12 May 2015

Hon Roger Gyles AO QC
Acting Independent Security Legislation Monitor
PO Box 6500
CANBERRA ACT 2600

By email: INSLMsubmissions@pmc.gov.au

Dear Mr Gyles,

As you are aware, representatives of the Joint Media Organisations gave evidence at the public hearing of the current review of the impact on journalists in the operation of section 35P of the *Australian Security and Intelligence Organisation Act* (ASIO Act) (the Review of 35P). The material provided in this correspondence responds to questions taken on notice during the hearing and some further material for your consideration.

We take this opportunity to draw attention to the context of the issue at hand – that of public interest communication including public interest reporting – which the recent national security reforms has brought to the fore.

As articulated by the leaders of our nation, the current times pose an unprecedented set of circumstances, and the recent tranches of national security amendments have been made in response to activities on our shores and overseas. We believe that the Australian public has a right to know what is going on in our society at this time, as at any other time. However, the effect of section 35P, and the other offences for disclosure of unauthorised information (including those not relating to intelligence operations) is that no light is shone upon information that could help the public to understand the environment that is currently at play and may not ever me able to be reported. This is because the entire chain, from the source with information (including whistle-blowers) to journalists and editors, could expect to make a decision to self-censor or take their chances with the law and a risk of jail.

As representatives articulated at the public hearing, the media is not trying to reserve the right to catch intelligence agents out, or to threaten and undermine operations and lives. However, the effect of section 35P (and other unauthorised disclosure laws) means that in some circumstances there is no ability to report – even positively – how an operation took place, and caught or shut-down a threatening and illegal activity in our society.

Section 35P is an example of a law, but is not the only law, that places restrictions on public interest communication including public interest reporting.

Specifically, we were formally asked to comment on the following:

ALRC's Secrecy Laws and Open Government concerning requirements in disclosure offences to cause harm or intent to cause harm, and the AGD/ASIO submission that section 35P is consistent with those recommendations

Section 35P applies to any/all persons who may disclose information relating to an SIO. It is an offence under section 35P(1) to disclose information related to an SIO without it being required that the disclosure

causes harm or the person making the disclosure intends to cause harm. This is acknowledged, including by AGD/ASIO in a joint submission to the Review of 35P[1].

AGD/ASIO provide the following as the policy intention for section 35P(1): *'The basic offence is designed to reflect that the very disclosure of the existence and conduct of an SIO creates an unacceptable risk that the operation may be compromised, and that the safety of the participants (and potentially their family or associates) may be jeopardised.'*[2] The AGD/ASIO submission cites the Australian Law Reform Commission (ALRC) Report on Secrecy Laws and Open Government in Australia[3] (the ALRC Report) as a source of support for this policy rationale, including stating that *'The ALRC concluded that secrecy offences in respect of intelligence-related information did not need to include an element requiring proof of harm or intent to cause harm in making a disclosure, on the basis that the harm is implicit.'*

However, the ALRC Report (as it relates to the AGD/ASIO submission) was dealing with offences for disclosure by intelligence officers – not disclosures by any/all persons as 35P(1) does. The ALRC Report says:

> *'The ALRC considers that a prohibition on the disclosure of information obtained or generated by intelligence agencies is justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies. The existing* [Australian Intelligence Community] *(AIC) secrecy offences cover a limited range of people who handle intelligence information, namely officers and employees, and people with whom the agency has an agreement or arrangement. The ALRC considers that it is appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive intelligence information.'*[4]

And goes on the say:

> '*…the ALRC accepts that specific secrecy offences covering the disclosure of information obtained or generated by or on behalf of the AIC by officers in AIC agencies, or people subject to an agreement or arrangement with the AIC, do not necessarily need an express requirement of harm...'*[5]

The ALRC went on to consider different secrecy provisions pertaining to any/all persons, it found it acceptable where the provisions were narrowly tailored. The ALRC Report referenced examples of narrowly targeted provisions, and said: *'While these offences cover disclosures by 'any person', they are limited to particular information the disclosure of which causes, or is likely to cause, harm.'*[6]

We reference an issue previously raised about 35P – and crucial in this context – that it is not narrowly tailored. Rather, its boundaries are unknown as it is information that 'relates to' that is collected into its purview.

The broad scope of the information to which 35P(1) pertains, combined with the application of the provision to any/all persons means, in our view, that it is beyond what the ALRC Report considered appropriate in the circumstances.

---

[1] AGD/ASIO Joint submission to the review of 35P, http://www.dpmc.gov.au/sites/default/files/inslm/8%20-%20AGD%20and%20ASIO%20-%20joint%20submission_0.pdf, p10
[2] Ibid, p10
[3] 2009, http://www.alrc.gov.au/sites/default/files/pdfs/publications/ALRC112.pdf
[4] Ibid, at [8.62]
[5] Ibid, at [8.65]
[6] Ibid, at [8.76]

Impact of the disclosure offences applying to controlled operations by the AFP and law enforcement agencies (sections 15HK and 15HL of the Crimes Act) on the reporting of security matters

As was expressed at the hearing by media organisation representatives, we should have been much more agitated than we were about the introduction of the offences for unauthorised disclosures applying to controlled operations in 2010[7].

