The expanding ambit of telecommunications interception and access laws: The need to safeguard privacy interests

Niloufer Selvadurai and Rizwanul Islam†*

The Telecommunications (Interception and Access) Act 1979 (Cth) allows law enforcement agencies to obtain a warrant to intercept or access telecommunications where there are reasonable grounds for suspecting activities or purposes that are prejudicial to security, or otherwise pose a threat serious enough to warrant investigation. Since its enactment in 1979, there have been a variety of amendments that have significantly extended the ambit of the operation of the TIA Act. As the Act is now over 30 years old, it is useful to consider the extent to which the legislation is achieving a proper balance between protecting national security interests or the prevention of specified types of serious offences, and the protection of privacy. Issues of interest include the 2007 amendments in relation to stored communications, the 2008 amendments in relation to access to 'telecommunications data', and the proposed 2009 amendments directed at improving the capacity of owners and operators of computer networks to undertake activities to protect their networks.

In recent years, the interception of telecommunications for the purpose of garnering intelligence to prevent or investigate crimes has become an increasingly significant tool of law enforcing agencies (LEAs). The Telecommunications (Interception and Access) Act 1979 (Cth) (the TIA Act) enables law enforcement agencies to obtain a warrant to intercept or access telecommunications where there are reasonable grounds for suspecting engagement in activities or purposes that are prejudicial to security or the commission of certain types of serious offences. As such activities necessarily involve an encroachment on civil liberties, it is imperative to achieve a proper balance between the interests of national security or prevention of other serious offences, and the need to not unduly compromise the privacy of individuals.

Since its enactment in 1979,[1] there have been a variety of amendments that have significantly extended the ambit of the operation of the TIA Act. This is consistent with many other western liberal democracies where public concern about terrorism and the increasing sophistication and use of telecommunication technologies have given rise to a consistent expansion of the ambit of investigative powers of LEAs.[2] This incremental increase to the

* Senior Lecturer, Department of Business Law, Macquarie University; BA LLB (Hons I) (University of Sydney); PhD (Macquarie University).

† PhD Candidate, Macquarie Law School; Casual Lecturer, Department of Business Law, Macquarie University.

1 Initially, the Act was titled the Telecommunications (Interception) Act 1979 (Cth).

2 For discussions of the trend of expansion of investigative powers of LEAs and concerns over

ambit of the Act has, however, aroused grave concerns among advocates of civil liberty, both in Australia and around the world. In this context, it is useful to consider the extent to which the legislation is achieving a proper balance between protecting national security interests or prevention of serious offences, and the protection of privacy.

This article begins by briefly exploring the application of the concept of privacy to the telecommunications sector. It then examines the present laws and identifies a number of areas of concern. The areas of change include the 2007 amendments in relation to stored communications,[3] the 2008 amendments in relation to access to 'telecommunications data', and the proposed 2009 amendments directed at improving the capacity of owners and operators of computer networks to undertake activities to protect their networks. This is followed by a consideration of some continuing issues in relation to the proper overseeing of the legislation and notification of innocent individuals.

Privacy in the telecommunications context

It is useful to begin by briefly considering the ambit of the concept of privacy in the context of telecommunications.[4] Privacy is an extremely intricate and multi-layered concept, and while the use of the term privacy and the importance of the principle are commonplace, a widely agreed upon definition has remained elusive.[5] A useful discussion is found in Lord Mustill's judgment in *R v Broadcasting Standards Commission; Ex parte:*

> To my mind the privacy of a human being denotes at the same time the personal 'space' in which the individual is free to be itself, and also the carapace, or shell, or umbrella, or whatever other metaphor is preferred, which protects that space from intrusion. An infringement of privacy is an affront to the personality, which is damaged both by the violation and by the demonstration that the personal space is not inviolate.[6]

In the telecommunications milieu, the main areas of concern in relation to privacy are:

---

civil liberty in western liberal democracies, see A Lynch, E MacDonald and G Williams, *Law and Liberty in the War on Terror*, Federation Press, Sydney, 2007; P Rosenzweig, 'Civil Liberty and Response to Terrorism' (2004) 42 *Duquesne L Rev* 663. For a discussion of the costs of interception, see P Barrett, *A Review of the Long-Term Cost Effectiveness of Telecommunications Interception*, 1994 (the Barrett Review) p 91. Interception of telecommunication is generally less expensive in comparison with other means of surveillance that may be adopted by LEAs.

