Submission No 194

Inquiry into potential reforms of National Security Legislation

Name: **Stephen Keim**
President

Organisation: **Australian Lawyers for Human Rights**

AUSTRALIAN
LAWYERS
FOR
HUMAN RIGHTS

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

29 August 2012

PJCIS Secretariat
GPO Box 6021
CANBERRA ACT 2600
pjcis@aph.gov.au

Dear Secretary,

Inquiry into potential reforms of National Security Legislation

1. Australian Lawyers for Human Rights (ALHR) thanks the Parliamentary Joint Committee for Intelligence and Security for the opportunity to comment on the Inquiry into Potential Reforms of National Security Legislation.

2. ALHR was established in 1993. ALHR is a network of Australian lawyers and law students active in practising and promoting awareness of international human rights. ALHR has a national membership of over 2000 people, with active National, State and Territory committees. Through training, information, submissions and networking, ALHR promotes the practice of human rights law in Australia. ALHR has extensive experience and expertise in the principles and practice of international law, and human rights law in Australia.

3. In summary, in this submission, ALHR raises concerns about the foreshadowed general expansion of powers provided to intelligence and law enforcement agencies because of the potential of these powers to substantially prejudice the interests of members of the Australian public beyond those persons directly subject to any investigation. Such

powers must be carefully considered and there are insufficient safeguards foreshadowed to ensure that the rights of the public are not unacceptably encroached upon. Of particular concern is the proposed data retention scheme which has the potential to deleteriously impact the security of private data on Australian networks.

General Concerns

4. The framing of these legislative changes as urgent and important is unusual when one considers the amendment history for the *Telecommunications (Interception and Access) Act 1979* (Commonwealth) ("TIAA") or the *Australian Security Intelligence Organisation Act 1979* (Commonwealth) ("ASIO Act". The urgency is particularly concerning in the light of the more extensive COAG review of this same area of law, that seems to have been announced almost contemporaneously with this inquiry.[1]

5. Substantial amendments to any law that have the potential to prejudice the rights of those accused of crimes and to substantially intrude on the rights of ordinary, private citizens demand serious scrutiny. This is difficult to provide in the present case because insufficient detail is provided in the terms of reference to discern potentially important aspects of the intention of government concerning the changes.

6. Moreover, as the Independent National Security Monitor (**INSM**), Bret Walker SC, highlights in his 2011 Annual Report to Parliament, despite all the hyper counter terrorism legislating by successive Australian governments since 9/11, "*the most serious cases of terrorism could not be treated any more seriously under the CT Laws* [Australia's counter-terrorism and national security legislation] *than under pre-existing law.*"[2] The main tasks that the INSM is charged with is to ensure that:

> "Australia's CT [Australia's counter-terrorism and national security legislation] Laws are effective in deterring and preventing terrorism, are effective in responding to terrorism, **are consistent with Australia's international obligations and contain appropriate safeguards for protecting the rights of individuals**."
> (Emphasis added)

7. In the Report, Mr Walker SC quotes Lord Hoffman dissenting in *A v Secretary of State for the Home Department* [2005] 2 AC 68 (at 131-132 [95]-[97]), a case about the consistency of United Kingdom's counter terrorism laws with its international human rights treaty obligations concerning equality and the protection of individual rights:

> "Of course the Government has a duty to protect the lives and property of its citizens. But that is a duty which it owes all the time and which it must discharge without destroying our constitutional freedoms.
>
> ... Terrorist violence, serious as it is, does not threaten our institutions of government or existence as a civil community. ... The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws such as these. That is the true measure of

---

[1] *COAG Review of Counter-terrorism Legislation* (2012) Council of Australian Governments <http://www.coagctreview.gov.au/Pages/default.aspx> at 19 August.
[2] Independent National Security Monitor, *Annual Report 2011*, Commonwealth of Australia, 2012, 4.

what terrorism may achieve. It is for Parliament to decide whether to give the terrorists such a victory."[3]

8. In any assessment of Australia's counter terrorism and national security laws, it is vital to achieve an effective balance between the government's responsibilities (including international obligations) to protect its citizens from terrorism and its responsibilities and international obligations to preserve and promote its citizens' fundamental human rights. It is erroneous to cast the two events as opposed or mutually exclusive.

9. The Australian Government must ensure that the country's national security and counter-terrorism laws comply with our international obligations to respect and protect the rights of individuals. This was the purpose of creating and filling the INSM role. It is a continuing and important obligation. One way to fulfill this obligation is to respect and implement the recommendations of the INSM.