This could have been because other elements of law enforcement processes act as checks and balances of police operations, including that they work so closely with the public, and that the result of law enforcement operations eventually end up in the public arena (for example, courts action, and the court decides what is made public of law enforcement operations, and what is not). In short, the veil of secrecy – perceived or otherwise – does not exist as it does regarding intelligence gathering and intelligence operations.

However, we offer that the three tranches of national security law amendments introduced during 2014 and 2015 – of which section 35P is but one provision that concerns us – has shone a light on the issues that either restrict outright and/or making public interest reporting increasingly difficult. These comprise – but are not limited to:

- Inadequate protections for whistle-blowers;
- Inadequate protections for sources;
    - A combination of inadequate, non-uniform and in some states a lack of, shield laws;
    - Journalists' metadata able to be accessed for the purpose (or effect) of identifying sources; and
- Criminalising unauthorised disclosures, and therefore criminalising sources and journalists.

It is realistic to opine that the media attention to the most recent tranche of national security law amendments will have a chilling effect on those people willing to come forward with information because of logistics involved in 'safe' information transferal and criminal sanctions for disclosing, and also the ability for journalists to check the information that they receive – let alone having a story and deciding whether or not to broadcast or publish.

Lastly, we note that the AGD/ASIO submission claims that the absence of – or zero – prosecutions under the controlled operations unauthorised disclosure provisions proves that the provisions are *'not operating as an undue limitation on reporting of national security matter and that section 35P is not likely to operate as such a limitation'*[8]. As we discussed during the hearing, this is not a definitive conclusion. We put that an absence of prosecutions could also indicate an absence of disclosures, which is a realistic consequence of criminalising disclosures.

The distinction between section 35P and the more limited disclosure offences applying to ASIO's questioning and questioning and detention warrants (section 34ZS of the ASIO Act), and particularly any views you might have on the degree of weight placed on that distinction

We make no comment on the penalty structure within the ASIO Act, nor maximum penalty relating to the basis offence.

It may be useful to add here that it while the duration of the penalty that is an issue, the key problem is criminalisation itself – particularly as it criminalises sources and journalists, and inhibits public interest reporting.

[7] *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010*
[8] Op. cit, p15

Additional matters

ASIO whistle-blowers – internal process to IGIS

Section 8A of the *Inspector-General of Intelligence and Security Act 1986* extends the functions of the Inspector General for Intelligence and Security (IGIS) to cover disclosures of information allocated under section 43 of the *Public Interest Disclosure Act 2013* (PID Act) if the disclosable conduct to which the information is associated related to an intelligence agency.

As we outlined in our submission to the PID Act, and in other submissions including the Australian Law Reform Commission (ALRC) current 'Freedoms Inquiry'[9] the PID Act provides inadequate protections for whistle-blowers, particularly intelligence agency personnel who remain without protection if they make an external disclosure, and a lack of real avenue for other 'unauthorised' disclosures.

We note that the IGIS 2013-14 Annual Report[10] (the IGIS Report) states that between 15 January and 30 June 2014 the Office of the IGIS received one disclosure that directly fell within the PID scheme parameters. The IGIS Reports states that the disclosure was made in April 2014 *'by a former intelligence agency employee who raised concerns about an officer in another Australian government agency. In this case, the OIGIS referred the matter to the agency in question for investigation'.*

Additionally, the IGIS Report overviews the other PID cases that have been raised and allocated across the six intelligence agencies. The IGIS Report says: '*Investigations were completed in four of these before the end of the reporting year 2013–14. Cases have mostly involved a range of personnel management matters. One case involved administrative deficiencies in the procurement of external services, and the agency concerned has advised that investigation of this disclosure identified useful refinements to administrative processes'.*

This illustrates the point made at the hearing by media organization representatives that the whistle-blowing process for intelligence officers is contained within internal parameters and processes, and there is little transparency. Further, if the discloser is unsatisfied with the outcome of the internal process, there is no protection available for an external disclosure, and the risk of a criminal offence would likely discourage such a disclosure. Thereby activities which should be addressed (systemic or otherwise) may well go unaddressed due to the lack of *risk* of public exposure and accountability, notwithstanding the almost surety of lack of actual public exposure.

Could/should ASIO be compelled to answer media queries regarding section 35P?

Following consideration of this issue as raised during the hearing, we are of the view that this is not a cure for what we see as the issues that arise from section 35P for news gathering and reporting in the public interest.

We expand on this in the following scenario, but do not suggest that this is the only scenario that would deliver this outcome. Take, for example, the application of a rule that ASIO must tell you if information is not related to an SIO. We believe that an inquiry about information that would trigger this call to the 'media hotline' would likely not be responded for a range of reasons, including but not limited to:

- The information may not be about the SIO itself, by may be 'related' to an SIO – the risk is high in saying to the media 'no, that information is not related to an SIO;' and
- Whether the information was about an SIO or related to an SIO, it would be best that the information – which would likely be unauthorised otherwise the journalist would not be inquiring of

[9] Joint Media Organisation submission, http://www.alrc.gov.au/sites/default/files/subs/70._org_joint_media_organisations_final.pdf
[10] http://www.igis.gov.au/annual_report/13-14/pdfs/IGIS_annual_report_13-14.pdf

the media hotline as to its status – was not reported and therefore the question would likely not be answered. The story would likely not be written – regardless of whether the information related to an SIO or not – because while not saying the information related to an SIO, it was also not said that it did not.

We are of the view that a compulsion to answer media queries would likely leave the media in the same place as without it.