3 The TIA (or TI Act as it was initially titled) was also amended in the past to extend the ambit of interception; see S Bronitt and J Stallios, 'Regulating Telecommunications Interception and Access in the Twenty-first Century' (2006) 24 *Prometheus* 413.

4 For an example of the differing views on the expectation of privacy, see Australian Telecommunications Authority, *Telecommunications Privacy: Final Report of AUSTEL's Inquiry into the Privacy Implications of Telecommunications Services*, Melbourne, 1992, pp 17–18.

5 For useful general discussions of privacy law, see D Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *MULR* 131; D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *MULR* 339; ALRC, *Review of Australian Privacy Law*, Discussion Paper No 72, September 2007, p 116.

6 [2001] QB 885; [2000] 3 All ER 989; [2000] 3 WLR 1327; [2000] EWCA 59 at [48].

(a) interception of telecommunications;
(b) the misuse of personal information acquired by the telecommunication carriers or service providers or other commercial enterprises;[7] and
(c) unsolicited telecommunications made to individuals advertising goods or services.[8]

Interception of telecommunications is distinct from the other two types of issues relating to privacy because in this case it is the actions of government LEAs which may potentially jeopardise the privacy of individuals. Categories (b) and (c) largely relate to the actions of corporate entities and are outside the scope of the present discussion.

Strong support for the importance of protecting privacy in the context of telecommunications interception is found in the April 2002 submission of the Office of the Federal Privacy Commissioner to the Senate Legal and Constitutional Legislation Committee Inquiry into a number of anti-terrorism bills. In the submission, the office considered proposed amendments to the TI Act (as it then was) in relation to the regulation of stored communications such as emails, voicemails, SMS and MMS messages. With regard to privacy, it is noted:

> In general, people expect their private conversations, including those via telecommunications systems, to be free from intrusion by state and commercial interests. This expectation is limited where there are prevailing interests of national security and law enforcement relating to serious criminal offences. Strong justification is needed for the interception of private conversations.[9]

The 2005 Report of the Review of the Regulation of Access to Communications[10] by Anthony Blunn (the Blunn Report) affirms the overarching importance of protection of privacy and stresses that any legislation allowing interception power should lend fundamental consideration to the protection of privacy of individuals.[11] The findings seek to balance privacy with security and law enforcement. It is initially noted that '[t]he protection of privacy should continue to be a fundamental consideration

7 For discussions of the issues relating to the misuse of personal information in the telecommunications context, see, eg, A W Haynes, 'Online Privacy Policies: Contracting Away Control over Personal Information?' (2007) 111 *Pennsylvania State L Rev* 587; C A Ciocchetti, 'E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors' (2007) 44 *American Business LJ* 55; S Ludington, 'Reining in the Data Traders: A Tort for the Misuse of Personal Information' (2006) 66 *Maryland L Rev* 140.

8 For studies on the issue of unsolicited telecommunications see, for instance, N J King, 'Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices' (2008) 60 *Federal Communications LJ* 229; E B Cleff, 'Privacy Issues in Mobile Advertising' (2007) 21 *International Review of Law, Computers & Technology* 225; K M Rogers, 'Viagra, Viruses and Virgins: A Pan-Atlantic Comparative Analysis on the Vanquishing of Spam' (2006) 22 *Computer Law and Security Report* 228; D Zwick and N Dholakia, 'Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing' (2004) 24 *Jnl of Macromarketing* 31.

9 Office of the Federal Privacy Commissioner, *Submission to the Senate Legal and Constitutional Legislation Committee Inquiry*, April 2002.

10 A S Blunn, *Report of the Review of the Regulation of Access to Communications*, Attorney-General's Department, 2005, p 5.

11 Ibid.

in, and the starting point for, any legislation providing access to telecommunications for security and law enforcement purposes'.[12]

However, it is subsequently noted that interception of communications and access to telecommunications data is, and for the foreseeable future will remain, 'fundamental' to effective security and law enforcement. Legislation has since been enacted which adopts many of the key recommendations of the Blunn Report. It is useful to consider the present operation of the TIA Act, including the substantive amendments made to the original Act, to more fully assess the extent to which the law is balancing the 'protection of privacy' and the interception and access of information for effective 'security and law enforcement'.

