CHAPTER 6

OTHER ISSUES

International, national and state obligations

6.1 The Castan Centre for Human Rights Law (Castan Centre) submitted that 'in the absence of an express right to privacy under Australian Law, legislation such as the TIA Act plays an important role in safeguarding the privacy of individuals'.[1] In particular, their submission stated that Australia should ensure it meets its international obligations under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which states that:

> 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.

6.2 A representative of the NSW Council for Civil Liberties stated that the proposed amendments for device-based warrants constitute 'an arbitrary interference with the right of privacy' in contravention of obligations such as the ICCPR. The representative also considered that the proposed amendments would contravene various state and territory legislation for example, the *Charter of Human Rights and Responsibilities Act 2006* (Vic), and the *Human Rights Act 2004* (ACT)[2]. The representative said that these obligations and legislation enshrine a right to privacy, and that:

> One would (expect to) find that this committee would have before it a statement of compatibility, prepared by the minister introducing this bill, as to the compatibility or non-compatibility of the provisions of the bill with that privacy right.[3]

6.3 The Committee also sought information from representatives of the Attorney-General's Department about interception standards in any United Kingdom legislation comparable to the TIA Act. The Department's response was that the provisions most likely to be related to the addition of devices in a warrant were governed by the *Regulation of Investigatory Powers Act 2000* (RIPA). The Department stated:

> …RIPA makes provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, as well as other investigatory techniques. An important difference between RIPA and the Australian *Telecommunications (Interception and Access) Act 1979* (the TIA Act) is that the UK regime is non-evidentiary based. As the intercepted material is not used in evidence, RIPA has different approaches to the

---

1 *Submission* 1, p. 4.

2 Respectively, this refers to section 13 and 12 of the Acts.

3 *Committee Hansard*, 17 April 2008, p. 7.

> collection of information, use and disclosure, and record keeping requirements.[4]

6.4 The Department further stated that the RIPA equivalent of device-based named person warrants in the TIA Act must describe either.

> (a) one person as the interception subject; or
>
> (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place. [And]
>
> (2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.[5]

6.5 The Department advised that the RIPA allows the addition of devices to an existing warrant, which does not extend the original duration of the warrant. A description of the approval authorities followed:

> Whilst only a Secretary of State is authorised to issue a warrant, scheduled parts of a warrant may be modified by a Secretary of State or by a senior official acting upon their behalf (this, except in urgent cases, does not include the senior official who made the warrant application). A senior official is defined in subsection 81(1) of RIPA as a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service. These designations are equivalent to the Australian Senior Executive Service and represents a similar proportion of the entire Civil Service/Public Service workforce.
>
> … In urgent cases, and where the warrant specifically authorises it, the person who submitted the application (…they are listed in subsection 6(2) and are Heads of Agencies, ie Director-General of the Security Service, the Commissioner of Police of the Metropolis etc) or a subordinate (where identified in the warant) may modify scheduled parts of the warrant. These modifications are valid for five working days only unless endorsed by a senior official acting on behalf of the Secretary of State.[6]

Five year review of the TIA Act

6.6 In its submission to the committee, the Office of the Privacy Commissioner (OPC) reiterated its view that the operation of the TIA Act 'should be subject to overall independent review at least every five years.'[7] The OPC considered this necessary due to the number of amendments to interception legislation in recent years and the resulting incremental expansion in powers.

---

4 Attorney-General's Department: answers to questions on notice, received 24 April 2008

5 Attorney-General's Department: answers to questions on notice, received 24 April 2008

6 Attorney-General's Department: answers to questions on notice, received 24 April 2008.

7 *Submission* 7, p. 9.

6.7 The OPC also submitted a framework against which to assess issues such as privacy and security. The OPC recommended that the committee consider the amendments in the Bill against this framework because of the incremental expansion of powers and suggested that it may also be a useful tool for interception agencies to use.[8]

Committee findings

6.8 In relation to international obligations and state legislation, the committee is unable to make any specific comments in the context of the current inquiry. Nevertheless, in development of amendments to interception legislation and in any review of that legislation, due consideration of the international obligations must be undertaken. A summary statement in the EM of consistency with international obligations (in lieu of an express right to privacy under Australian law) would be a useful guide in consideration of future legislative amendments.

6.9 In relation to the five year review process proposed by the Office of the Privacy Commissioner, the committee draws the attention of the Senate to recommendation 4 of the committee's report on the TIA Amendment Bill 2007, proposing an independent review of the TIA Act within five years.[9] There has been no government response to this recommendation.

6.10 The committee also reminds the Senate of its recommendation in its report in relation to the Provisions of the Telecommunications (Interception) Amendment Bill 2006:

> …the Bill should include a provision for the provisions to expire in five years, with a review at that time or earlier. The Review should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime, together with consideration of ways in which the Act may be amended to take account of emerging technologies such as peer-to-peer technology.

6.11 The Howard Government did not accept this recommendation stating:

> Where it was considered appropriate, sunset provisions have been included for specific provisions in the Bill….
>
> However, the Government does not consider a sunset clause to be appropriate in relation to the wider Bill. The matters proposed in this bill do not reflect a response to a particular short term issue that is likely to dissipate in the longer term. Rather, this legislation reflects a response to permanent changes in the law enforcement and national security environment, caused in large part by changes in technology. As such, it is anticipated that these legislative provisions will assume even greater importance in future.

---

8 *Submission* 7, p. 2.

9 Telecommunications (Interception and Access) Amendment Bill 2007, p. 48.

6.12 In this context, the committee notes that it is currently considering amendments to the device-based warrant regime which was enacted in 2006. It also notes that several of the issues which raised concerns in both the 2006 and 2007 bills have re-emerged in the context of the current inquiry.

Recommendation 6

6.13 **The Committee recommends that the Australian Government commission an independent review of the operation of the *Telecommunications (Interception and Access) Act 1979* within 3 years.**

Recommendation 7

6.14 **The Committee further recommends that the Australian Government introduce amendments to the *Telecommunications (Interception and Access) Act 1979* in subsequent legislation, to provide for a statutory requirement that the TIA Act be independently reviewed every five years.**

Recommendation 8

6.15 **Subject to the preceding recommendations the committee recommends that the Senate pass the Bill.**

Senator Trish Crossin

Chair