

+61 2 61253971



Canberra ACT 0200 Australia
Telephone: +61 2 6125 8140
Facsimile: +61 2 6125 0103
Email: james.stellios@anu.edu.au

10 July 2007

Sue Harris Rimmer
Senior Researcher Law & Bills Digest Group
Department of Parliamentary Services
Parliament House, Canberra ACT 2600

Fax: (02) 6277 5286

Dear Sue

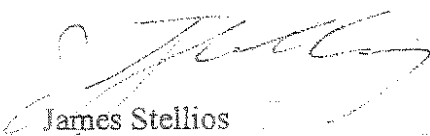
As indicated yesterday, unfortunately, neither Simon Bronitt or I are in a position to make a formal submission to the Senate Legal and Constitutional Affairs Committee on the Telecommunications (Interception and Access) Amendment Bill 2007 by 11 July.

However, in 2006, we published the following two papers on the 2006 amendments to the *Telecommunications (Interception and Access) Act 1979* (Cth):

- 'Regulating Telecommunications Interception and Access: A Sea-Change in Surveillance Laws', in Michael and Michael (eds), *Social Implications of Information Security Measures on Citizens and Business* (2006);
- 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?' (2006) *Prometheus* 413.

On behalf of Professor Bronitt and myself, I have forwarded the second of these papers by email, and now send through the first paper to you. We hope that they might be of some assistance to the Committee.

Yours sincerely



James Stellios
Senior Lecturer
ANU College of Law

+61 2 61253971

8

Regulating telecommunications interception & access: a seachange in surveillance laws

Simon Bronitt and James Stellios
ANU College of Law, The Australian National University

Abstract

The federal Parliament's recent amendments to the telecommunications interception legislation have significantly overhauled the regulatory scheme for the protection of communications passing over the telecommunications system. The amendments have introduced new provisions for accessing stored communications, and have provided government agencies with further tools for security and law enforcement purposes. This paper considers the changes to the legislative scheme, and how privacy interests have been 'balanced' away in favour of providing government agencies with enhanced surveillance tools.

Keywords: privacy, telecommunications interception, surveillance, data access, wire tap, warrants, security, law enforcement

+61 2 61253971

1 Introduction

The federal Parliament has recently amended the legislative scheme for the regulation of telecommunications interception, representing possibly the most significant overhaul and expansion since the current regime was established by the *Telecommunication (Interception) Act 1979* (Cth) ('The TI Act'). The changes were introduced to implement recommendations of a 2005 review by Anthony Blunn ('the Blunn Report').¹

Prior to the 2006 amendments, the TI Act regulated the interception of communications passing over a telecommunications system, prescribing general prohibitions on interception and subsequent use of intercepted communications, and a range of exceptions. While the original intention of the legislation may have been to protect national telecommunications infrastructure, the prevailing view is that the legislation is an important vehicle for the protection of privacy for those using the telecommunications system. This conception of the purpose of the prohibitions in the TI Act creates a tension with the purpose underlying the important exceptions: primarily the warrant system for security and law enforcement purposes. Accordingly, reforms which have expanded the legislative scheme have been seen as requiring the 'balancing' of interests in privacy protection with the interests in security and law enforcement.

This 'balancing' approach was put to the test with the 2006 amendments to the TI Act. The TI Act, renamed the *Telecommunication (Interception and Access) Act 1979* (Cth) ('TIA Act'), was amended to expand the regulatory scheme to cover prohibitions on access to stored communication (i.e., put broadly, communications that have ceased passing over the telecommunications system) and subsequent use, and exceptions to those prohibitions. While these exceptions are structurally similar to those under the interception provisions, the scope of those exceptions is much broader. The new TIA Act also expands the interception tools for security and law enforcement, with the introduction of device warrants and B-Party warrants (i.e., those directed to innocent third parties because of their connection with a 'person of interest').

The amendments were introduced by the government into the House of Representatives on 16 February 2006, and passed the Senate on 30 March 2006. After their introduction into the Senate on 1 March, the amendments were referred to the Senate Legal and Constitutional Legislation Committee ('the Senate Committee'), which reported on 27 March. The Senate Committee produced a report, with the bipartisan support of government and opposition members, which expressed concerns that many of the amendments impacted unduly on privacy interests, and recommended a range of amendments. The Democrats produced

¹ Anthony Blunn, *Report of the Review of the Regulation of Access to Communications* (2005).

a :
fu
th
de
gc
w
C

in
cc
(P
of
fa
of

2

2

re
le;
ha
be
th
th
te
w
ex

A.
pr
cit
an

2

3

+61 2 61253971

The First Workshop on the Social Implications of National Security

a supplementary report, which dissented only to the extent that it recommended further changes to protect privacy. The Senate Committee, it seems, came to the view that the new amendments got the 'balance' wrong. However, its recommendations designed to restore the 'balance'; for the most part, were not accepted by the government. The amendments were passed by a government controlled Senate, with the commitment that the government would continue to consider the Senate Committee's recommendations.

This paper will consider, first, how the 2006 amendments have affected the interception provisions in the TIA Act (Part 2) and, secondly, the new stored communications scheme introduced by the amendments (Part 3). In the final part (Part 4), the paper will argue that the process of law reform, as well as the provisions of the TIA Act, demonstrate how privacy interests have been 'balanced' away in favour of providing government agencies with surveillance tools for the purposes of national security and law enforcement.

2 Interception Regime

2.1 Introduction

The core provisions relating to the interception of telecommunications have remained in place following the 2006 amendments. This section will explain the legislative scheme under the TI Act for interception, and how the 2006 amendments have affected the provisions. Telecommunications interception in Australia has been regulated exclusively at the federal level since 1960 with the enactment of the *Telephonic Communications (Interception) Act 1960* (Cth). Under the *Constitution*, the federal Parliament has legislative power to enact laws with respect to 'postal, telegraphic, telephonic and other like services'.² Although this power is concurrent with the legislative power of State Parliaments, the High Court has held that the exhaustive federal legislation in the area leaves no room for State intervention.³

The TI Act was enacted to replace the *Telephonic Communications (Interception) Act 1960* (Cth). The long title of the TI Act described the legislation as 'An Act to prohibit the interception of telecommunications except where authorised in special circumstances or for the purpose of tracing the location of callers in emergencies, and for related purposes.' The matters motivating the enactment of the TI Act

² *Commonwealth Constitution*, s 51(v). The constitutional validity of the legislation has been upheld in various cases: *Grollo v Commissioner of Australian Federal Police* (1995) 184 CLR 348; *Love v Attorney-General (NSW)* (1990) 169 CLR 307; *Hilton v Wells* (1985) 157 CLR 57; *John Fairfax Publications Pty Ltd v Doe* (1995) 37 NSWLR 81; *Kizon v Palmer* (1997) 72 FCR 409.

³ *Miller v Miller* (1978) 141 CLR 269.

+61 2 61253971

included *security matters and the detection of narcotic offences*.⁴ It is quite clear, however, that the scope of the legislative scheme has shifted considerably from its original intentions.

2.2 The interception provisions – prohibition on interception

The interception prohibitions in the TIA Act work in two phases. The first, considered in this section, is the prohibition on interception. The second, considered in Part 2.6, is the prohibition on subsequent use of intercepted communications. Subject to a range of exceptions, the TIA Act prohibits the interception of communication passing over a telecommunications system (s 7(1)). 'Communication' is defined in s 5(1) to include a 'conversation and a message', in whole or part, whether in the form of: speech, music or other sounds; data; text; visual images; signals; or in any other form or in any combination of forms. An 'interception of a communication passing over a telecommunications system' consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication (s 6(1)). The 2006 amendments seek to provide clearer guidance as to when a communication is passing over a telecommunications system. A communication starts passing over a system when it is sent or transmitted by the sender, and continues passing over the system until it becomes accessible to the intended recipient (s 5F). A communication 'is accessible to its intended recipient if it has been received by the telecommunications service provided to the intended recipient, is under the control of the intended recipient, or has been delivered to the communications service provided to the intended recipient' (s 5H).

