assess that it is "unlikely a breach would be given a high priority if there was very little or no evidence of potential harm," when it remains a criminal offence nonetheless. The chilling effect of these offences is very real, whether or not they are actively prosecuted in circumstances not involving evidence of real or potential harm.

The Commonwealth Director of Public Prosecutions must consider the public interest before a prosecution

Addressing Question 9 in the Issues Paper

The Human Rights Law Centre has previously submitted that the Attorney-General should issue the Commonwealth Director of Public Prosecutions (**CDPP**) with guidance on the factors to be considered when deciding whether to prosecute whistleblowers and journalists.[16] We reiterate this submission and suggest this guidance should sit alongside the *Prosecution Policy of the Commonwealth* and must include consideration of the public interest test. We also suggest that the CDPP issue explanations of its own decisions to prosecute under Part 5.6 of the *Criminal Code*, given the significant public interest in any secrecy offence prosecution.

> **Recommendation 6:** The Attorney-General should issue the Commonwealth Director of Public Prosecutions with guidance on considering the public interest test when deciding whether to prosecute whistleblowers and journalists.
>
> **Recommendation 7:** The Commonwealth Director of Public Prosecutions should issue explanations of its decisions to prosecute under Part 5.6 of the *Criminal Code*.

A threshold of 'serious harm' should be adopted for serious offences

Addressing Questions 10 and 11 in the Issues Paper

As we outlined above, in our view all offence penalties, serious and general, should be reduced to ensure proportionality across all offences. A further aspect of this

[16] *Joint Submission to the Secrecy Provisions Review* (n 6) 10.

recommendation is the adoption of a requirement of 'serious harm' for offences attracting serious penalties.

Serious offences by Commonwealth officers are offences involving communication of information that attract a term of imprisonment of seven years, as found in sections 122.1(1) and 122.2(1). For serious offences, the provisions should require the communication of information to have 'caused serious harm', be 'likely to cause serious harm', or 'intended to cause serious harm', to an essential public interest such as Australia's security or defence. It follows that serious offences and higher penalties should follow a higher threshold of harm.

We note that the focus on a harm requirement is consistent with prior recommendations of the Australian Law Reform Commission.[17]

> **Recommendation 8:** For serious offences by Commonwealth officers with a harm element, there should be a requirement for 'serious harm.'

Aggravated offences should be repealed or reduced

Addressing Question 12 in the Issues Paper

Aggravated offences in section 122.3 should also align with the principles discussed above. Aggravated offences under section 122.3 have the effect of increasing serious offences in sections 122.1 and 122.2 from seven years to ten, and for smaller offences in these sections from three to five years.

These penalties are already significant, and making them aggravated offences, without reference to harm caused, is not a proportional approach. Aggravated offences should be abolished entirely, or a serious harm requirement adopted.

> **Recommendation 9:** Aggravated offences in section 122.3 of the *Criminal Code* should be abolished. Alternatively:
>
> 1. For an offence in section 122.1 to be an aggravated offence, there must be an element of 'serious harm' introduced; and
> 2. For an offence in section 122.2 to be an aggravated offence, the current threshold must be upgraded to 'serious harm'.

Secrecy offences need to be harmonised

Addressing Question 13 in the Issues Paper

The Human Rights Law Centre supports the harmonisation of the many secrecy offences scattered across the federal statute book. We therefore support the centralisation of secrecy offences in the *Criminal Code*.

[17] *ALRC Secrecy Laws Report* (n 8) 119.

Policy frameworks are not appropriate tools to determine security classifications

Addressing Question 17 in the Issues Paper

It is not appropriate for a policy framework to dictate whether information has been applied the correct security classification. This is particularly relevant for the application to criminal offences. Policy frameworks, such as the *Protective Security Policy Framework,* may change at any time, with changes in government or senior leadership. It cannot be incumbent on those in the public sector to keep up with these potential changes, with such severe penalties for failing to do so, in a way that legislative change prevents.

When considering lower-level classifications of information, the application of a policy framework is even less desirable, as inconsistency of its application becomes even greater. The communication, dealing or otherwise of poorly or inconsistently classified information becomes a real risk under this model.