The telecommuncations interception and access framework

The primary objective of the Telecommunications (Interception and Access) Act 1979 (Cth) is to protect the privacy of individuals who use the Australian telecommunications system by making it an offence to intercept communications passing over that system, except in accordance with the provisions of the Act.[13] The TIA Act hence serves the *dual objective* of protecting the privacy of individuals who use the Australian telecommunications system as well as controlling the circumstances in which communications may be lawfully intercepted and accessed.

The general prohibition

The TIA expressly limits the circumstances in which interception of telecommunications may be permitted. It limits these circumstances to investigation of relatively serious crimes (eg, class 1 or class 2 offences).[14] The TIA Act contains a general prohibition on the interception of communications passing over a telecommunications system and access to stored communications (ie, email, SMS and voice mail messages stored on a carrier's equipment).[15]

Section 7(1) proscribes any person from intercepting; authorising, suffering or letting another person intercept; or doing any act or thing that will enable him or her or another person to intercept a communication passing over a telecommunications system. Under s 5 of the Act, 'communication' includes conversation and a message, and any part of a conversation or message, whether: (a) in the form of: (i) speech, music or other sounds; (ii) data; (iii) text; (iv) visual images, whether or not animated; or (v) signals; or (b) in any other form or in any combination of forms.

A telecommunications system is defined to mean:

> (a) a telecommunications network that is within Australia; or

12 Ibid.

13 Commonwealth Government, *Report of the Security Legislation Review Committee*, 2006, p 182. See Pt 13 of the Telecommunications Act 1997 (Cth).

14 Ibid.

15 TIA Act ss 7(1) and 108(1).

(b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia; and includes equipment, a line or other facility that is connected to such a network and is within Australia.[16]

The term 'interception' is defined as 'listening to or recording, by any means, a communication in its passage over the telecommunications system without the knowledge of the person making the communication'.[17] Accessing a stored communication is defined as 'listening to, reading or recording such a communication by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication'.[18]

Exception for the general prohibition

The central exception to this general prohibition of interception is to permit LEAs to lawfully intercept or access telecommunications in certain circumstances pursuant to an interception warrant or a stored communications warrant issued under the TIA Act.

Although a warrant remains the primary means of access and interception, the Australian Federal Police or the police force of a state, is allowed to intercept a communication without a warrant under the following specified circumstance:

(a) where the officer or another officer of the police force is a party to the communication under interception, or the person to whom the communication is directed has consented to be intercepted; and
(b) there are reasonable grounds for suspecting that another party to the communication has done an act that has resulted or may result in loss of life, serious injury or serious damage to properties; or that the person consented to be intercepted is likely to receive a communication from a person whose act has resulted or may result in loss of life, serious injury or serious damage to properties; and
(c) the need for interception is so urgent that it is not reasonably practicable to make a warrant application.[19]

Therefore, the regulatory scheme provided in the TIA Act ostensibly seeks to ensure that any interception of private telecommunications is proportional to the seriousness of the law enforcement or security issues involved, limited to only that degree of privacy invasion which is required, and subject to specific accountability and oversight mechanisms, including a reporting scheme.[20] In other words, by imposing a general ban, the Act purports to create exceptions for specific cases where interception is lawful for achieving the stated objectives. However, despite this general mechanism to ensure compliance, a number of serious concerns remain as to the adequacy of the privacy protection afforded by the legislation. It is useful to consider each of these issues in turn.

16 Ibid, s 5.
17 Ibid, s 6(1).
18 Ibid, s 6AA.
19 Ibid, ss 7(4) and (5).
20 See Pt VI for further on the oversight mechanism.

The 2006 amendments: Does the B-party warrant cast the net too wide?

The first significant extension to the ambit of the TIA Act relates to stored communications. The TIA was originally limited to communications 'passing over' a telecommunications system. In 2006, the Telecommunications (Interception) Amendment Act (Cth) was enacted and established a warrant framework relating to 'stored communications'. The Act adopted certain recommendations made by Anthony Blunn in his report, mentioned above .