The Act excludes from these definitions communications to emergency services numbers (s 6(2B)). Until the 2006 amendments, there was another important exception for interceptions by persons lawfully on premises listening to communications (s 6(2)). When the TI Act was first enacted, the exception in s 6(2) was intended to exempt the activities of telecommunications carriers and their employees from the prohibition on interception to allow equipment testing. The Explanatory Memorandum to the 2006 amendment stated that the operation of the provision 'has become redundant in the deregulated and rapidly changing telecommunications environment',⁵ and its continued operation only 'undermines the strict privacy protections contained in the Act because it may allow participant monitoring'.⁶ During the Senate Committee inquiry, submissions were made opposing the repeal of the provision on the basis that it had other useful applications,

4 Second Reading Speech, Telecommunications (Interception) Bill, House of Representatives, 23 August 1979, 560.
5 Explanatory Memorandum, Telecommunications (Interception) Bill 2006 (Cth) 48.
6 Ibid.

ir
sp
th

2

or
ty
iss
At
rel

Ac
age
of
leg
In
ope
of
thr
wh
dec
Stat
rep

ope
(Ct
tele

7 S
2
P
8 S
(I
ac
fo
9 Fe
of
10 TI
11 TI
sg

+61 2 61253971

including allowing organisations to monitor incoming email for viruses and to filter spam.⁷ The Senate Committee supported the repeal of the provision on the basis that other amending provisions would address the concerns expressed.⁸

2.3 The exceptions to the prohibition on interception – the warrant system

The TIA Act (Parts 2.2, 2.3, 2.5) sets out a number of exceptions to the prohibition on interception, principally interceptions pursuant to a warrant. There are two types of warrants: Part 2.2 warrants and Part 2.5 warrants. Part 2.2 warrants may be issued to the Australian Security Intelligence Organisation ('ASIO') by the federal Attorney-General and the Director-General of Security for intelligence gathering in relation to national security or for the purpose of obtaining foreign intelligence.

Part 2.5 warrants may be issued by federal judges and members of the Administrative Appeals Tribunal ('AAT') to federal⁹ and State law enforcement agencies to intercept telecommunications made in connection with the investigation of specified federal and state offences. Thus, although the scheme is federal, the legislation does not limit Part 2.5 warrants to federal law enforcement officers. In fact, the latest Annual Report by the Attorney-General to Parliament on the operation of the TI Act for the year ending 30 June 2004 reveals that two-thirds of Part 2.5 warrants were issued to State rather than federal agencies in the last three reporting years (see Table 1).¹⁰ State agencies may apply for Part 2.5 warrants where they have been declared to be eligible by the federal Attorney-General.¹¹ A declaration can only be made where the federal Attorney-General is satisfied that the States have enacted legislation requiring the State authorities to meet inspection and reporting requirements equivalent to those set out for Commonwealth agencies.

The scope of the warrant exception has expanded significantly from its original operation. Prior to the TI Act, the *Telephonic Communications (Interception) Act 1960* (Cth) permitted only limited exceptions to the prohibition on the interception of telephonic communications, including circumstances where a warrant had been

7 Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 14 March 2006 (The Australian Banker's Association); Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 20 March 2006 (Telstra).

8 Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Bill 2006* (2006) paras 5.23-5.24. Specifically, the Committee was of the view that the new s 108(2) would address the concern. Subsection 108(2)(e) provides an exception to the prohibition on accessing stored communication for a person exercising duties relating to the installation, connection or maintenance of equipment.

9 Federal law enforcement agencies are the Australian Federal Police and the Australian Crimes Commission: see definition of 'Commonwealth agency' in s 5.

10 The report for the year ending 30 June 2005 has not yet been reported to Parliament.

11 The definition of 'eligible authority' in s 5 of a State covers State police forces and other listed State crime and corruption agencies.

+61 2 61253971

The First Workshop on the Social Implications of National Security

granted by the federal Attorney-General or Director-General of Security for national security purposes. The enactment of the TI Act saw the scheme expanded to allow the issue of warrants for narcotic offences to advance the federal government's 'war on drugs'. Since the late 1980s, the TI Act has been broadened to include categories of offences beyond drugs, most recently to terrorism offences.

Prior to the 2006 amendments, the categories of offences were divided into serious 'Class 1 offences' which included murder, kidnapping, narcotic and terrorism offences. Lesser offences were designated 'Class 2 offences', which included offences involving loss of life or serious injury, serious property damage, serious arson and child pornography. Under this twofold classification privacy considerations were restricted to 'Class 1' offences only. As we shall explore below in 2.5, the utility and practical effect of this approach (in terms of establishing a more stringent threshold for granting Class 1 warrants) is contestable. Indeed, 2006 amendments have removed the distinction between Class 1 and Class 2 offences, redefining existing offences under Classes 1 and 2 offences as 'serious offences' and applying privacy as a factor to be considered in *all* cases. These amendments were supported by the Senate Committee.¹²

Ta
Tel
Tal
AG
AU
NA
AU
CO
NE
CR
INC
AG
NE
POI
COI
SOL
VIC
WES
WES
ANT
COM
WES
COF
COM
TOT

¹² Senate Legal and Constitutional Legislation Committee, above n 8, para 5.9.

+61 2 61253971

The First Workshop on the Social Implications of National Security

Table 1 – Applications for Part 2.5 Warrants (information taken from the *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004*, Table 1).

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR PART 2.5 (PART VI) WARRANTS		
		01/02	02/03	03/04
AUSTRALIAN FEDERAL POLICE	Made	556	691	671
	Refused/withdrawn	1	1	11
	Issued	555	690	660
NATIONAL CRIME AUTHORITY	Made	274	164	-
	Refused/withdrawn	0	0	-
	Issued	274	164	-
AUSTRALIAN CRIME COMMISSION	Made	-	221	390
	Refused/withdrawn	-	0	0
	Issued	-	221	390
NEW SOUTH WALES CRIME COMMISSION	Made	644	803	827
	Refused/withdrawn	0	5	3
	Issued	644	798	824
INDEPENDENT COMMISSION AGAINST CORRUPTION	Made	55	38	31
	Refused/withdrawn	0	0	0
	Issued	55	38	31
NEW SOUTH WALES POLICE	Made	392	383	470
	Refused/withdrawn	0	1	7
	Issued	392	382	463
POLICE INTEGRITY COMMISSION	Made	36	81	62
	Refused/withdrawn	0	0	0
	Issued	36	81	62
SOUTH AUSTRALIA POLICE	Made	54	42	126
	Refused/withdrawn	0	0	0
	Issued	54	42	126
VICTORIA POLICE	Made	343	406	269
	Refused/withdrawn	2	0	0
	Issued	341	406	269
WESTERN AUSTRALIA POLICE	Made	148	190	182
	Refused/withdrawn	1	2	4
	Issued	147	188	178
WESTERN AUSTRALIAN ANTI-CORRUPTION COMMISSION	Made	16	48	22
	Refused/withdrawn	0	0	4
	Issued	16	48	18
WESTERN AUSTRALIAN CORRUPTION AND CRIME COMMISSION	Made	-	-	9
	Refused/withdrawn	-	-	2
	Issued	-	-	7
TOTAL	Made	2518	3067	3059
	Refused/withdrawn	4	9	31
	Issued	2514	3058	3028

+61 2 61253971

2.4 Types of warrants

2.4.1 Service and named person warrants

Both Part 2.2 warrants and Part 2.5 warrants may be issued in respect of a telecommunications service or a person.¹³ Service warrants are issued in relation to a particular 'telecommunication service' where there is a relevant connection between the person of interest and the service.¹⁴ Where a person of interest is using more than one telecommunication service, there is provision for the issue of a named person warrant, which authorises the interception of those telecommunications services in relation to a particular person of interest.

2.4.2 Device warrants

The 2006 amendments have broadened the scope of named person warrants to authorise the interception of communications that are made by means of a 'telecommunications device' used by the person of interest. A 'telecommunications device' is defined as 'a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system' (s 5(1)). The Second Reading speech gives examples of mobile handsets and computer terminals. The issuing authority must not issue a telecommunications device warrant unless 'there are no other practicable methods available' at the time of making the application to identify the telecommunications services used by the person of interest or the interception of a telecommunications service 'would not otherwise be practicable' (ss 9A(3); 46A(3)).¹⁵ The Explanatory Memorandum said this amendment was designed 'to assist interception agencies to counter measures undertaken by persons of interest to evade telecommunications interception such as adopting multiple telecommunications services.'¹⁶

The enactment of this measure was met with some controversy as to whether technology has developed to a point which would allow devices to be identified with sufficient precision, and the potential impact upon the privacy of innocent

¹³ See ss 9, 9A, 11B, 11C, 45, 45A, 46, 46A. In relation to the collection of foreign intelligence there are foreign communications warrants which authorise broader interceptions than service or named person warrants (s 11C).

¹⁴ 'Telecommunication service' is defined to mean 'a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication' (s 5).

¹⁵ The Explanatory Memorandum said that this latter situation 'covers instances in which agencies may be able to identify all services, but is impractical to intercept each service. For example, a person of interest may transfer hundreds of different Subscriber Identity Module (SIM) cards through a mobile handset in quick succession. Interception of each telecommunications service (currently identified by reference to the SIM card) is extremely impractical to achieve before the person of interest changes the SIM card being used' (Explanatory Memorandum, Telecommunications (Interception) Bill 2006 (Cth) 34.)