An 'interference with' offence must adopt a threshold of serious harm

Addressing Question 22 in the Issues Paper

We reiterate the general principles of this submission that all penalties in Part 5.6 of the *Criminal Code* should be reduced. An offence that attracts a potential penalty of seven years' imprisonment should incorporate actual, serious harm as an element.

'Prejudice to the working of government' is too broad

Addressing Question 25 and 26 in the Issues Paper

The Australian Law Reform Commission, in its seminal, deeply-considered review into secrecy laws, reached the view that "to warrant a criminal penalty, disclosures must harm more than the effective working of government or commercial or personal interests." We agree.[18]

> **Recommendation 10:** There should not be a new offence inserted into Part 5.6 that applies to disclosure of information that is prejudicial to the effective working of government.

The impact of 'dealing with' offences on non-Commonwealth officers is significant and detrimental

Addressing Question 27 in the Issues Paper

Broadly, the Human Rights Law Centre maintains its previously submitted position that sections 122.4A(1) should be refined and section 122.4A(2) should be abolished. In our May

[18] *ALRC Secrecy Laws Report* (n 8) 274.

2023 submission to the Attorney-General's Department, the Human Rights Law Centre outlined section 122.4A(1) is:

> "*…extremely wide. While its effect is somewhat mitigated by the available defences, its scope goes beyond what is justifiable to impose on 'outsiders'. We would recommend that the provision be recast to require intent as to the harm caused by the communication, and those categories of harm be narrowed. The maximum term should also be reduced, to reflect the fact that it applies to Australians at large rather than a defined category with pre-existing confidentiality obligations.*"

And that section 122.4A(2):

> "*…is even more problematic. It applies in relation to the same elements, but for dealing with information, rather than communicating it, with a maximum penalty of two years. The lack of clarity around the breadth of 'deals with information' means that it is possible that the receipt of information, even unsolicited, could give rise to criminal liability. We would recommend that s 122.4A(2) be repealed in its entirety.*"

We refer to our answers above at Question 7 regarding the impact of Part 5.6 of the *Criminal Code* on civil society groups, including on the Human Rights Law Centre.

The definition of 'classified information' is unclear

Addressing Question 28 and 29 in the Issues Paper

We refer to our answers above and reiterate that section 122.4A relating to non-Commonwealth officers in Part 5.6 of the *Criminal Code* should be abolished or substantially amended.

Security classified information for the purposes of section 122.4A relating to non-Commonwealth officers is defined as 'information that has a security classification.'[19] 'Inherently harmful information' also means information that is security classified information.[20]

Non-Commonwealth officers, including journalists and those from civil society organisations, cannot reasonably be expected to know if or how information is classified, including the significance and risk of certain levels of classification. It is not certain that these groups of people would know what type of information would have a security classification or how to identify if it does, and further that mere dealing with it might constitute an offence under section 122.4A. Given that section 122.4A presents a potentially passive criminal offence in relation to 'dealing with' offences, this opens up non-Commonwealth officers to even greater potential risk if they are unable to identify if the information is classified. For this reason, offences for non-Commonwealth officers must be contained, in line with our earlier recommendations.

The *Criminal Code* provides no guidance on what information is classified. In contrast, as evidenced in the INSLM's Annexure to the Issues Paper on the Five Eyes Secrecy Laws, the

[19] *Criminal Code 1995* (Cth) s 121.1 definition of 'security classified information' (*Criminal Code*).
[20] Ibid s 121.1 definition of 'inherently harmful information.'

United States does define the types of information that are classified information. There are also rule of law implications in having a criminal offence 'pick up' a policy document, the Protective Security Policy Framework, which may change from time to time.

> **Recommendation 11:** 'Classified information' should be defined in more narrow and specific terms.

The journalists' defence in s 122.5(6) must be an exemption, and there should be a general, fail-safe public interest defence

Addressing Question 30 in the Issues Paper

The journalists' public interest defence in section 122.5(6) of the *Criminal Code* must be re-framed as an **exemption**. In theory, journalists can utilise the public interest defence in section 122.5(6), however, they bear the evidentiary burden to prove the defence, and bear the cost and weight of prosecution. We are not aware of any cases where the defence has been tested. However, there is evidence that the defence has been insufficient to address the chilling effect of the *Criminal Code* reforms.[21] We note the approach adopted in the recent *Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Act 2023*, which excludes journalistic conduct from the scope of offences – see, for example, s 80.2H – and thereby exempts it rather than requiring a defence to be made out.

