AUSTRALIAN
LAWYERS
FOR
HUMAN RIGHTS

20 April 2015

PO Box A147
Sydney South NSW 1235
DX 585 Sydney
alhr@alhr.org.au
www.alhr.org.au

The Hon Roger Gyles AO QC
Acting Independent National Security Legislation Monitor
PO Box 6500
Canberra ACT 2600

Email: INSLMsubmissions@pmc.gov.au

Dear Sir

Inquiry into section 35P of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act)

Thank you for your invitation of 30 March 2015 to Australian Lawyers for Human Rights (ALHR) to provide a submission in relation to the Inquiry referred to above.

ALHR was established in 1993 and is a national network of over 2600 Australian solicitors, barristers, academics, judicial officers and law students who practise and promote international human rights law in Australia. ALHR has active and engaged National, State and Territory committees and a secretariat at La Trobe University Law School in Melbourne. Through advocacy, media engagement, education, networking, research and training, ALHR promotes, practices and protects universally accepted standards of human rights throughout Australia and overseas.

1. Our concerns

1.1 ALHR's primary concerns are that Australian legislation (1) should not on its face breach the human rights[1] of persons affected by that legislation; and (2) should not be capable of being applied so as to infringe those persons' rights.

1.2 Section 35P of the ASIO Act imposes severe penalties on disclosure of information. That is, it restricts freedom of speech and freedom of the press, irrespective of any benefit which may result from the disclosure.

---

1 We follow here the definition in the *Human Rights (Parliamentary Scrutiny) Act 2011* of human rights as the rights and freedoms contained in the seven core human rights treaties to which Australia is a party. These treaties are: •International Covenant on Civil and Political Rights • International Covenant on Economic, Social and Cultural Rights •International Convention on the Elimination of All Forms of Racial Discrimination • Convention on the on the Elimination of All Forms of Discrimination against Women • Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment • Convention on the Rights of the Child • Convention on the Rights of Persons with Disabilities.

1.3 Where, as here, there is a clear countervailing national security interest, our concerns are that the legislation is:

- proportionate to the harm in question;
- contains appropriate safeguards for protecting the rights of individuals;
- contains appropriate transparency and accountability mechanisms; and
- recognises the public interest in the disclosure and suppression of unlawful activity.

1.4 We note that your Inquiry is to review any impact on journalists of the operation of section 35P. An impact on journalists is also necessarily an impact on any whistleblowers who seek to draw the attention of journalists to government employee misfeasance, in the absence of action by the government.

1.5 Legal protections for whistleblowing in relation to intelligence operations is understandably restricted, however this does not mean it should not exist at all. Whistleblowing protection is essential for good governance in all areas, including intelligence operations. Protection for the journalist is therefore inseparable from protection for the whistleblowers.

1.6 Our comments below are not confined to the impact on journalists or whistleblowers but of course apply to them as well as to all other affected persons.

2. Summary

2.1 We submit that:

2.1.1 the concept of 'recklessness' should be more fully spelt out in relation to the offence identified by Section 35P;

2.1.2 the offence should not apply to events which are no longer of major security relevance, for example by virtue of lapse of time;

2.1.3 further exceptions should be considered, including disclosure to parliamentarians;

2.1.4 a strong 'public interest' defence should be available in relation to Section 35P. This will strengthen our democratic system through enabling a check upon government action which is not in the public interest.

3. Background

3.1 We submit that in considering whether, in respect of Section 35P, the ASIO Act:

- contains any appropriate safeguards for protecting the rights of individuals;
- is proportionate to any threat of terrorism or to national security, or both (or unjustifiably encroaches on freedoms); and
- remains necessary;

it is appropriate to apply (1) international human rights standards and (2) the principles of transparency and accountability.

3.2 International law, including human rights standards, is a legitimate and important influence on the development of the common law, particularly where the common law on an area is uncertain or unsettled. It is a principle of the common law 'that statutes should be interpreted

and applied, so far as their language permits, so as not to be inconsistent with international law or conventions to which Australia is a party'.[2]

3.3 The protection of 'rights and fundamental freedoms' is not limited to where there is direct congruence with an existing human right under international law. Various common law protections exist even in the absence of a corresponding international human right.