¹⁶ Explanatory Memorandum, Telecommunications (Interception) Bill 2006 (Cth) 34.

+61 2 61253971

The First Workshop on the Social Implications of National Security

persons where the device identification cannot be determined with such precision.¹⁷ The Blunn Report considered the difficulties of identifying a service being used by a person of interest, particularly the problems associated with the trading of SIM cards. The Report concluded that the 'SIM card and its associated service number is not an effective method of identification'.¹⁸ The Report recommended that 'priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access'.¹⁹ It was suggested that the International Mobile Equipment Identifier ('IMEI') presented a possible system of identification. The Report also indicated that the existing legal regime of named persons warrants may need to be changed to accommodate these developments.²⁰ Having heard the evidence of officers from the Attorney-General's Department and the Australian Federal Police ('the AFP') as to the steps that will be required to be taken by warrant applicants to show a unique identifier, the Senate Committee was not entirely convinced that 'the device being targeted under the warrant was able to be certified as uniquely identifiable'.²¹ Nevertheless, the Committee considered that the operational requirements for law enforcement officers warranted the introduction of the provisions at this time. The technological development needed to have a unique and indelible identifier of the source of telecommunications would take some time,²² and operational needs, it would seem, justified any potential impact on the privacy of innocent parties.

2.4.3 B-Party warrants

Privacy interests have also been significantly affected by the new B-Party provisions inserted by the 2006 amendments. National security telecommunications service warrants under Part 2.2 and Part 2.5 telecommunications service warrants are now available not only in relation to 'persons of interest' but, following the 2006 amendments, also in relation to other innocent third parties who use a telecommunications service to communicate with the person of interest. For Part 2.2 warrants, interception of a telecommunications service may be authorised where the service 'is being or is likely to be the means by which a person receives or sends a communication from or to' a person of interest and the interception 'will, or is likely to, assist' ASIO in its security intelligence gathering functions (s 9(1)). In relation to Part 2.5 warrants, the issuing authority can issue a warrant in respect of a telecommunication service used by an innocent person where information

17 See Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 12 March 2006 (Electronic Frontiers Australia), noted in Senate Legal and Constitutional Legislation Committee, above n 8, para 4.118.

18 Blunn, above n 1, para 2.2.

19 Ibid para 3.3.5.

20 Ibid para 3.2.3-3.2.4.

21 Senate Legal and Constitutional Legislation Committee, above n 8, para 4.122.

22 Ibid para 4.125.

+61 2 61253971

The First Workshop on the Social Implications of National Security

'that would be likely to be obtained' by the interception 'would be likely to assist' in connection with the investigation of a serious offence, in which another person is involved and with whom the innocent person 'is likely to communicate' (s 46(1)).

These circumstances that trigger the issue of a warrant are very broad, and once the warrant has been issued under either Part 2.2 or 2.5, there is little limitation on the type of communication that may be intercepted. There are no limitations as to the identity of the innocent party who uses the telecommunications service, the content of communication that may be intercepted, or the identity of other parties to the intercepted communication. For example, the B-Party might be the suspected person's legal representative with the result that the interception may lawfully capture otherwise privileged communications. It is also wide enough to capture the privileged communications between the legal representative and other clients, as well as collateral intimate communications between the legal representative and spouse, which have no bearing on the investigation. Alternatively, the B-Party may be the suspected person's medical practitioner or religious leader, and the intercepted communication may include communication by the medical practitioner with other patients or by the religious leader with other members of the religious community.

From a law enforcement perspective, it could be argued that anything short of full interception would impose significant burdens upon security and law enforcement agencies to filter out what might be considered to be unrelated communication. From a privacy perspective, the collateral damage to innocent third parties can be limited – indeed, the US federal wiretap regime generally (18 USC § 2510, Ch 119 (1994)) imposes a duty of minimisation on law enforcement officials: 'Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days'. In the Australian context, a policy of minimisation has never been given serious consideration, though there are statutory positions like the Public Interest Monitor (PIM) used in Queensland, that would be suitably qualified (both in terms of high security clearance and promotion of privacy interests) to perform this role. The role of the PIM is discussed below at 4.4.

There are some constraints placed upon the issuing authority. The issuing authority must not issue the warrant unless 'all other practical methods of identifying telecommunications services' used by the person of interest have been exhausted or interception of communications used by the person of interest 'would not otherwise be possible' (ss 9(3), 46(3)). The Second Reading Speech said that:

A
d
P

P
of

cc
T
nu
cc
Bl
as
for
pr
up
ass
ju
op
tha
an
an
pre
23
24
25

26
27
28
29
30

+61 2 61253971

The First Workshop on the Social Implications of National Security

[t]his amendment will assist interception agencies to counter measures adopted by persons of interest to evade telecommunications interception, such as adopting multiple telecommunications services. The ability, as a last resort, to intercept the communications of an associate of a person of interest will ensure that the utility of interception is not undermined by evasive techniques adopted by suspects.²³

There is also the power to impose conditions or restrictions (ss 9(1); 49(1)). Although there is some evidence in the Attorney-General's reports to Parliament that conditions and restrictions have been imposed to protect privacy in relation to Part 2.5 warrants, the cases in which these have been imposed are very few.²⁴

In recognition of the potential privacy intrusion for non-suspects, the time periods for B-Party warrants under both Part 2.2 and Part 2.5 are half the periods of other service warrants.²⁵

The provisions are extremely broad in their scope and, unsurprisingly, attracted considerable attention during the Senate Committee review of the amendment. The potential intrusion on the privacy of innocent third persons was criticised in a number of submissions to the Committee. Indeed, the Australian Privacy Foundation complained that the B-Party amendment had come 'out of the blue'.²⁶ While the Blunn Report had discussed B-Part interceptions, it was in the context of uncertainty as to whether B-Party interceptions were allowable under the provisions in their form at that time. Blunn recognised that law enforcement agencies interpreted the provisions as not allowing B-Part intercepts, but referred to Federal Court authority upholding the validity of B-Party warrants.²⁷ The potential impact on privacy associated with the use of B-Party warrants should not, it was said, 'depend on non-judicial interpretation of the relevant sections, the meaning of which is certainly open to argument'.²⁸ It was in that context that the Blunn Report recommended that the Act 'be amended to clarify that B-Party services may be intercepted in *limited and controlled circumstances*'.²⁹ Blunn, however, made it clear that there are 'obvious and serious privacy implications involved' and that controls must be put in place to prevent the use of B-Party intercepts as 'fishing expeditions'.³⁰

23 Commonwealth of Australia, *Parliamentary Debates*, House of Representatives, 16 February 2006 (P Ruddock) 8.
24 See *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004*, paras 4.13-4, Table 5.
25 Whereas ASIO may seek a telecommunications service under Part 2.2 for a period of six months, B-Party warrants are only available for three months. Similarly, while law enforcement officers can seek a Part 2.5 warrant for 90 days, B-Part warrants under Part 2.5 may only be issued for 45 days (see ss 9B(3A) and 49(3)).
26 Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, March 2006. (Australian Privacy Foundation) 8.
27 Blunn, above n 1, paras 12.1-12.10. Blunn referred to the Federal Court case of *Flanagan v Commissioner of the Australian Federal Police* (1995) 60 FCR 149.
28 Ibid para 12.7.
29 Ibid para 12.10 (emphasis added).
30 Ibid paras 12.6-12.9.

+61 2 61253971

The First Workshop on the Social Implications of National Security

The Senate Committee expressed concern about the potential privacy invasion:

... the Committee accepts the need for B-party warrants. However, the invasion of privacy of innocent parties who become the subject of surveillance merely by reason of association is very significant. The key question is therefore the extent to which the Bill provides a framework for controls over the proposed warrants to balance privacy protection with effective law enforcement.³¹

The Committee recommended various amendments to confine the scope of B-warrants. These recommendations included:

- a requirement for a stronger nexus between the information intercepted and security intelligence gathering and law enforcement purposes before a warrant can be issued;³²
- that agencies exhaust all other methods of identifying the communications services used, rather than exhausting all other 'practicable' methods;³³
- that B-Party warrants cannot be renewed;³⁴
- that certain communications be exempted from B-Part warrants (including communications between lawyer and client; clergy and devotee; doctor and patient and communications by the B-Party with any person other than the person of interest);³⁵
- that there be limits on the subsequent use of intercepted communications;³⁶
- that there should be stricter supervision of destruction of non-material content;³⁷
- that B-Party statistics be separately recorded by each agency and separately reported to Parliament;³⁸
- that the B-Party provisions expire after five years and that they be reviewed

31 Senate Legal and Constitutional Legislation Committee, above n 8, para 4.27.

32 Ibid Rec 18, para 4.43; Rec 19, para 4.56.

33 Ibid Rec 20, para 4.57.

34 Ibid Rec 21, para 4.61.

35 Ibid Rec 22, para 4.80.

36 Ibid Rec 23, para 4.81.

37 Ibid Rec 24, para 4.97.

38 Ibid Rec 24, para 4.97.

+61 2 61253971

prior to or at that time;³⁹ and

- that such a review look more broadly at the use of AAT members to issue warrants and issues of emerging technologies.⁴⁰

Of these recommendations, only the enhanced recording and reporting requirements were adopted by the government in its Senate amendments. Attempts by the Opposition and Democrats to implement the other recommendations were not supported by the government.