Further, we recommend the adoption of a **general public interest defence,** available where disclosure was made in the public interest, but where some other defence or exemption is not available. This is particularly relevant where the technical requirements of defences may not have been met – it would be a defence of last-resort when the public interest has been served by disclosure. We note our prior submissions in relation to the utility of such a fail-safe defence.[22]

Finally, Australia may look to international practice in safe avenues for disclosure through parliamentary processes. In the US and Ireland, whistleblowers have access to parliamentary avenues, or dedicated receivers for intelligence information, that ensure their safety from criminal prosecution.

US parliamentary avenues

In the US, the Permanent Select Committee on Intelligence of the United States House of Representatives and the Select Committee on Intelligence of the United States Senate, or any members of these Committees, are authorised to receive protected disclosures relating to intelligence information. This avenue includes disclosing matters of 'urgent concern' but is broader than that. The Office of the Whistleblower Ombuds also provides Congress with resources and training on working with whistleblowers and provides intelligence whistleblowers with guidance on making protected disclosures to Congress. In the absence of external avenues for disclosure in relation to intelligence information under the *PID Act*,

[21] Rebecca Ananian-Welsh, Sarah Kendall and Richard Murray, 'Risk and uncertainty in public interest journalism: the impact of espionage law on press freedom' (2021) 44(3) *Melbourne University Law Review* 764-811.
[22] *Joint Submission to the Secrecy Provisions Review* (n 6) 8-9.

consideration should be given to creating equivalent channels – such as to the Parliamentary Joint Committee on Intelligence and Security.[23]

The Disclosure Recipient in Ireland

Ireland's *Protected Disclosures Act 2014* provides a protected and independent avenue for intelligence, security, defence and international relations whistleblowing. Section 18 of the *Protected Disclosures Act 2014* outlines the type of intelligence, security, defence and international relations information that can be disclosed in certain circumstances to the 'Disclosure Recipient.' Schedule 3 of the *Protected Disclosures Act 2014* sets out the specifics of the Disclosure Recipient, including that they are to be a judge or retired judge of the High Court of Ireland, with an initial term of appointment of five years, to be appointed by the parliament. The Disclosure Recipient must report the disclosure to the relevant public body and recommend a course of action. This channel is available to anyone disclosing information that relates to national security, not just those employed by the military or intelligence services. Critically, this includes journalists.

Providing further avenues for protected public interest disclosures of intelligence information should be in addition to tightening defences and exemptions for journalists and whistleblowers.

> **Recommendation 12:** The journalist defence in section 122.5(6) should be framed as an exemption, and a fail-safe general public interest defence made available.
>
> **Recommendation 13:** Additional avenues for disclosure of intelligence information should be established in Australia, including through parliamentary avenues and external recipients.

Obtaining the consent of the Attorney-General necessary at this time

Addressing Question 33 in the Issues Paper

The requirement for the Attorney-General to give their consent before commencement of a prosecution is not preferable as a matter of principle, but in the absence of strong protections such as a general public interest defence, necessary in practice.

We agree with the Issues Paper at [3.25] that an effective use of the Attorney-General's consent is to "safeguard against over-classification of information." However, it may not be appropriate that the Attorney-General, in making this determination, takes advice from the agencies who set the classification of a specific piece of information in the first instance. This is a further reason that more specific definitions of 'classified information' would be helpful.

It would be appropriate and preferred for the Attorney-General to issue guidance to the CDPP setting out the matters to be considered when deciding whether to prosecute whistleblowers or journalists. This would be useful to both the CDPP in bringing a prosecution in the first instance, and achieving greater transparency in the Attorney-General's decision-making when consent is sought.

[23] *HRLC PID Act Review Submission* (n 7) 9, 12.

Conclusion

We commend the INSLM for undertaking this important review of the secrecy provisions in the *Criminal Code* and urge reform that would limit overly broad secrecy offences and thereby better support transparency and accountability in government. Transparency is not only the enabler of good government, decision-making and ethical practice, it is also a critically important democratic value. This review has the opportunity to change Australia's reputation as one of the most secretive democracies in the world and embrace transparency as an enabler of our national security, not its antithesis.