Privacy

> "The right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously. The Internet allows individuals to access information and to engage in public debate without having to reveal their real identities, for example through the use of pseudonyms on message boards and chat forums. Yet, at the same time, the Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of the Internet users' right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online."
>
> The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression[4]

10. ALHR are very concerned that the measures the government seeks to adopt to bolster national security and protect our democratic way of life will overstep the line and undermine that way and the fundamental rights and freedoms on which it depends.

11. The right to privacy is guaranteed by Article 12 of the *Universal Declaration of Human Rights 1948* ("UDHR") and Article 17 of the *International Covenant on Civil and Political Rights* ("ICCPR").

12. Many of the proposed amendments to the various Acts appear to ALHR to encroach unjustifiably on Australian citizens' right to privacy and thereby to contravene Australia's international obligations under various international human rights treaties to which it is a party.

The Universal Declaration of Human Rights 1948

---

[3] Ibid, 6.

[4] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue, 16 May 2011, para. [53] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

13. Article 12 of the UDHR provides:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

14. Article 19 of the UDHR provides:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

15. It is important to remember Australia's leadership in founding the United Nations and playing a prominent role in both the negotiation of the UN Charter in 1945 and in being one of the eight nations involved in drafting the UDHR. ALHR submits that Australia should continue its leadership in the field of international human rights by striking the appropriate balance between protecting civil liberties and implementing national security safeguards.

The International Covenant on Civil and Political Rights

16. Article 17 of the ICCPR provides:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks."

17. Article 17 provides for positive obligations on States parties to address the activities of private persons or entities. In ICCPR General Comment 16 on the Right to Privacy[5] the UN Human Rights Committee importantly stated:

> "1. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right...
>
> 3... Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.
>
> 4. The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. **In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law**. The introduction of the concept of arbitrariness is intended to guarantee that even

[5] ICCPR General Comment 16 (Thirty-second session, 1988): Article 17: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, A/43/40 (1988) 181 at paras. 1-11.

interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances." (emphasis added)

18. These international protections, against any arbitrary or unlawful interference apply to "correspondence". This includes not only written letters and the like, but also all forms of communication including communication via the internet[6] such as emails, chat board messages and social network postings.

19. Under Article 17(2), the Government has a comprehensive obligation "to regulate, through clearly articulated laws, the recording, processing, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as private parties".[7]

20. Furthermore, as stated in the UN Human Rights Committee's General Comment on the Right to Privacy, in complying with its legal obligations under the ICCPR, the Australian Government must ensure that:

> "In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files."[8]

21. Current privacy legislation at the Commonwealth level is largely comprised of the *Privacy Act 1988* (Commonwealth) ("Privacy Act") which provides a framework for how organisations[9] must deal with information that identifies people or may directly lead to the identification of a person (such as a tax file number) in accordance with the National Privacy Principles.[10] In addition, there is the role of the Privacy Commissioner[11] who has authority to make determinations in respect of breaches of privacy. By default, State and Commonwealth agencies are subject to the Act and the Commissioner is granted particular additional powers in respect of some government bodies, such as the Australian Taxation Office.[12]

22. Political parties[13] and a number of government agencies[14] escape scrutiny under the Act. Providing blanket protections to entire agencies seems at odds with the goals of the Act which states that, where an organisation holds a record that contains personal information, that person has a right to require correction or amendment of documents.[15] The same government agencies that are exempt from any such provisions are the same organisations

---

[6] M Nowak, *UN Covenant on Civil and Political Rights. CCPR Commentary* (Kehl am Rhein, Engel, 2005), 401.
[7] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedomof Opinion and Expression*, Frank La Rue, 16 May 2011, paragraph [58].
[8] UN Human Rights Committee, General Comment No. 16 on Article 17 of the ICCPR, paragraph 10.
[9] *Privacy Act 1988* (Cth) s 6C.
[10] Ibid, Schedule 3.
[11] Ibid, Part IV generally.
[12] Ibid, s 28.
[13] Ibid, s 7C.
[14] Ibid, s 7(1A), including ASIO, ASIS, ONA and the IGIS.
[15] Ibid, s 14 Principle 7, 2.

which have extraordinary powers in respect of detention,[16] in relation to the circumvention of evidentiary laws and due process,[17] and in respect of being exempt from administrative and judicial review.[18]

Role of Private Enterprise

23. ALHR supports the statements of the Special Rapporteur on the role of private enterprise in upholding fundamental human rights values that underpin our way of life:

> "[W]hile States are the primary duty-bearers of human rights, the Special Rapporteur underscores that corporations also have a responsibility to respect human rights, which means that they should act with due diligence to avoid infringing the rights of individuals. The Special Rapporteur thus recommends intermediaries to: only implement restrictions to these rights after judicial intervention; be transparent to the user involved about measures taken, and, where applicable, to the wider public; provide, if possible, forewarning to users before the implementation of restrictive measures; and minimize the impact of restrictions strictly to the content involved. Finally, there must be effective remedies for affected users, including the possibility of appeal through the procedures provided by the intermediary and by a competent judicial authority."[19]

24. ALHR supports endeavours by the government to improve existing privacy laws and suggests a requirement for mandatory disclosure of data breaches. Under the Privacy Act in its current form, organisations have no obligation to inform customers or interested parties if their data has been subject to unauthorised access. While criminal penalties exist for unauthorised access,[20] numerous other countries have mandatory disclosure laws that may help to mitigate the impact of access by criminal organisations to information such as credit card data.[21] Mandatory disclosure laws for data breaches would more effectively and consistently implement the Australian Government's international obligations to protect human rights including protecting the right to privacy under Articles 17 (and 16)[22] of the ICCPR.

25. Importantly, the UN Human Rights Committee has stated in ICCPR General Comment 16:

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated bylaw. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of

---

[16] ASIO Act, s 34E.
[17] Ibid, ss. 34ZS, 34ZT.
[18] Ibid, s 34ZW.
[19] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, above n 4, paragraph [76].
[20] These exist at state and commonwealth level, for example *Criminal Code Act 1995* (Cth) Schedule 1 Division 477.
[21] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) at 51.35 and 51.46.
[22] Article 16 of the ICCPR is written in identical terms to Article 17 except it expressly affords such rights to children who these days are significant users and creators of online data.

persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."[23]

Data Retention Schemes

26. Data Retention Schemes, as proposed in the foreshadowed changes to the national security laws, provide a significant additional requirement for organisations to maintain records that would, in other contexts, ordinarily be subject to the Privacy Act.

27. ALHR shares and echoes the concerns of the Special Rapporteur who notes that:

> "The right to privacy is essential for individuals to express themselves freely[24]... [T]he Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."[25]

28. The Special Rapporteur further states that:

> "The Special Rapporteur is deeply concerned by actions taken by States against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism. While such ends can be legitimate under international human rights law, surveillance often takes place for political, rather than security reasons in an arbitrary and covert manner.[26]
> ...
> A number of States are also introducing laws or modifying existing laws to increase their power to monitor Internet users' activities and content of communication without providing sufficient guarantees against abuse."[27]

29. Each year, under the TIAA, there are disclosure requirements, which frame the volume of material that has been made accessible to law enforcement and intelligence agencies, both as part of a telecommunications interception warrant and in relation to requests which do not require a warrant to effect. In 2011 alone, nearly three and a half thousand telecommunications interception warrants were granted and more than 240,000 warrantless access authorisations were made.[28]

30. Such a substantial use of existing powers under the TIAA suggests that the existing

---

[23] ICCPR General Comment 16, above n. 5
[24] Ibid, paragraph [53].
[25] Ibid, paragraph [20].
[26] Ibid, paragraph [54].
[27] Ibid, paragraph [55].
[28] Report to Parliament, *Telecommunications (Interception and Access) Act 1979 for 2010-2011* (2011) 18.

provisions already result in very considerable incursion into private communications. While the discussed new powers may provide some advantage in terms of consolidating procedural affairs required to obtain access to telecommunications data, our concerns include:

(a) The proposals offer no additional assurances to the public that the data will be deleted when no longer in use,[29]

(b) They provide no further consideration of procedural fairness where that data is forcibly compelled from private companies, and

(c) They offer no insight as to how the government intends to solve not insignificant issues related to encryption, obfuscation and technology that are available to serious criminal enterprises.[30]

31. While the Committee's terms of reference which contain the proposals suggest guidelines on security of stored data, there have been a substantial number of recent breaches of security, resulting in the disclosure of private user data.[31] These disclosures have not been by small businesses or organisations which lack the financial means to employ or train staff who are capable of managing secure environments. The policies that guide access to and use of this data should not be built around the diminishing returns that stem from increasing already substantial powers but from addressing the interests and rights of the majority of the users of any telecommunications services. Focusing on privacy, security standards and providing that the minimum amount of confidential data is retained for the smallest period of time possible would afford legitimate users a greater expectation of privacy, safety and less scope for exploitation of their data by unscrupulous third parties.