2.5 Part 2.5 warrants and privacy considerations

When considering applications for Part 2.5 warrants, the issuing authorities are required to take a range of considerations into account.⁴¹ Prior to the 2006 amendments, the considerations were broadly similar in relation to Class 1 and Class 2 offences, except that the potential invasion of privacy was not a consideration required to be taken into account for warrant applications in relation to Class 1 offences. We have previously observed this to be anomalous, as the need for specific consideration of privacy interests does not diminish with the increased seriousness of the offence under consideration – indeed, there are plausible arguments that the privacy interest become of greater rather than of lesser significance.⁴² The Blunn Report recognised that privacy considerations should be a matter to be considered in all Part 2.5 warrant applications.⁴³ The Second Reading Speech accompanying the amendments⁴⁴ and the Senate Committee Report⁴⁵ also recognised the positive outcome for privacy protection following the removal of the distinction between Class 1 and Class 2, and the requirement to consider privacy considerations in all cases. In light of the low rate of refusal for warrants across both classes, the reality, as the Blunn Report recognised, is that ‘privacy considerations are unlikely to preclude the issue of a warrant for any of the offences characterised as Class 1 offences or indeed for many of the Class 2 Offences’.⁴⁶

³⁹ Ibid Rec 25, para 4.111.

⁴⁰ Ibid Rec 25, para 4.112.

⁴¹ Privacy considerations are not matters expressly to be considered by the issuing authority in relation to Part 2.2 warrants.

⁴² S Bronitt and J Stellios, “Telecommunications Interception in Australia: Recent Trends & Regulatory Prospects” (2005) 29 *Telecommunications Policy* 875, 885.

⁴³ Blunn, above n 1, para 6.4.

⁴⁴ Commonwealth of Australia, *Parliamentary Debates*, House of Representatives, 16 February 2006.

⁴⁵ Senate Legal and Constitutional Legislation Committee, above n 8, para 5.9.

⁴⁶ Blunn, above n 1, para 6.4.

+61 2 61253971

2.6 Interception – prohibition on subsequent use of intercepted communications

The second prohibition in the interception regime is at the stage of subsequent use of intercepted material. Section 63(1) prohibits the communication, use or recording of intercepted information. The primary exceptions from the prohibition include the communication of lawfully intercepted information for security (ss 64, 68(a)) and law enforcement purposes (s 68), and the communication by ASIO of foreign intelligence information (s 64). Law enforcement purposes include the investigation or prosecution of a serious offence or any offence punishable by imprisonment for life or for a period of at least 3 years (ss 5 and 67). Lawfully intercepted information may also be given in a range of proceedings, including a prosecution of any serious offence or offence punishable by imprisonment for life or for a period of at least 3 years (ss 5B and 74). Thus, while the lawful interception of communications may only be in relation to serious offences, lawfully intercepted information may be used for the investigations of, and given in proceedings for, lesser offences. Importantly, the offence which is the subject of the investigation or prosecution need not be connected to the serious offence which motivated the lawful interception. Once that information is given as evidence in an exempt proceeding, it may then be given in any proceeding (s 75A).

2.7 Destruction, record keeping and reporting requirements

Section 79 of the Act imposes destruction obligations on the AFP and the Australian Crimes Commission ('ACC'). Where the chief officer of the agency is satisfied that a restricted record⁴⁷ 'is not likely to be required for a permitted purpose', the records must be destroyed 'forthwith'. The AFP and ACC are also required to keep detailed records of the warrants that have been issued and the use made of intercepted information (ss 80 and 81). The same requirements are imposed on State authorities as preconditions to being authorised to apply for Part 2.5 warrants (s 35(1)(a), (f), (g)).

In relation to Part 2.5 warrants, the Commonwealth Ombudsman is given the responsibility of inspecting the records of Commonwealth agencies in order to ascertain compliance with destruction and record-keeping obligations (s 83). The Ombudsman must report to the Attorney-General within three months of the end of each financial year (s 84), and may report on any other breach of the Act (s 85). In relation to State agencies, regular inspections must be undertaken by an independent State authority, with reports being given to the Commonwealth Attorney-General (s 35(1)(h)-(n)). As indicated above, these are preconditions to being authorised

⁴⁷ Defined as 'a record other than a copy, that was obtained by means of an interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system'.

+61 2 61253971

to apply for Part 2.5 warrants. Commonwealth and State agencies also must give annual reports to the Commonwealth Attorney-General in relation to Part 2.5 interception warrants and the use made of intercepted information (ss 94 and 96). The Attorney-General must then report on these matters to Parliament.⁴⁸

Prior to the 2006 amendment, the Commissioner of the AFP had the responsibility of keeping registers of Warrants, containing information about Part 2.5 warrants. That responsibility is now to be exercised by the Secretary of the Attorney-General's Department. The effect of the amendments is that all Part 2.5 warrants (whether issued by Commonwealth or State agencies) must be notified to the Secretary of the Attorney-General's Department (s 53(1)).⁴⁹

In relation to Part 2.2 warrants, the Inspector-General of Intelligence and Security conducts inspections of all requests for warrants under the *Inspector-General of Intelligence and Security Act 1986* (Cth).

3 (Data)veillance laws: the new stored communication scheme

3.1 Introduction

The 2006 amendments introduced provisions for the protection of stored communication, though permitting access to the material under defined conditions. The scheme broadly contains similar prohibitions, exceptions and reporting requirements to those contained in the interception provisions, although with important differences. The introduction of these provisions followed a protracted attempt by the government to amend the TI Act to deal with stored communications. In 2002 and again in 2004, the government sought amendments to remove the requirement for a warrant where stored communications could be accessed without the use of a telecommunications line. There followed disagreement between the Commonwealth Attorney-General's Department and the AFP on how the existing interception provisions were to be interpreted. The central issue was whether a stored communication had ceased 'passing over the telecommunications system'. The Department's position was that the accessing of communications prior to reaching the recipient's receiving terminal (e.g., from internet service providers) constituted a contravention of the interception provisions, whereas the AFP was of the view that such information could be accessed using the warrants provision in s 3L of the *Crimes Act* (Cth). On this latter view, governmental agencies could use

⁴⁸ At the time of writing, the most recent report is for the period ending 30 June 2004.

⁴⁹ With the repeal of s 54, all Part 2.5 warrants now come into force upon issue.

+61 2 61253971

The First Workshop on the Social Implications of National Security

their general statutory access and notice to produce powers in relation to accessing such information.

In the face of continuing disagreement over the proposed amendment, the Senate Legal and Constitutional Legislation Committee recommended an independent review of the position, and that the status quo be maintained until that review was undertaken.⁵⁰ The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth) was enacted to exclude stored communications from the interception prohibition (s 7(2)(ad)). In recognition that this was to be an interim measure, the 2004 amendment was subject to a 12 month sunset clause and, thus, was to cease operation on 14 December 2005. To allow the government sufficient time to implement the Blunn recommendations, the sunset date was extended to 14 June 2006 by the *Telecommunications (Interception) Amendment (Stored Communications and other measures) Act 2005* (Cth).

Blunn accepted that there was a distinction between intercepting real-time communications and accessing stored communications, although he acknowledged that there may seem to be little difference from a privacy point of view. Real-time voice communications, it was said, 'are likely to be more spontaneous than other forms of data communication and do not provide the opportunity for "second thoughts" prior to transmission offered by those other forms'.⁵¹ The Report recommended that the distinction be maintained.⁵² Although it was recognised that much of modern communication passing over the telecommunications system is not voice communication, Blunn considered it 'impractical and undesirable' to suggest different regimes for real-time access (i.e., interception) depending on whether the communication is voice or in some other form.⁵³

The Blunn Report also recognised that access to stored communications was inadequately regulated by other legislation. While law enforcement agencies could access such information for their purposes, there was insufficient privacy protection in the access authorisation, and the storage and disposal processes.⁵⁴ Blunn recommended that a warrant scheme should be enacted with similar elements to those existing for interceptions, including access by warrants issued by independent issuing authorities who are to consider privacy implications; regulation of subsequent

50 See Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment Bill 2004* (2004); Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (2004).

