Chapter 2

The *Telecommunications (Interception and Access) Act 1979*

2.1 This chapter of the report considers the need for reform of the *Telecommunication (Interception and Access) Act 1979* (TIA Act) and the possible approaches to reform.

Why is reform needed?

2.2 Legislation to protect the privacy of individuals was introduced in 1960 through the *Telephonic Communications (Interception) Act 1960*, which prohibited the interception of telephonic communications except where authorised in the interests of the security of the Commonwealth.[1] That Act was repealed and replaced by the *Telecommunications (Interception) Act 1979* on 1 June 1980.[2] In 2006, the *Telecommunications (Interception) Act 1979* was amended to change the name of the Act (amongst other things) to the current *Telecommunications (Interception and Access) Act 1979* (TIA Act).[3] The Attorney-General's Department (the department) has advised that the objectives of the TIA Act are as follows:

- to protect the privacy of telecommunications by criminalising the interception or accessing of communications; and
- to enable law enforcement, anti-corruption and national security agencies to investigate serious wrongdoing by allowing those agencies to apply for warrants to intercept communications when investigating serious crimes and threats to national security.[4]

2.3 The objectives of the TIA Act remain largely the same as those in the 1960 legislation.[5] Of course, the TIA Act dates well before the age of the internet, and

---

1 http://www.comlaw.gov.au/Details/C1960A00027 (accessed 3 July 2014).

2 http://www.comlaw.gov.au/Details/C1960A00027 (accessed 3 July 2014).

3 At the time that the Act was amended to change its name, it was also amended to implement a number of the recommendations of the Report of the Review of the Regulation of Access to Communications (the Blunn Report) which had concluded: '[T]here was inadequate regulation of access to stored communications, as well as insufficient protection of privacy during the access, storage, and disposal processes of stored communications [and that] the distribution of provisions between the Telecommunications Act and the Telecommunications (Interception) Act (as it was then known) dealing with access to telecommunications data security was complicated, confusing and dysfunctional'. See: ALRC, For Your Information: Australian Privacy Law and Practice, 2008, pp. 2478–2479.

4 Attorney-General's Department, *Submission 26*, pp 3–4.

5 Section 5 of the *Telephonic Communications (Interception) Act 1960* provided that telephone communications were not to be intercepted, the exception being by ASIO where the interception was in connection with the performance by ASIO 'of its functions or otherwise for the security of the Commonwealth'.

although written with the aim of remaining 'technology neutral', evidence taken by the committee indicated that it has failed to keep pace.

Support for reform

2.4 Although those who gave evidence during this inquiry had different views on how reform should progress, there was universal support for urgent reform of the telecommunications legislation.

Law enforcement and national security agencies

2.5 The committee heard that all law enforcement and national security agencies agreed that the current TIA Act was at risk of becoming ineffective without reform. For example, the Australian Crime Commission (ACC) advised the committee that advancements in technology and security had 'diminished the authority initially issued by Parliament in 1979 in relation to interception'. As a result, according to the ACC there is:

> …a compelling need to modernise the TIA Act to ensure provisions keep pace with changes in technology…Because of changes in technology, the ACC is hindered in its investigation of serious and organised crime due to the restrictions on its ability to collect and share material obtained under the TIA Act.[6]

2.6 The ACC explained that, in its view, the TIA Act 'must be capable of overcoming technological advances which are deliberately used to prevent law enforcement from lawfully intercepting and accessing communications'.[7]

2.7 Similarly, the Australian Security Intelligence Organisation (ASIO) advised the committee that without modernisation not only will there be 'detrimental consequences' for Australia's national security and law enforcement capacities, but also for individual privacy.[8]

2.8 The Australian Federal Police (AFP) emphasised to the committee that the need for comprehensive reform to 'avoid further degradation of existing capability whilst ensuring transparency' was 'becoming increasingly pressing'.[9]

2.9 In addition to these Commonwealth agencies, state and territory law enforcement agencies also supported reform. For example, Victoria Police expressed the view that 'holistic reform of the TIA Act' was urgently needed 'if law enforcement agencies [were] to maintain an adequate investigative capability'.[10] The Western Australian Police argued that the current legislative framework was 'not sufficient to adequately deal with technological change, and the attempt to address such

---

6 Australian Crime Commission, *Submission 23*, pp 3–6.

7 Australian Crime Commission, *Submission 23*, pp 3–6.

8 Australian Security Intelligence Organisation, *Submission 27*, p. 4.

9 Australian Federal Police, *Submission 25*, p. 3.

10 Victoria Police, *Submission 6*, p. 1.

advancements [through constant legislative amendments had] resulted in a complicated regime'.[11]

Civil liberty and rule of law stakeholders

2.10 Support for reform was also expressed by stakeholder organisations that seek to promote and protect the right to privacy and the rule of law. For example, the Law Council of Australia (Law Council) gave its 'general support' for a comprehensive review that considered:

> …how this legislation fits within the broader surveillance and interception legislative regime; whether the TIA Act can and should respond to emerging technological developments; and what safeguards and other provisions should be included in the TIA Act to ensure that it does not unduly burden individual rights, including the right to privacy.[12]

2.11 ThoughtWorks Australia also supported review. It observed that, as the TIA Act had 'been amended more than 45 times since September 2001, [it] requires an overhaul to bring it into the digital age, to properly integrate Australia's National Privacy Principles, and to uphold…[Australia's] obligations under international human rights law.'[13]

2.12 Blueprint for Free Speech similarly noted that it would be 'prudent to modernise the legislation to account for new technology and new challenges faced in gathering evidence for criminal investigations'.[14]

Approach to reform

2.13 The findings of the ALRC and PJCIS reports and evidence received throughout the inquiry indicate that legislative reform must seek to achieve administrative efficiencies, remain technology neutral and maintain adequate oversight and privacy protections. The then Secretary of the Attorney-General's department expressed this approach to reform succinctly:

> The key driver for reform is the need to create a privacy and access regime that is fit for the modern telecommunications environment and that can withstand rapid technological change into the future…[R]eform of the TIA Act…also represent[s] an opportunity to modernise and strengthen protections afforded to Australian telecommunications, limit the range of agencies in accessing telecommunications data while also introducing

---

11 Western Australian Police, *Submission 20*, p. 4. Northern Territory (NT) Police also expressed support for reform of the TIA to 'provide greater simplicity, clarity and efficiency of operations under those acts'. See: NT Police, *Submission 21*, p. 10.

12 Law Council of Australia, *Submission 34*, p. 4.

13 ThoughtWorks Australia, *Submission 5*, p. [2]. The Australian Privacy Foundation (APF), made similar comments, stating its support for a holistic review to consider the cumulative effect of the many marginal changes over time. See: Mr Nigel Waters, Australian Privacy Foundation, Committee Hansard, 29 July 2014, p. 30.

14 Blueprint for Free Speech, *Submission 4*, p. 15.

> stronger oversight mechanisms and improv[ing] the effectiveness and efficiency of the current accountability and reporting regimes.[15]

2.14 The department suggested that although the 'basic values underpinning the Act are probably sound and do not require revision or amendment':

> [T]he law requires agencies and other users to navigate an incredibly complex modern communications environment using powers and procedures designed in the 1970s…The antiquated nature of the Act presents real and very pressing challenges for these agencies…The privacy protections and the oversight regimes established by the Act are in better shape, but even these protections are fragmented and, in places, internally inconsistent after 35 years of ad hoc amendment.[16]

2.15 This approach to reform was consistent with views expressed by the technology industry—the Internet Society of Australia (ISOC-AU) submitted that:

> [A]ny legislative changes should adopt a technology neutral, principles based approach that would better withstand technological change and couple that with preservation of fundamental citizen rights. At least, any changes to the legislation should avoid wherever possible being unduly technology specific, as that obviously leads to endless amounts of specification that would need to be adjusted on a continuing basis.[17]

Balancing the right to privacy and national interests

2.16 Any programme of reform must balance individual and national interests with sensitivity and maturity. The need for balance was clearly expressed by the Australian Law Reform Commission (ALRC) following its 2006-8 review of the *Privacy Act 1988* (Cth):

> As a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience. It is often the case, however, that privacy rights will clash with a range of other individual rights and collective interests, such as freedom of expression and national security. International instruments on human rights and growing international and domestic jurisprudence in this field all recognise that privacy protection is not an absolute. Where circumstances require, the vindication of individual rights must be balanced carefully against other competing rights.[18]

2.17 Although the view that the need for urgent reform of the telecommunications legislation was universal, the objective of protecting privacy was not diminished. The

---

15 Mr Roger Wilkins AO, Secretary, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 2.

16 Mr Roger Wilkins AO, Secretary, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 2.

17 Ms Narelle Clark, President, Internet Society of Australia (ISOC-AU), *Committee Hansard*, 23 April 2014, p. 32.

18 *For Your Information – Australian Privacy Law and Practice*, Australian Law Reform Commission (ALRC) Report #108, p. 104.

evidence received by the committee emphasised that the right to access telecommunications information should only be exercised when both proportionate and appropriate. For example, the Law Council explained:

> …where a State seeks to restrict human rights, such as the right to privacy, for legitimate and defined purposes, for example in the context of telecommunications access and interception, the principles of necessity and proportionality must be applied. The measures taken must be appropriate and the least intrusive to achieve the objective.
>
> In the context of telecommunications access and interception, this involves balancing the intrusiveness of the interference, against operational needs. Interception of, or access to communications, will not be proportionate if it is excessive in the circumstances or if the information sought could reasonably be obtained by other means.[19]

19 Law Council of Australia, *Submission 34*, p. 5.