3.4 In the light of the foregoing, we submit that the following documents set out appropriate principles to guide the Inquiry:

(a) *Guidance Notes 1 and 2* issued by the Parliamentary Joint Committee on Human Rights, December 2014;

(b) *Guide to Human Rights*, Parliamentary Joint Committee on Human Rights, March 2014;

(c) *Rule of Law Principles*, a Policy Statement of the Law Council of Australia, March 2011.[3]

3.5 In summary, those documents provide that laws encroaching on a freedom should:

(a) Be clear, accessible and precise so that people know the legal consequences of the limitations or the circumstances under which authorities may restrict the right or freedom;

(b) Be in pursuit of a legitimate objective;

(c) Be necessary in pursuit of that objective;

(d) Have a rational connection to the objective to be achieved;

(e) Apply to all people equally and not discriminate on arbitrary or irrational grounds;

(f) Be proportionate to the objective being sought (taking into consideration whether there are other less restrictive ways to achieve the aim, the impact of the legislation upon human rights, whether affected groups are particularly vulnerable, whether the merits of individual cases can be taken into account)[4];

(g) Contain effective and transparent safeguards or controls (including as to monitoring and access to review, public trial, no limitations on judicial discretion or information available to legal representatives, notification to persons affected by the legislation);

(h) Not be disproportionately severe (eg not involve reverse burden offences and/or strict liability offence);

(i) Not be retrogressive in terms of diminishing any existing rights or accepted norms, including international human rights norms;

(j) Only permit proportionate subordinate legislation (in particular, not subordinate legislation that creates new offences or confers new powers on executive agencies);

(k) Be transparent so that decisions made under the laws are open to scrutiny; and

(l) Enshrine accountability by specifying to whom the decision-maker is accountable, by what process, according to what standards and involving what effects.

3.6 If any of these standards or principles is not met we submit that, to that extent, the interference or encroachment is not justified.

---

2 *Momcilovic v The Queen* [2011] HCA 34, [18] per French CJ (referencing *Zachariassen v The Commonwealth* (1917) 24 CLR 166, 181 per Barton, Isaacs & Rich JJ; *Polites v Commonwealth* [1945] HCA 3; 70 CLR 60, 68-69 per Latham CJ, 77 per Dixon J, 80-81 per Williams J).

3 See also "Legislative Standards', 3 Sept 2013, accessed 16 Feb 2015 at http://www.lawcouncil.asn.au/lawcouncil/index.php/legislative-standards.

4 In our view, adherence to international human rights law and standards is also an indicator of proportionality.

4. Particular concerns in relation to interpretation of 'national security' issues

4.1 We submit that the fact that the harm addressed by Section 35P involves disclosure of a matter relating to national security which would otherwise be secret should not be a reason to avoid best practice review and public transparency standards.

4.2 An increased focus in respect of 'national security' in Australia in recent decades has involved a departure from previous review and public transparency standards. In response to 9/11, Australian legislation authorised the interception of non-suspects' communication,[5] allowed the Attorney General to issue warrants on the application of ASIO's Director General;[6] introduced a new regime allowing the government to intercept 'stored communications' – that is, communications sent across a telecommunications system and accessible to the intended recipient;[7] and allowed the Director-General of ASIO to apply to the Attorney-General for questioning and detention warrants.[8]

4.3 Effectively, Australia:

a. moved from largely relying on Australia's criminal law (with all its tested procedural safeguards) in promoting national security, to relying on a system that uses special provisions to target classes of people that may include innocent bystanders; [9]

b. moved from allowing judges to authorise the interception of communications to and from a telecommunications service in specific circumstances –where there were reasonable grounds for suspecting that a particular person was likely to use the service, and the information obtained was likely to assist the investigation of an offence in which the person involved - to a system that allows elected officials to issue such warrants on the ASIO Director-General's application;

c. expanded the scope of communications that the Government could monitor for the purposes of national security protection; and

d. included non-suspects within the class of persons numerous government and semi-government bodies could monitor.