51 Blunn, above n 1, para 1.4.2.

52 Ibid para 1.4.3.

53 Ibid para 1.4.4. A similar approach was recommended by an earlier review of the US federal wiretap laws: *The Electronic Frontier: The Challenge Of Unlawful Conduct Involving The Use Of The Internet - A Report Of The President's Working Group On Unlawful Conduct On The Internet* (March 2000): <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#ECPA>.

54 Ibid para 1.8.1.

+61 2 61253971

use; and storage and destruction provisions.⁵⁵ Importantly, Blunn was of the view that the data access procedures should apply not only to communications stored within the system, but also information stored in electronic equipment in the possession of the intended recipient. For Blunn, the privacy issues applied equally to both.⁵⁶

3.2 The prohibition on accessing stored communication

Purporting to implement these Blunn recommendations, s 108 of the TIA Act prohibits the accessing⁵⁷ of stored communication without the knowledge of either the intended recipient or the sender of the communication.⁵⁸ It is sufficient to have knowledge for these purposes if a written notice has been given to the person (s 108(1A)). The knowledge element preserves other overt access mechanisms which involve the knowledge of one of the parties to the communication.⁵⁹

The definition of 'stored communication' has been amended to mean a communication that is not passing over a telecommunications system, is held on equipment operated by a carrier, and cannot be accessed on that equipment by a person who is not a party to the communication without the assistance of an employee of the carrier (s5(1)). The amended definition is intended to clarify that the provisions do not cover access to information that involves the knowledge of a party (i.e., overt access) or which does not require the assistance of an employee (i.e., access to voicemail or text message where a mobile phone is seized from a suspect's premises).⁶⁰

3.3 The warrant provisions

There is a range of exceptions to the prohibition on accessing stored communications, primarily those allowing access under an interception warrant (s 108(2)(b)) or a stored communications warrant (s 108(2)(a)). The former essentially operates to expand the authority of an interception warrant to cover stored communication that would have been covered by the interception warrant if it were still passing over a telecommunications system (s 108(3)). As the Explanatory

⁵⁵ Ibid para 1.6.1.

⁵⁶ Ibid para 1.6.3.

⁵⁷ 'Accessing' a stored communication consists of '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' (s 6AA).

⁵⁸ The amending provision originally referred only to the knowledge of the recipient, but was amended in the Senate: Commonwealth of Australia, *Parliamentary Debates, Senate*, 29 March 2006, 86; Commonwealth of Australia, *Parliamentary Debates, Senate*, 30 March 2006, 3.

⁵⁹ See discussion *ibid* 2.

⁶⁰ Supplementary Explanatory Memorandum, Telecommunications (Interception) Bill 2006 (Cth) 2. As the note to s 108 says, the section 'does not prohibit accessing of communications, that are no longer passing over a telecommunications system, from the intended recipient or from a telecommunications device in the possession of the intended recipient'.

+61 2 61253971

The First Workshop on the Social Implications of National Security

Memorandum said, '[i]n the absence of this exception, interception warrants, which only operate prospectively from the time they are served on the carrier, would not authorise access to stored communication previously sent, meaning that an agency would need to also obtain a stored communication warrant to ensure complete access to all communications'.⁶¹ Access to stored communications for ASIO is authorised in this way: the authority of Part 2.2 interception warrants is extended to cover stored communications (s 109).

However, because there is a broader group of enforcement agencies who can apply for a stored communications warrant than those entitled under Part 2.5, Part 3.3 sets out a separate stored communication warrant system for enforcement agencies. Issuing authorities can issue stored communications warrants in respect of a person where there are reasonable grounds for suspecting that a carrier holds stored communications to or from the person, and information 'that would be likely to be obtained' from access 'would be likely to assist in connection with the investigation' of 'a serious contravention in which the person is involved' (s 116). In deciding whether to issue the warrant, the issuing authority is to consider a range of matters including privacy considerations. There is the possibility for conditions and restrictions to be placed upon the warrant (s 117).

Although resembling the broad framework of interception warrants, there are important differences. First, issuing authorities include not only federal court judges and AAT members, but also State magistrates (s 6DB). Secondly, additional agencies may apply for stored communication warrants. In addition to those entitled under the interception provisions, all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue may apply for a stored communications warrant.⁶² The Explanatory Memorandum suggests that these agencies would include the Australian Customs Services, the Australian Tax Office, the Australian Securities and Investment Commission, and similar State and Territory agencies.⁶³ Unlike the framework under the interception regime, there is no Commonwealth vetting mechanism for State agencies. As discussed above, on satisfaction that State agencies have requisite inspection and reporting mechanisms in place, the Attorney-General can declare a State agency to be eligible to apply for interception warrants. No such mechanism applies under the stored communication provisions.

Thirdly, warrants may be sought in relation to 'serious contraventions'. These are defined to include not only 'serious offences' as in the case of interception

61 Explanatory Memorandum, *Telecommunications (Interception) Bill 2006* (Cth) 10.

62 'Enforcement agencies' are defined (see s 5(1)) by reference to s 282 of the *Telecommunications Act 1997* (Cth). Potentially, many agencies of State and Territory government could be granted access to these warrants for the purpose of enforcing any law which carry the prescribed pecuniary penalties.

63 Explanatory Memorandum, *Telecommunications (Interception) Bill 2006* (Cth) 12.

+61 2 61253971

The First Workshop on the Social Implications of National Security

warrants, but also offences punishable by imprisonment for at least three years or a fine of at least 180 penalty units (or 900 in the case of a corporation); and statutory contraventions that give rise to a pecuniary penalty or equivalent monetary liability of 180 penalty units (or 900 in the case of a corporation) (s 5E). Fourthly, as will be considered further below, reporting requirements for stored communication warrants are not as burdensome.

The broadening of the access regime and the relaxation of various thresholds in relation to stored communications appeared to be justified primarily on the basis of a perceived difference between real-time and stored communications, a distinction made in the Blunn Report. Blunn focused on the distinction between 'spontaneous' forms of communication and forms of communication which allowed for 'second thoughts'. This was reflected by the responses by the Attorney-General's Department to the Senate Committee when quizzed about the Blunn distinction between real-time and stored communication:

Mr McDonald [Assistant Secretary, Attorney-General's Department]: I had some quite interesting discussions with Mr Blunn about this issue, and it is not an easy one, but certainly the idea that it is slightly more considered is something that was in his mind or was something that we discussed. It is something that is in writing – something that definitely involves more consideration of the expression – although there is the speed issue.⁶⁴

Mr McDonald then explained that some written forms like text messaging can be sent quite quickly.

However, there is a number of difficulties with the making of that distinction. Even if one accepts the rationale, that written forms of communication involve more consideration or reflection, the live/stored distinction is not a good approximation for the spontaneous/considered distinction that Blunn had in mind. Both live communication and stored communication may comprise forms of spontaneous and considered communication. In fact, the amendments recognise this by extending the authority of interception warrants to cover stored communications. However, as alluded to by Mr McDonald of the Attorney-General's Department, the assumption that the written form is more considered does not hold as a general rule. This point was the subject of discussion during the Senate Committee process and the Senate debate.⁶⁵ The opposition to such a distinction was well illustrated by Senator Stott Despoja's comments during the course of the Senate debates: '[t]he premise that more consideration or thought may be put into an SMS, an email message or a message left on voicemail in comparison to a telephone conversation is, in this day

64 Evidence to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 15 March 2006, (Geoffrey McDonald) 55.

65 See, for example, Evidence to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 15 March 2006, (Prof George Williams) 28, 31.

+61 2 61253971

The First Workshop on the Social Implications of National Security

and age, spurious.⁶⁶

In any event, even if one were to accept the spontaneous/considered distinction, and that the live/stored distinction was a reasonable approximation, it might still be argued – as Blunn accepted – that from a privacy perspective, there is no relevant difference that would justify different levels of protection.⁶⁷ Clearly, as the Blunn Report concluded, the mode of expression does not alter the reasonable expectation of privacy in respect of such personal communications. Moreover, it is possible to argue that law enforcement access to stored communications (email, SMS messages, etc) enlivens an even stronger privacy interest: in these cases, the state is seeking access to past communications that record thoughts and behaviours of individuals over a much longer period (if measured in the equivalent of real-time) than the standard three months of prospective surveillance permitted under interception warrants. In such cases, the conditions of access to such material should be more rather than less stringently enforced.