Schedule 2 of the Telecommunications (Interception) Amendment Act 2006 (Cth) introduced into the TIA Act a new form of warrant called the B-party warrant. This type of warrant is issued against a so-called 'B-party', that is, an individual who is *not suspected* for any wrongdoing but someone *who may simply use a telecommunication service* for communicating with a suspected individual. The B-party may be a totally innocent person, no more than a conduit for a relevant communication, and may not have any connivance or knowledge of the use being made of them.[21]

LEAs can be granted a B-party warrant by establishing that the surveillance of the communication of a B-party or services used by that person would be intercepting communication by a person of interest and this latter person is engaged in, or is reasonably suspected of being engaged in, activities prejudicial to the national security or involved in the commission of a serious criminal offence.[22]

There is a considerable probability that many of the communications intercepted through this type of warrant would garner personal information that does not have any bearing on the specific investigation for which the warrant has been issued. For example, once a person of interest communicates with legal counsel, the latter can be a B-party and her or his communication with other clients, as well as any intimate communication with their spouse, could be intercepted.[23] These types of communications are at common law treated as privileged communications and should not be allowed to be intercepted so easily.

It is also problematic that the Australian Security Intelligence Organisation (ASIO) can obtain a warrant against a B-party by simply making a request for interception to the Attorney-General, alleging that the person is using or likely to be using the telecommunications service for acts threatening national security.[24] This process does not involve any scrutiny or authorisation by the judiciary. It is acknowledged that the ASIO regime is different from the interception regime applicable to LEAs; nonetheless, from a privacy standpoint this seems to be an odd provision.

Australia is a signatory to the International Covenant on Civil and Political

21 Blunn Report, above n 10, p 75.
22 TIA Act ss 9(1) (a) (ia) and (b), 46(1)(d)(ii).
23 Bronitt and Stallios, above n 3, at 417.
24 TIA Act s 9(1).

Rights (ICCPR),[25] which it ratified on 13 August 1980.[26] Article 17 of the ICCPR provides that:

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.

With regard to the adoption of treaty obligations in the domestic legal sphere, Australia follows the doctrine of incorporation: that is, any principle of international treaty is not part of the Australian legal corpus unless and until that international treaty is given effect by legislation of the parliament.[27]

Federal parliament has enacted the Privacy Act 1988 (Cth), which protects privacy of personal information of individuals retained by government agencies and some large private sector organisations. Significantly, the Privacy Act does not contain any provision that expressly deals with interception and access of telecommunications, although some information privacy principles have relevance for interception.[28]

The High Court ruled in *Lim v Minister for Immigration Local Government & Ethnic Affairs*[29] that principles of international law can be applied as an aid to the interpretation of any Commonwealth statute. The court stated: 'We accept the proposition that the courts should, in a case of ambiguity, favour a construction of a Commonwealth statute which accords with the obligations of Australia under an international treaty'.[30] Subsequently, in *Minister of State for Immigration & Ethnic Affairs v Teoh*,[31] the High Court has followed the same principle and noted that the fact that an international treaty has been ratified but not incorporated into domestic legislation is not without substance.[32] This is because, in view of the High Court, the Commonwealth Parliament would prima facie attempt to honour any legal obligations that it has under international law.[33]

However, even though citizens of Australia may not have a cause of action under Art 17 of the ICCPR before any court of law, that lack of remedy does

25 International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) (ICCCPR).

26 Australian Law Reform Commission, above n 5, p 118.

27 This position is explained by Mason J in *Koowarta v Bjelke-Petersen* (1982) 153 CLR 168 at 225; 39 ALR 417; [1982] HCA 27; BC8200052:

> It is a well settled principle of the common law that a treaty not terminating a state of war has no legal effect upon the rights and duties of Australian citizens and is not incorporated into Australian law on its ratification by Australia . . . [T]he approval by the Commonwealth Parliament of the Charter of the United Nations in the Charter of the United Nations Act 1945 (Cth) did not incorporate the provisions of the Charter into Australian law. To achieve this result the provisions have to be enacted as part of our domestic law, whether by Commonwealth or State statute. Section 51(xxix) arms the Commonwealth Parliament with a necessary power . . . to legislate so as to incorporate into our law the provisions of [any international treaty].

28 Privacy Act 1988 (Cth) s 14.

29 (1992) 176 CLR 1; 110 ALR 97; 67 ALJR 125; BC9202669.

30 Ibid, at CLR 38.

31 (1995) 183 CLR 273; 128 ALR 353; [1995] HCA 20; BC9506417.