4.4 The movement towards the wholesale monitoring of non-suspects - that is, of all Australians via their electronic metadata - has continued with the passing of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

4.5 We submit that a number of recent pieces of Federal legislation which have been presented to the Australian public as 'counter- terrorist' – as establishing a retaliatory and preventative framework in the 'war on terror' – are largely impractical, inconsistent with accepted human rights of Australian citizens and residents, and based upon amorphous and unsubstantiated foundations. In many areas they remove judicial overview and undermine the rule of law.

4.6 Counter-terrorism legislation by its very nature enshrines "extreme measures."[10] The initial (yet no less deeply disturbing) concern about this type of legislation is the "general willingness on

---

5 *Telecommunications (Interception) Amendment Act 2006* (Cth) sections 9 and 46.

6 Ibid, section 9(1).

7 Ibid, section 110.

8 *Australian Security Intelligence Organisation Act 1979* (Cth) Part III div III.

9 David Hume and George Williams, 'Who's Listening? Intercepting the telephone calls, emails and SMS's of innocent people" (2006) 31 *Alternative Law Journal*, 211; Kent Roach, *The 9/11 Effect: Comparative Counter-terrorism* (Cambridge University Press, 2011) 317; George Williams, 'A Decade of Australian Anti-terror Laws' (2011) 35 *Melbourne University Law Review* 1137; 1140; and George Williams, 'One year On: Australia's Legal Response to September 11' (2002) *Alternative Law Journal* 212.

the part of the public to accept greater civil liberties deprivations in the face of a specific threat."[11] In a predictable sequence, the enactment of legislation which restricts human rights on the basis of 'national security' then forms a pathway whereby such infringements 'bleed' into other areas of jurisprudence.[12] Sadly, these laws "reflect major problems of process and political judgment."[13]

4.7 Given that current and proposed Federal legislation in this area is potentially so deleterious to Australia's domestic human rights environment, it is of great concern that minimal attention has been given to the introduction of any 'check and balance' mechanisms, especially in the context that Australia is the one of the few democratic nations that cannot pride itself upon having an overriding 'check and balance' apparatus in the form of a Bill or Charter of Rights or Human Rights Act.[14]

4.8 Legislation such as the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*, the *Migration and Maritime Powers Legislation Amendment (Resolving the Asylum Legacy Caseload) Act 2014* and the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* are put to Federal Parliament on the basis that they will protect our country and the rights of its citizens and residents. But in responding to real fears (or, it might be argued, to a fear-based campaign), these pieces of legislation are crafted without adequate attention to rudimentary human rights concerns.

4.9 We note that the manner in which Australia responds to security concerns is in itself a measure of the strength and nature of our society. As noted by the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism in their *2010 Report*:

> *Compliance with human rights while countering terrorism represents a best practice because not only is this a legal obligation of States, but it is also an indispensible part of a successful medium and long-term strategy to combat terrorism.*[15]

4.10 That is to say, legislation which infringes our human rights is the very evil from which national security procedures are intended to protect us. We should not respond to terrorist threats by restricting our own human rights. To do so is to admit that in our attempt to oppose the terrorists we have given them effective control over us and our own legal system.

4.11 A fundamental concern with regard to such legislation is that singular, exceptional responses to a purported threat are translated into 'normalised' law and order methodology without cognizance of the collateral cost to the domestic human rights framework.[16] Such a state is a pathogenic environment where liberty is an expendable element, routinely expunged from consideration, and where procedural protections are substantively undermined.[17]

---

10 Ananian-Welsh R and Williams G, 'The New Terrorists : The Normalisation and Spread of Anti-Terror Laws in Australia' (2014) 38(2) *Melbourne University Law Review* (Advance Copy) at 2.

11 Baldwin F & Koslosky, D, 'Mission Creep in National Security Law' (2011) 114 *West Virginia Law Review* 669, 671.

12 Ibid at 672.

13 Williams G, "A Decade of Australian Anti-Terror Laws" (2011) 35 *Melbourne University Law Review*, 1136, 1163.

14 ibid at 1169.

15 Quoted in Australian Lawyers for Human Rights, *Submission to the Independent National Security Legislation Monitor*, 25 September 2012, par 8.