The Senate Committee accepted that the relevant distinction in this context is between covert and overt searches, and the guiding test should be the impact on individual privacy.⁶⁸ Given the significant impact of covert access on privacy, and considering that the wider group of enforcement agencies have access to covert access methods,⁶⁹ the Committee recommended that: (i) enforcement agencies able to access stored communications should be limited to those eligible under the interception provisions;⁷⁰ (ii) States enact complementary legislation as a precondition to being entitled to apply for a warrant;⁷¹ (iii) warrants be limited to criminal offences;⁷² and (iv) issuing authorities be limited to those under the interception provisions.⁷³

The government did not seek to implement these recommendations, and did not support the Opposition and Democrat amendments seeking to do so. In rejecting these amendments and a correspondence of live and stored communication, Senator Ellison said that:

to compare stored communications with a communication that is taking place is

66 Commonwealth of Australia, *Parliamentary Debates*, Senate, 28 March 2006.
67 See Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, March 2006 (*New South Wales Council for Civil Liberties*) 3; Australian Privacy Foundation above n 26, 5.
68 Senate Legal and Constitutional Legislation Committee, above n 8, para 3.39.
69 In fact, ASIC had provided information that '[t]he majority of ... access to emails [came] from access at the user's end' and that in the previous 12 months it had not accessed stored communications from an internet service provider: *ibid* paras 3.36-7.
70 *Ibid* Rec 2, para 3.42.
71 *Ibid* Rec 6, 3.67. Or, at least as an interim measure, that the definition of enforcement agency be amended to allow an agency to be excluded from being able to obtain a stored communication warrant (Rec 7, para 3.68).
72 *Ibid* Rec 3, 3.43.
73 *Ibid* Rec 5, 360.

+61 2 61253971

The First Workshop on the Social Implications of National Security

somewhat unreal. ... [O]nce a message or communication has been transmitted it is of a different nature to one that is in process. That is precisely what was acknowledged by Mr Blunn in his report when he acknowledged the difference between real-time interception and a communication that has been received.⁷⁴

However, given the discussion above, if a transmitted communication is *different in nature* to a communication whilst in transmission, that rationale is yet to be provided.⁷⁵

3.4 Prohibition on subsequent use

The prohibition on subsequent use of stored communication information and related exceptions broadly mirror those for the interception scheme. Stored communication information cannot be communicated, used, recorded or given in evidence in a proceeding (s 133). The principal exceptions include the communication of lawfully accessed information for security (ss 136, 137) and law enforcement purposes (s 68), and the communication by ASIO of foreign intelligence information (ss 136, 137). Law enforcement is, however, much broader than under the interception provisions. The permitted purposes include investigations and prosecutions for offences punishable: by imprisonment for a period of 12 months or by a fine of at least 60 penalty units (or 300 penalty units in the case of corporations); and investigations and proceedings for recovery of pecuniary penalties of at least 60 penalty units (or 300 penalty units in the case of corporations) (ss 5B and 143). Lawfully accessed information may also be given in a range of proceedings. Again, the proceedings are broader than those under the interception provisions (ss 5B and 143). As with the interception provisions, the threshold for subsequent use is lower than the warrant thresholds, and subsequent use need not be connected to the purpose for which the information was accessed. Once that information is given in evidence in an exempt proceeding, it may then be given in any proceeding (s 145).

3.5 Destruction, record keeping and reporting requirements

Similar to the interception provisions, stored communication information in the possession of an enforcement agency, must be destroyed 'forthwith' where the information is no longer required for the relevant purpose (s 15). However, there are important differences in relation to the record keeping and reporting requirements

⁷⁴ Commonwealth of Australia, *Parliamentary Debates, Senate*, 29 March 2006 (Sen. Chris Ellison) 42.

⁷⁵ It should be noted that Senator Ellison also tried to justify the different treatment on the basis that an interception warrant involves ongoing monitoring, whereas a stored communication warrant involves access at a fixed point in time to information already received (*ibid*). While there may be such a difference, it still remains unclear why this should be a relevant consideration supporting less stringent treatment for stored communications warrants. To the contrary, the retroactive nature of stored communications warrants may suggest that more stringent measures be put in place for stored communications warrants.

+61 2 61253971

The First Workshop on the Social Implications of National Security

for stored communications warrants when compared with those discussed above in relation to interception warrants. First, while enforcement agencies have to keep records, the content of those records are not required to be as detailed as those under the interception provisions. Secondly, the information to be provided by enforcement agencies to the Attorney-General, and then reported by the Attorney-General to Parliament, is also significantly less detailed (ss 162 and 163). Thirdly, as noted earlier, there is no equivalent mechanism to that in the interception provisions that requires a State agency to have record keeping and reporting mechanisms in place as preconditions to accessing the stored communications warrants. The less burdensome requirements were said in the Explanatory Memorandum to reflect 'the wider agency access and the lower threshold to be met'.⁷⁶

These less burdensome requirements were the subject of criticism through the Senate Committee process and in the Committee's report. In response, the Committee emphasised that the 'reporting obligations are vital to provide adequate transparency and accountability for the stored communications warrant regime' and that 'a lower offence threshold does not equate to a lesser reporting obligation'.⁷⁷ The Committee recommended that the 'Bill be amended to require agencies and the [Attorney-General] to report on the use and effectiveness of stored communications warrants in a manner equivalent to the existing reporting obligations for telecommunications interception warrants'.⁷⁸ The Committee also recommended that time limits be included within the legislation for the review and destruction of stored communication information.⁷⁹

The government, however, did not implement these recommendations, and the Opposition and Democrat proposed amendments designed to give them effect, were not supported by the government in the Senate. In opposing the amendments, Senator Ellison said:

We believe that the reporting proposed by the government is sufficient. When you look at the [TI Act] reports that are being furnished to the parliament, they are indeed detailed ... It is a comprehensive report. We believe that to go as far as the Democrats are suggesting could well have some operational impact and we are not inclined to support these amendments.⁸⁰

It appears that the 'operational impact' the Senator had in mind was that organised criminals would be able to track the trends of law enforcement revealed in the

⁷⁶ Explanatory Memorandum, Telecommunications (Interception) Bill 2006 (Cth) 13.

⁷⁷ Senate Legal and Constitutional Legislation Committee, above n 8, para 3.88.

⁷⁸ Ibid Rec 11, para 3.91.

⁷⁹ Ibid Rec 10, para 3.81.

⁸⁰ Commonwealth of Australia, *Parliamentary Debates, Senate*, 30 March 2006 (Sen. Chris Ellison) 28.

+61 2 61253971

annual reports, and change their methods accordingly.⁸¹ When pressed further by Senator Stott Despoja on how the 'basic' statistical information revealed in the interception reports might create operational problems,⁸² Senator Ellison replied that the Senate Committee's recommendation about reporting requirements are still being considered, and that Senator Stott Despoja's concerns would be 'taken on board'.⁸³ If the 'operational impact' is affecting policy development in this way, there is a real danger that future amendments might, in fact, go the other way and lower the reporting requirements for interceptions as well.

Finally, the Ombudsman is given an inspection and reporting role in relation to stored communications warrants issued to enforcement agencies (s 153). The Ombudsman must report on agency compliance with record-keeping and enforcement obligations within three months after the end of each financial year. During the Senate Committee inquiry, the Ombudsman submitted to the Committee his concern that the expanded role would impose an additional burden on the resources of his office. Professor McMillan indicated that it would be likely that greater resources would be necessary to complete the additional functions, and that it would be useful if the reporting deadline under the stored communication regime be extended from three to six months.⁸⁴ The Senate Committee supported these requests.⁸⁵ In declining to support Opposition and Democrat amendments to give effect to these recommendations, Senator Ellison said: '[the government] sees no reason to delay the report of the Ombudsman – in fact, it should be reporting which is fairly expeditious'. Although recognising that the government would continue to consider the Committee's recommendations, the Senator concluded that '[a]t this stage, there is no compelling reason ... to agree to this amendment'.⁸⁶

4 Balancing away privacy interests

4.1 Introduction

We have previously observed that various developments since the enactment of the TI Act have placed considerable pressure on privacy in a way not initially

⁸¹ Ibid 28-9.

⁸² Ibid 29.

⁸³ Ibid 30.

⁸⁴ Submission to Senate Legal and Legislation Committee, Parliament of Australia, Canberra, March 2006 (Commonwealth Ombudsman) 2-3.

⁸⁵ Senate Legal and Constitutional Legislation Committee, above n 8, Rec 12 and 13, paras 3.92 and 3.93.

⁸⁶ Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 March 2006 (Sen. Chris Ellison) 26. Ironically, this position was put forward shortly prior to the Senator's forced acknowledgment that the Attorney-General's report to Parliament for the year ending 30 June 2005 had not yet been reported to Parliament (ibid 28).