Conclusion

32. Australia's counter-terrorism and national security laws can and must exist with a human rights framework. As a State signatory to numerous ratified international human rights instruments, Australia has an obligation to comply with international law. Such compliance gives international law its strength and integrity. ALHR believes that a human rights framework will strengthen counter-terrorism and national security laws in Australia by appropriately balancing the various objectives.

33. ALHR notes that this theme has been at the forefront of international human rights commentary and jurisprudence since 9/11 including in the following statements:

---

[29] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 73.85.

[30] Alana Maurushat "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?" [2011] *University of New South Wales Faculty of Law Research Series* 20.

[31] See Ellen Messmer, *Update: Yahoo's massive data breach includes Gmail, Hotmail, Comcast user names and passwords* (2012) Network World https://www.networkworld.com/news/2012/071212-yahoo-breach-update-260855.html at 19 August 2012; Jim Finkle, *LinkedIn suffers data breach* (2012) Reuters http://www.reuters.com/article/2012/06/06/net-us-linkedin-breach-idUSBRE85511820120606 at 19 August 2012; Hamish Barwick, Anonymous releases some AAPT data (2012) CIO https://www.cio.com.au/article/432044/anonymous_releases_some_aapt_data_/ at 20 August 2012.

(a) On 10 March 2005, the then United Nations Secretary-General Kofi Annan stated in his address to the International Summit on Democracy, Terrorism and Security:

> "Human rights law makes ample provision for strong counter-terrorist action, even in the most exceptional circumstances. But compromising human rights cannot serve the struggle against terrorism. On the contrary, it facilitates achievement of the terrorist's objective — by ceding to him the moral high ground, and provoking tension, hatred and mistrust of government among precisely those parts of the population where he is more likely to find recruits."[32]

(b) Since 9/11 there have been repeated statements by the Security Council, the General Assembly, the Secretary-General and other organs and officers of the United Nations plainly to the effect that counter-terrorism requires observance of international obligations that protect human rights.[33]

(c) Resolution 60/288 adopted by the UN General Assembly in September 2006 stated:

> "The promotion and protection of human rights for all and the rule of law is essential to all components of the [United Nations Global Counter-Terrorism] Strategy, recognizing that effective counter-terrorism measures and the promotion of human rights are not conflicting goals, but complementary and mutually reinforcing."[34]

(d) The Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism (operating under the Human Rights Council) stated:

> **"Together with the responsibility of States to protect those within their jurisdiction from acts of terrorism, States have an obligation to comply with international law, including human rights law, refugee law and humanitarian law**. These legal obligations stem from customary international law, applicable to all States, and international treaties, applicable to States parties. **Compliance with all 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**."[35]

(e) ALHR submits that the Government (and the Committee) must bear this in mind along with Australia's international legal obligations when amending our already voluminous and excessive national security and counter-terrorism laws.

34. Australia has a robust, existing regime of legislation which provides for intelligence services and other government agencies to gain access to communications, to issue

---

[32] K Annan, 'A Global Strategy for Fighting Terrorism' (Speech delivered at the Closing Plenary of the International Summit on Democracy, Terrorism and Security, Madrid, 10 March 2005) http://english.safe-democracy.org/keynotes/a-global-strategy-for-fighting-terrorism.html .

[33] Independent National Security Monitor, *Annual Report 2011,* Commonwealth of Australia, 2012, 16.

[34] General Assembly resolution 60/288, see Appendix 10. Other examples are collected in Appendix 11.

[35] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/16/51), paras 8 and 12.

warrants and to gain operational intelligence from a range of organisations, whether they are foreign intelligence services or private enterprises. There is no clear evidence that the existing frame work has proven insufficient, or even overly inclusive in assisting these agencies to perform the work they currently undertake.

35. Ultimately, ALHR expresses significant concern and maintains a guarded vigilance about the Government's proposal to expand the powers provided to intelligence and law enforcement agencies, especially, in an already excessively policed and heavily legislated environment. This is due to the potential of such powers to prejudice the interests of members of the Australian public beyond those persons directly subject to any investigations. ALHR submits that any proposed increase in powers must be very carefully considered. ALHR further submits that, as the terms of reference for the Committee's inquiry currently stand, there are insufficient safeguards to ensure that both the rights of the public are upheld and the Australian government adheres to its obligations under international law.

36. If you would like to discuss any aspect of this submission, please contact Stephen Keim, President on 0433 846 518 or email:s.keim@higginschambers.com.au

Best regards,

Stephen Keim SC
President, Australian Lawyers for Human Rights
Email: s.keim@higginschambers.com.au
Mobile: 0433 846 518

Contributors: Benedict Coyne, Patrick Gardner