16 McGarrity N, 'From Terrorism to Bikies: Control Orders in Australia' (2012) 37 *Alternative Law Journal* 166, 168.

17 Ibid at 166.

5. Clarifying the concept of recklessness

5.1 The concept of recklessness in Section 35P is, according to a note to the version of the *ASIO Act* which appears on the Australian Legal Information Institute website, 'the fault element for the circumstance described in paragraph (2)(b)--see section 5.6 of the *Criminal Code'*. However there is no equivalent note in the version of the *ASIO Act* which appears on the ComLaw website.

5.2 Section 5.6 of the *Criminal Code* provides as follows:

> ***5.6 Offences that do not specify fault elements***
>
> *(1) If the law creating the offence does not specify a fault element for a physical element that consists only of conduct, intention is the fault element for that physical element.*
>
> *(2) If the law creating the offence does not specify a fault element for a physical element that consists of a circumstance or a result, recklessness is the fault element for that physical element.*

5.3 Given that 'disclosure' could be either an act or a result, it is submitted that at the very least clarification of the requisite element of intent would be of assistance. We note that a similar clarification is provided in Section 35M in relation to other provisions of the Act. Using similar language, we recommend at the very least adding an additional paragraph to section 35P reading along the following lines:

> *For the purposes of this section, a person is reckless about:*
>
> *(a) the existence of a special intelligence operation; or*
>
> *(b) whether information relates to a special intelligence operation and is capable of identifying to the general public that a special intelligence operation exists or existed* ***within the past [ ] years****;*
>
> *if:*
>
> *(i) the person is aware of a substantial risk that the information disclosed by them relates to a special intelligence operation which exists* ***or did exist within the past [ ] years***[18]*; and*
>
> *(ii) having regard to the circumstances known to the person,* ***including the likely extent of the harm or risk of harm created by the disclosure***,[19] *it is unjustifiable to take the risk that the information disclosed by them does not relate to a special intelligence operation*.

6. The time which has elapsed since the special intelligence operation

6.1 In its current form, Section 35P criminalises disclosure about any Australian special intelligence operation without any time limit. This is disproportionate and unnecessary. If the operation is long past, there may well be no current security reason for its continued secrecy. This will be a matter which depends upon the nature of each particular security operation. If a public interest defence is to be allowed, the length of time since the operation would be one of the matters that could be considered in the context of the extent of the harm or risk of harm created by the disclosure.

---

18 See section 6 below.

19 Again, this is relevant to the time which has elapsed since a past operation.

6.2 However if there is no public interest defence (as is currently the case), we submit that the issue of the time which has elapsed since the operation was carried out should be taken into account, particularly where the passing of time is relevant to the extent of the harm or risk of harm created by the disclosure.

6.3 We have therefore suggested the black wording in bold in the draft subsection included in Section 5.3 above. We would also recommend a consequential exception be included in Section 35P (3).

7. The degree of connection with the special intelligence operation

7.1 Section 35P is extremely widely drafted, so that the disclosure need only 'relate to' a special intelligence operation for the discloser to be convicted. This is an additional reason for the concept of recklessness to be clarified in relation to section 35P. If the discloser had no means of knowing that the information they disclosed would signal to – for example – the intelligence agencies of a foreign power that Australia had conducted a special intelligence operation, then the discloser should not be liable.

7.2 It is submitted that the wording 'relate to' is far too wide. Numerous types of disclosures can be imagined that 'relate to' a special intelligence operation but which do not disclose to the man in the street either that the operation existed or that it was a special intelligence operation (that is, which do not cause any general harm or risk by their disclosure).

7.3 This point overlaps somewhat with the previous one in Section 6, and to an extent this issue would not arise if the clause recommended in Section 5 above were adopted. The wording marked in blue in the clause relates to this issue.

8. Are the exceptions in subsection (3) wide enough?

8.1 As mentioned, the question of whether so much time has elapsed that disclosure of the operation no longer poses any security threat, and whether the nature of the information disclosed is capable of revealing the existence of a security intelligence operation could be included as an exception under Section 35P(3). We recommend that the exception should address all the points marked in bold and in blue in our draft clause in Section 5.3 above.