+61 2 61253971

The First Workshop on the Social Implications of National Security

contemplated. The regulatory landscape has shifted to such an extent that there is no longer a position that resembles a 'balance'. We called for legislative reform that places rights protection - which extend beyond privacy to include rights for a fair trial and due process - at the centre of regulatory design.⁸⁷

The response to such calls seemed promising, at least in respect of privacy. In his findings, Blunn said that 'the protection of privacy should continue to be a fundamental consideration in, and *the starting point for*, any legislation providing access to telecommunications for security and law enforcement'.⁸⁸ The Senate Committee commenced its task with the following statement: '[t]he principal consideration of legislation which governs access to personal communications should be the protection of privacy'.⁸⁹

Despite these statements, the government's approach remains one of 'balancing' privacy considerations with security and law enforcement objectives and, indeed, most of the parliamentary debate is couched in terms of finding the right 'balance'.

However, there is a growing recognition that a balancing approach to the legal regulation of covert surveillance is problematic. The New South Wales Law Reform Commission had initially taken the balancing approach, arguing that privacy interests must be weighed against legitimate societal interests in preventing and prosecuting crime.⁹⁰ It subsequently revised that approach following further research, concluding that the balancing approach was 'inherently flawed'.⁹¹ Although a persistent idea in all areas of policy development, balancing models rarely achieve an accommodation between competing interests. In other law enforcement contexts, critical scholars have argued that 'balancing' tends to prioritise the interests of crime control over due process.⁹² In the context of telecommunications interception, the balancing process has systematically traded-off privacy interests in favour of law enforcement.

The remainder of this paper will consider the extent to which privacy interests have been balanced away through the adoption of 'balancing' rhetoric. First, it will be seen that the accelerated passage of the 2006 amendments through Parliament did not allow for a proper consideration of the privacy implications (Part 4.2.). The Senate Committee process, which is often praised for the contribution that it makes during the legislative process towards rights-protection, was marginalised

⁸⁷ Bronitt and Stellios, above n 42, 887.

⁸⁸ Blunn, above n 1, 5 (emphasis added).

⁸⁹ *Ibid* 7.

⁹⁰ New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report No. 98 (2001).

⁹¹ *Ibid* para 2.4.

⁹² A Ashworth, 'Crime, community and creeping consequentialism' [1996] 43 *Criminal Law Review*, 220-30; S Bronitt and D Roche, 'Between Rhetoric and Reality: Sociolegal and Republican Perspectives on Entrapment' (2000) 4 *International Journal of Evidence and Proof* 77.

+61 2 61253971

(Part 4.3.). Secondly, it will be seen that the two main mechanisms within the legislative scheme to protect the privacy interests of a person who is the subject of a warrant – the warrant system (Part 4.4.) and civil remedies (Part 4.5.) – are largely illusory. Thirdly, the 2006 amendments illustrate that, when the opportunity arises for a consideration of which interests should prevail, security and law enforcement objectives systematically prevail over privacy interests (Part 4.6.).

4.2 The process of 'balancing'

If the model of 'balancing' interests is to have any legitimacy, the process of law-making needs to be capable of taking various interests into account. The 2006 amendments to the TI Act, however, are an example of a process that did not adequately allow for a proper exploration of how the proposed law impacts upon competing interests.

The amendments were introduced into the House of Representatives on 16 February 2006, and were debated on the evening of 28 February and the morning of 1 March. The Bill was then introduced into the Senate on 1 March 2006 and was immediately referred to the Senate Legal and Constitutional Legislation Committee for review by 27 March. Written submissions were invited by 13 March, and a public hearing was held on 15 March. Only seven days notice was given for those wanting to provide written submissions, and only three days notice was given for those wanting to appear at the hearing. The Senate Committee reported on 27 March. The Senate debated various amendments on 27, 29 and 30 March, with the legislation passing the Senate with amendments on 30 March.

Various submissions to the Senate Committee complained about the lack of time to properly consider the amendments. The Law Society of South Australia said that '[t]he very short timeframe given for consideration of this major piece of proposed legislation is of great concern and has not allowed proper consultation and consideration of it'.⁹³ The Law Council of Australia said that '[i]n the context of the Bill, it is particularly important to provide reasonable time for consultation to ensure that the government can properly consider concerns of the Australian people and to achieve an appropriate balance between safeguarding fundamental human rights and the "threat to the Australian people"'.⁹⁴ Even the most comprehensive submission made by Electronic Frontiers Australia complained of insufficient time to consider all the amendments properly.⁹⁵ The Supplementary Report of the

93 Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 14 March 2006 (Law Society of South Australia) 1.
94 Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 13 March 2006 (Law Council of Australia) 4.
95 Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 12 March 2006 (Electronic Frontiers Australia), above n 17, 8.

at that there is
ve reform that
ights for a fair
of privacy. In
ntinue to be a
ion providing
8 The Senate
[t]he principal
mmunications
s of 'balancing'
d, indeed, most
'balance'.
ch to the legal
s Law Reform
ivacy interests
d prosecuting
s, concluding
sistent idea in
ommodation
ritical scholars
ntrol over due
ncing process
ement.
ivacy interests
c. First, it will
gh Parliament
s (Part 4.2.).
tribution that
marginalised

30-30; S Bronitt and
2000) 4 *International*

+61 2 61253971

The First Workshop on the Social Implications of National Security

Australian Democrats to the Senate Committee's Report noted 'with dismay the lack of time that the committee had been allocated to report on the bill'.⁹⁶ The lack of time for both the Senate Committee and those submitting to the Committee was a frequent complaint by the Opposition, Democrats and Greens throughout the Senate debate.⁹⁷

The government defended these attacks on the basis that urgent legislation was needed on stored communications before the sunset date of 14 June. While this may address the stored communication provisions, it provides an insufficient basis to explain why the other privacy-impacting amendments were pressed at that time in the face of opposition in Parliament and from the Senate Committee's bipartisan report. The government emphasised on a number of occasions through the parliamentary debates that this was the first step in the process of responding to the Blunn report, and that other recommendations from the Blunn report and the Senate Committee's report are the subject of ongoing review. It remains to be seen whether other privacy-protecting recommendations will be the subject of future amendments.

The speed with which the amendments were considered not only denied sufficient time for consideration of their impact, but it also at times created confusion within the Senate whilst amendments were being debated. The most obvious example was when the Senate was considering an Opposition amendment dealing with copies of stored communication. As explained above, the amendments introduced a new definition of stored communication. Electronic Frontiers Australia had argued to the Senate Committee that it was not clear whether a copy of a stored communication is to be regarded as a stored communication for the purposes of the Act. The Senate Committee recommended that the Bill be amended 'to ensure that copies of communications can not be accessed without a stored communications warrant'.⁹⁸ The Opposition's amendment to implement this recommendation was supported by the Democrats, but opposed by the government. However, in explaining why the government opposed the amendment, it became clear that Senator Ellison misunderstood the nature of the amendment:

I think Mr Tom Sherman covered this aspect in a report several years ago. The government considered it then and decided not to proceed with it. As I understand it, the agencies concerned have indicated that there is an administrative burden in this which far outweighs any benefit that might be provided by possible enhanced

⁹⁶ 'Supplementary Report with Additional Comments of Dissent by the Australian Democrats', Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Bill 2006* (2006) para 1.4.

⁹⁷ See for example: Commonwealth of Australia, *Parliamentary Debates*, Senate, 28 March 2006, 54, 55, 76, 79; Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 March 2006, 29, 40.

⁹⁸ Senate Legal and Constitutional Legislation Committee, above n 8, Rec 14, para 3.107.

+61 2 61253971

accountability.⁹⁹

Senator Ellison was discussing a different point about extending the record keeping and destruction obligations under the TI Act to include copies of records. In his review of named person warrants in 2003, Tom Sherman had recommended that the definition of restricted record be amended to include copies of records.¹⁰⁰ There is no indication in the Senate debate that any of the parties recognised this misunderstanding.

Thus, in addition to the concerns expressed about time limitations affecting a proper consideration of the impact of the amendments, the speed with which the amendments were passed also impacted upon the capacity of legislators to understand the scheme being enacted. Both of these consequences have a negative effect on policy and legislative design. If the 'balancing' model is to be adopted, the process of law-making must provide a genuine opportunity for the balancing of competing interests.

4.3 The effectiveness of the Senate Committee system

Despite the limitations confronting the Senate Committee, its members displayed impressive comprehension of the legislative scheme and the issues arising from the proposed amendments. The Committee produced a bipartisan report which responded to the key issues raised by the written and oral submissions. The Committee considered that, in a number of important respects, the proposed amendments tilted the balance too far away from the protection of privacy interests and recommended various amendments – many of which have been or will be discussed in this paper. The Democrat Supplementary Report dissented only in the sense that it sought further privacy protection within the legislative scheme.