32 Ibid, at CLR 287.

33 Ibid.

not exonerate Australia's obligation under international law. In the absence of any authoritative judicial determination, it is difficult to determine whether or not the introduction of the B-party warrant is consonant with Art 17 of the ICCPR. For an action which invades privacy to be considered permissible under Art 17, the minimum threshold is that it must not be arbitrary or unlawful. Arguably, however, it is also implicit that intrusive actions would be very sparingly used. Hence, it does not seem plausible to argue that the B-party warrant system complies with the spirit of the Article. In the case of a B-party warrant issued by the Attorney-General, there is complete absence of judicial oversight and in all cases of B-party warrants, the privacy of innocent individuals appears to be unduly compromised.

The introduction of the B-party warrant into the TIA Act appears to be a response to increasing concern over potential acts of terrorism.[34] However, the desirability and wisdom of disproportionate measures to counter terrorism can severely erode civil liberties. In this regard, the UN High Commissioner for Human Rights very fittingly noted that:

> Human rights law wisely strikes a balance between the enjoyment of freedoms and the legitimate concerns for national security. It requires that, in the exceptional circumstances where it is permitted to limit some rights for legitimate and defined circumstances, the principles of necessity and proportionality must be applied. The measures taken must be appropriate and the least intrusive to achieve the objective. The discretion granted to certain authorities to act must not be unfettered.[35]

The 2007 amendments: Should there be a definition of 'telecommunications data'?

In 2007, a further extension was made to the ambit of the TIA Act. The Telecommunications (Interception and Access) Amendment Act 2007 transferred the provisions in the Telecommunications Act 1997 (Cth) which regulated access to 'telecommunications data' for national security and law enforcement purposes to the TIA Act.[36]

The new access provisions in the TIA Act are wider than those under the Telecommunications Act. This is because the TIA Act adopts a new two-tier regime for access that encompasses both historic and 'prospective' telecommunications data.

A subject of concern with the 2007 amendments is the absence of a definition of 'telecommunications data'. Neither the TIA Act nor the Telecommunications Act contains such a definition. As the access provisions turn on the threshold issue of 'telecommunications data', the absence of a

---

34 Indeed, expansion of invasive investigation powers of telecommunications by LEAs is part of a wider trend. For a critique of Australia's anti-terror laws in the aftermath of the September 11 terrorist attack on the United States see, for instance, J Tham, 'Casualties of the Domestic "War on Terror": A Review of Recent Counter-Terrorism Laws' (2004) 28 *MULR* 512; M Head, '"Counter-Terrorism" Laws: A Threat to Political Freedom, Civil Liberties and Constitutional Rights' (2002) 26 *MULR* 666.

35 United Nations High Commissioner for Human Rights, *Statement by Mary Robinson UN High Commissioner for Human Rights to the Third Committee: Report of the High Commissioner for Human Rights to the General Assembly*, UN General Assembly 56th session, 6 November 2001.

36 Telecommunications Act (Cth) ss 282 and 283 (repealed).

definition serves to make the ambit of the Act imprecise. The Act does not state whether 'telecommunications data' includes data generated by both landline and mobile communications and other applications such as internet browsing and voice-over-internet protocol telephone services.

Further, for purposes of telephone communications, the Act does not expressly state whether 'telecommunications data' includes subscriber details held on telecommunications networks, including telephone numbers of the parties involved. For the purposes of internet-based operations, the Act does not specify whether 'telecommunications data' encompasses Internet Protocol (IP) addresses and websites visited. While the Explanatory Memorandum does provide useful guidance in this regard and suggests that all of the above are encompassed in the term, it would be preferable to have the certainty of a legislative definition.

The Law Council of Australia voiced its protest over the absence of a definition in the following terms:

> The purpose of the Bill is to consolidate and refine the legislative provisions which set out the circumstances in which different types of telecommunication information can be disclosed for law enforcement purposes . . . It is assumed that one of the key aims of the exercise is to ensure that both the privacy rights of individuals and the powers of enforcement agencies are clearly understood. It seems unfortunate, and possibly counterproductive, in those circumstances not to properly define 'telecommunications data'.[37]

The proposed 2009 amendments: Networks

The most recent proposal for amendment to the TIA Act relates to the capacity of owners and operators of computer networks to undertake activities to protect their networks. At present, certain routine network protection activities designed to ensure that computer networks are not vulnerable to known or predicted security risks and are able to repel or survive an attack may inadvertently contravene the prohibitions in the TIA Act.