8.2 In addition, we recommend that:

a) disclosure to a member of State or Federal Parliament should be protected under subsection (3), irrespective of any other legislation, where a citizen has concerns as to the legality or appropriateness of the security operation. It is an appropriate democratic check and balance that citizens, including government employees, be able to confide in their MPs in relation to valid concerns about the operations of government bodies. This is particularly so in light of the fact that the Commonwealth *Public Interest Disclosure Act 2013* does not protect federal government whistleblowers in relation to intelligence matters; and

b) subsection (3)(e) should also cover legal advice in relation to the matter the subject of the offence, that is, the disclosure.

9. Public Interest defence

9.1 Finally, we strongly submit that a public interest defence should be included. This would apply to journalists (and whistleblowers) because of the media's vital 'public watchdog' role, but should not be limited to them. Discussion of topics of public concern is essential in a democracy.

9.2 Disclosure to the media and parliament, say Latimer and Brown, should be one of the foundations of a democratic society, and should be encouraged and protected.[20] Indeed, they say, disclosure to journalists and the media is so important that it is the truest example of 'whistleblowing' behaviour.[21]

9.3 We note that Australia does not have a central agency such as a Public Interest Disclosure Agency, which would otherwise be an appropriate body to which whistleblowers could resort before taking matters to a more public forum. In that absence, we do not think that it is appropriate to require disclosure to be made first to other government departments.

9.4 While the suggested wording does borrow from existing legislation in Australia (such as the *Public Interest Disclosure Act 2013*[22]) and other countries, it also departs from that legislation in several areas. For example, we do not think it is appropriate for the defence to have to prove that the matter disclosed would have amounted to a serious offence under Australian law, only that the discloser had a reasonable belief that the matter disclosed involved serious malfeasance or had serious public interest implications.

9.5 We suggest the inclusion of an additional section in the Act along the following lines:

35PA (1) No person is guilty of an offence under section 35P if the person establishes that he or she acted in the public interest.

(2) Subject to subsection (3), a person acts in the public interest if:

(*a*) the person acts for the purpose of disclosing an offence under an Act of Parliament, or similar substantial or serious misfeasance, whether or not amounting to an offence[23], that he or she reasonably believes has been, is being, or is about to be, committed by another person in the purported performance of that person's duties and functions for or on behalf of the Government of Australia; and/or

(*b*) the public interest in the disclosure on balance outweighs the public interest in non-disclosure.

(3) In deciding whether the public interest in the disclosure outweighs the public interest in non-disclosure, a judge or court must consider:

(*a*) the seriousness of the alleged offence;

(*b*) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;

(c) the nature of the public interest intended to be served by the disclosure;

(*d*) the person's reasonable belief as to the extent of the harm or risk of harm created by the disclosure;

(e) the person's reasonable belief as to the extent of the harm or risk of harm created by non-disclosure of the information;

(f) whether the person tried other reasonably accessible alternatives before making the disclosure in the way that they made it;

(g) whether no more information was publicly disclosed than the person

---

20 Paul Latimer and AJ Brown, 'Whistleblower Laws: International Best Practice' (2008) 31 (3) *UNSWLJ* 766, 781 citing Elletta Callahan, Terry Dworkin and David Lewis, 'Whistleblowing: Australian, 'UK and US Approaches to Disclosure in the Public Interest' (2004) 44(3) *Virginia Journal of International Law* 879, 905.

21 Latimer and Brown, op cit, citing Damian Grace and Stephen Cohen, *Business Ethics: Australian Problems and Cases* (1998) 150.

22 Note that this legislation specifically excludes conduct and information relating to intelligence agencies and intelligence information – see Section 26.

23 A person should not lose the protection of this defence because the misfeasance turns out not to include all the elements of an offence; the fact that the conduct appears to be harmful should be enough.

believed was reasonably necessary in the light of their perception of the extent or risk of harm involved; and

(*h*) the existence of exigent circumstances justifying the disclosure (including, but not limited to, whether the communication of the information was necessary to avoid grievous bodily harm or death).

If you would like to discuss any aspect of this submission, please email me at or call me on:

Yours faithfully

President
Australian Lawyers for Human Rights