In its submission on the Telecommunications (Interception and Access) Amendment Bill 2009, the Privacy Commissioner begins by affirming:

> The need for an appropriate balance between the public interest in computer network owners and operators being able to undertake legitimate activities aimed at detecting and responding to security risks and maintaining privacy.[38]

While this is appropriate, it is concerning that the exposure draft of the bill sets out a regime for enabling agencies to undertake such network protection activities without obtaining a warrant or any form of authorisation. It is important to note, however, that the provision would only allow an LEA to undertake these activities in relation to its own communications and hence would not provide a backdoor to access third party communications. A possible issue is whether this could be achieved in two stages; whether an

37 Law Council of Australia, *Submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Bill 2007*, July 2007.

38 Office of the Privacy Commissioner, Government of Australia, *Exposure Draft of the Telecommunications (Interception and Access) Amendment Bill 2009: Network Protection Submission to the Attorney-General's Department*, August 2009, p 2.

LEA could induce an operator of a computer network to undertake such an activity and then disclose it under Pt 4.

Is there adequate overseeing of the Act?

As well as the concerns generated by extensions to the ambit of the TIA Act, certain other concerns have remained since the enactment of the original TI Act. One of these relates to determining the proper independent and impartial watchdog to oversee the operation of the TIA Act. Under the TIA Act, the Commonwealth Ombudsman acts as the independent watchdog to oversee that interception power is properly exercised by different Commonwealth agencies (but not of interceptions by ASIO). It is the Ombudsman who periodically scrutinises the records kept by Commonwealth agencies in order to find out the extent to which their officials have complied with ss 79, 80 and 81, which deal with various record-keeping and destruction of certain restricted records.[39] The Ombudsman reports on the exercise of these powers to the Attorney-General.[40]

The reporting power of the Ombudsman is quite far-reaching as she or he can report on any breaches of the TIA Act committed by LEAs (but not by ASIO), not merely those relating to record-keeping and destruction of restricted records.[41] The Ombudsman's power to extract information would prevail over any other provision to the contrary in any other law, and a person is not excused from furnishing information, answering a question, or delivering a document on the ground that such information, answer or delivery of documents would contravene a law, would be contrary to the public interest or might tend to incriminate the person or may expose the person to be liable to a penalty.[42]

Despite the extensive power of the Ombudsman, a question arises as to the fittingness of vesting such a function in this office. This issue has been addressed several times in official reviews of the TIA Act. A review commissioned by the Federal Attorney-General's Department in 1991 opined that the oversight function would be more appropriately vested in the office of the Privacy Commissioner. Nonetheless, the review suggested that the function is essentially of an auditing nature and should therefore continue to be performed by the Ombudsman.[43]

The same issue was addressed by the Barrett Review in 1994, which stressed that the TI Act (as it then was) inspection and reporting functions exercised by the Ombudsman were not appropriate as the spotlight should be on privacy protection, not merely the audit or oversight of administrative processes, and unequivocally recommended that the function be shifted to the Privacy Commissioner.[44] This recommendation was again rejected by the Federal Government on the ground that the function was performed properly

39 TIA Act, s 83.
40 Ibid, s 84.
41 Ibid, s 85.
42 Ibid, s 88.
43 Commonwealth of Australia Attorney-General's Department, *Review of Telecommunications (Interception) Act 1979*, Canberra, 1991, p 61.
44 Barrett Review, above n 2, Recommendation 6.

by the Ombudsman and because it viewed the function to be a check of compliance with TIA Act, rather than an oversight of privacy issues.[45]

In 1999, the Ford Review of the TIA Act[46] also took this issue up. It concurred with the 1991 review and recommended that the function was suitably vested with the office of the Ombudsman. The raison d'être of the Ford Review was once again that the tasks performed by the Ombudsman basically involved reviewing the actions of different agencies and verifying to what extent they had complied with the requirements of the Act.[47] The review claimed that the privacy issue is sufficiently attended to during the grant of a warrant, and expressed concern that vesting the oversight in the Privacy Commissioner, whose basic function is to defend the notion of privacy, may tilt the balance unduly in favour of privacy concerns and disregard national safety.[48] It contended that the Privacy Commissioner was not necessarily neutral, and that shifting the power to this office may create uncalled for constraints on the action of government agencies.[49] It is interesting to note that the Ford Review found that all government agencies 'loathe' the idea of shifting inspection responsibilities from the Ombudsman to the Privacy Commissioner.[50]

The Ford Review's treatment of the issue seems to be flawed on several counts. Branding the Privacy Commissioner's office as partisan solely because of its function of protecting privacy seems to be too simplistic and untenable. The fact that privacy issues are a matter for consideration by the granting authority at the time of deciding on the application does not mean that once the warrant is granted the issue of privacy ceases to be relevant, nor can it be assumed that the acts that follow in execution of the warrant will be in total compliance with legal requirements.

The Australian Privacy Charter Council has rightly argued that the role of the Privacy Commissioner's Office as one of active investigator and educator is indeed a comparative strength of the Commissioner's Office over that of the Ombudsman's narrower focus on auditing.[51] The frosty response of government agencies to the idea of the potential involvement of the Privacy Commissioner in a watchdog role is curious and may trigger alarm bells among privacy advocates.

Are the provisions for the notification of innocent individuals adequate?

Finally, another continuing area of concern is the provision for the notification of innocent individuals. A key recommendation of the Barrett Review was that

45 Australian Senate, *Second Reading Speech, Telecommunications (Interception) Amendment Bill 1994*, 7 December 1994, referred to in Queensland Criminal Justice Commission, *Telecommunications Interception and Criminal Investigation in Queensland: A Report*, 1995, p 26.

46 P Ford, *Review of the Regulation of Access to Communications*, Attorney-General's Department, 1999 (the Ford Review).

47 Ibid, p 7.

48 Ibid, p 42.

49 Ibid.

50 Ibid, p 43.

51 Ibid, p 43.

a government agency invoking the power of interception of telecommunications be required to notify innocent individuals whose telecommunications have been intercepted by any agency of the fact of such interception within 90 days of the termination of the interception.[52] As an alternative to the compulsory notification requirement, the Barrett Review suggested that the agencies be obliged to maintain a register of those e-incidents where telecommunications of any innocent person has been intercepted by them. Parliament has adopted this alternative suggestion. It has inserted a new section into the TIA Act in the form of s 81C, which provides for inter alia a special register containing details of warrants that have not led to a charge being laid within 3 months of the expiry of the warrant.[53]

The issue of notification of individuals was once more evaluated by the Ford Review. The review found that a kind of notification system had functioned well in the United States but it also noted that the requirement of notification would add little to privacy protection and may create unnecessary red tape.[54] It was also concerned that the requirement of detailed notification may compromise prosecution.[55] The basis of this recommendation seems to be rather simplistic as there is insufficient analysis provided as to how the review came to the conclusion that a notification would have no implication for the protection of privacy. If a notification system is in place, it is always likely to be in the back of the mind of LEAs that any patently erroneous action might expose them to public criticism.

In contrast, the Charter Council has endorsed the idea of a notification requirement and argued that if agencies were required to publicly justify intrusions to privacy which have yielded no results, this would be a potent restraint against the abuse of the powers.[56] Interception of telecommunications is by no means an ordinary power and a mandatory requirement to notify innocent individuals is desirable as a counterbalance to any potential abuse or use of the power on mere frivolous suspicions.

Conclusion

Telecommunications occupies an increasingly significant part of communications between individuals. It is generally accepted that any set of legal rules giving rights of interception of telecommunications would involve some degree of encroachment on the right of privacy of citizens. This compromise of a degree of privacy is the price to be paid for increased security. However, it is important to achieve an effective and equitable balance between the powers of intrusive interception and the legitimate expectation of privacy. With each wave of amendments and expansions, it is imperative to ensure that the fight against the threats to national security and the keen interest in prevention of serious offences do not blur the vision for the protection of the inalienable rights of citizens. The concern in relation to Australia's present interception and access laws is that incremental increases

52 Barrett Review, above n 2, Recommendation 7.
53 Ad No 141, 1995.
54 Ford Review, above n 46, p 49.
55 Ibid.
56 Ibid, p 50.

to the ambit of the operation of the TIA Act have served to erode individual rights and threaten fundamental privacy interests.