While purporting to respond to the Committee's report, it is quite clear that the government's amendments in the Senate only reflected the privacy concerns of the Committee in a limited way. The only privacy enhancing recommendation incorporated by the government into its amendments was for B-Party warrant statistics to be separately reported to Parliament.¹⁰¹ The Opposition and the Democrats sought to introduce further amendments in an attempt to implement other Committee recommendations, however, none of these attempts were supported by the government, including Senators who supported the amendments as members

⁹⁹ Commonwealth of Australia, *Parliamentary Debates*, Senate, 29 March 2006 (Sen. Chris Ellison) 130.

¹⁰⁰ Tom Sherman, *Report of Review of Named Person Warrants and Other Matters*, (Commonwealth of Australia, 2003) Ch 9. The definition had been amended by the *Telecommunications (Interception) Legislation Amendment Act 2000* (Cth) to exclude copies from the definition.

¹⁰¹ See Senate Legal and Constitutional Legislation Committee, above n 8, Rec 24, para 4.97. There was some debate in the Senate as to how many Senate Committee recommendations the government had adopted; see Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 March 2006, 1-2.

+61 2 61253971

of the Senate Committee. This turnaround led Senator Stott Despoja to say during the Senate debates:

We have backbenchers in here today who signed off on the legislative report but were forced [to] vote against the recommendations contained in that report. Doesn't anyone have a problem with that? I think that is quite extraordinary. Some of the safeguards built into that majority report and proposed for legislation have since been voted against by the people who mooted them. Maybe the Senate committee process is a farce now.¹⁰²

The government defended its lack of support for further amendments to implement Committee recommendations on the basis that the recommendations are the subject of ongoing review. Thus, the telecommunications interception context may provide an early test to see whether the Senate Committee process will serve a useful role in an era of government control of the Senate.

4.4 Safeguarding privacy through warrants

The warrant system in Australia is often presented as an important safeguard for the protection of privacy interests. Following the 2006 amendment, privacy protection is a factor to be taken into account in the issuing of all Part 2.5 interception warrants and stored communications warrants. Although it is not a factor expressly to be taken into account by an issuing authority in relation to Part 2.2 warrants, the legislative scheme does not preclude consideration of the impact upon privacy. There are, however, some problems with seeing the warrant system as providing an effective bulwark against arbitrary intrusion into privacy.

First, as noted above, the Blunn report said that privacy considerations are unlikely to outweigh security and law enforcement considerations. This observation is supported by the experience with Part 2.5 warrants. Table 1 shows the application statistics for the last three reporting years. The figures clearly show that an almost negligible percentage of applications are refused or withdrawn. The figures are not further broken down into percentage of applications withdrawn and refused. However, even if all applications in this group were refused, the percentage of refusal is still very low, peaking in 2003/4 at one per cent.

There are mechanisms which could be incorporated into the legislative scheme at the point of issuing warrants which would allow for a stronger recognition of privacy interests. In Queensland, a PIM has the role of appearing at the hearing of applications for surveillance device warrants to examine witnesses and make

¹⁰² Commonwealth of Australia, *Parliamentary Debates, Senate*, 30 March 200, 43.

+61 2 61253971

The First Workshop on the Social Implications of National Security

submissions on the appropriateness of granting the application.¹⁰³ In its submissions to the Senate Committee, Electronic Frontiers Australia suggested that a public interest monitor be incorporated into the legislative scheme. During the course of the Senate debate, the Democrats suggested that a public interest monitor, based upon the Queensland model, be incorporated. However, no amendment was pressed.

Secondly, the involvement of judicial officers is often seen as central to the warrant process, but the judicial involvement is increasingly being marginalised. As noted, there is no judicial involvement in Part 2.2 warrants. But, even in relation to Part 2.5 warrants, judicial involvement is increasingly more limited for two reasons: first, Federal Court judges have been reluctant to participate in the process and, secondly, the overwhelming number of applications is now made to AAT members.

In relation to the first, there has been a general retreat from the warrant process by Federal Court of Australia judges since the High Court's decision in *Grollo v Palmer*.¹⁰⁴ The Court in that case considered whether the function of issuing a warrant was compatible with the constitutional scheme of separating powers among three arms of government: the legislature, the executive and the judiciary. It is well established constitutional doctrine, that federal courts created by Parliament are only able to exercise judicial power or non-judicial power that is incidental to the exercise of judicial power.¹⁰⁵ The High Court held that the issuing of an interception warrant is an exercise of executive, not judicial, power. However, with considerable judicial ingenuity, the Court cleared the way for federal court judges to issue warrants if: (i) the power is conferred on the judge in his or her personal capacity (i.e., as *persona designata*); (ii) the function is not incompatible with the capacity of the judge or the court to exercise judicial power; and (iii) the judge consents to the exercise of the power. In holding that the power to issue interception warrants was not incompatible with the exercise of judicial power, a majority of the High Court emphasised the desirability of having judicial supervision of the process:

Yet it is precisely because of the intrusive and clandestine nature of interception warrants and the necessity to use them in today's continuing battle against serious crime that some impartial authority, accustomed to the dispassionate assessment of evidence and sensitive to the common law's protection of privacy and property (both real and personal), be authorised to control the official interception of communication.¹⁰⁶

It was, the majority said, the 'professional experience and cast of mind of a judge'¹⁰⁷ that would guarantee an appropriate balance between law enforcement agencies and

¹⁰³ *Queensland Police Powers and Responsibilities Act 1997* (Qld) s 159.

¹⁰⁴ (1995) 184 CLR 348.

¹⁰⁵ *R v Kirby; ex Parte Boilermakers' Society of Australia (Boilermakers' Case)* (1956) 94 CLR 254.

¹⁰⁶ *Grollo v Palmer* (1995) 184 CLR 348, 367 (Brennan CJ, Deane, Dawson and Toohey JJ).

¹⁰⁷ *Ibid* 367.

+61 2 61253971

The First Workshop on the Social Implications of National Security

the person of interest. This, however, was not a view shared by all judges. McHugh J considered that 'public perception [of judges] must be diminished when the judges ... are involved in secret, *ex parte* administrative procedures, forming part of the criminal investigative process, that are carried out as a routine part of their daily work.'¹⁰⁸

In 1998, a number of judges of the Federal Court of Australia and the Family Court of Australia notified the Attorney-General that they would cease to participate in the granting of warrants under the legislation.¹⁰⁹ Consequently, Parliament amended the TI Act to allow AAT members to issue warrants. The most recent numbers show that Family Court judges and Federal Magistrates are still formally available to issue warrants (see Table 2), but only three Federal Court judges were formally available in the 2003/04 period.¹¹⁰

Table 2 – Availability of Federal Court Judges, Family Court Judges, Nominated AAT Members and Federal Magistrates to Issue Warrants (information taken from the *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004*, Table 30).

ISSUER	NUMBER ELIGIBLE
NOMINATED AAT MEMBERS	18
FAMILY COURT JUDGES	21
FEDERAL COURT JUDGES	3
FEDERAL MAGISTRATES	16

The second reason why judicial involvement with the warrant process is more limited is because law enforcement agencies are seeking warrants primarily from AAT members. In the 2003/4 period AAT members issued 76 per cent of the warrants issued (see Table 3). This figure was even greater in the 2002/3 period, when 91 per cent of warrants were issued by AAT members. The increased use of AAT members to issue warrants was noted by the NSW Council of Civil Liberties to the Senate Committee.¹¹¹ Although the Committee was careful not to make any negative

¹⁰⁸ Ibid 380. It was submitted to the Senate Committee that there may be some constitutional questions over the warrant provisions for stored communications because of the 'significantly more lenient' preconditions for exercising the power and the 'considerably less burdensome' reporting requirements: see Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 13 March 2006 (Gilbert & Tobin Centre of Public Law) 4. The central principle for determining validity in this context is whether the judge retains impartiality and independence from the other arms of government and the relevant court can be said to retain institutional integrity. This has been emphasised by the Court more recently in a context where similar principles are applied (*Fardon v Attorney General for the State of Queensland* (2004) 210 ALR 50). There does not appear to be anything in the legislative changes that threatens impartiality or integrity to any greater extent than the provisions before the Court in *Grollo*. If a future Court were to invalidate the provisions, it would be because it has adopted a different approach to that adopted in *Grollo*.

¹⁰⁹ *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004*, para 4.45.

¹¹⁰ These figures, however, may not be a true reflection of the actual number of judges who are prepared to participate as many of them have not formally withdrawn their consent to issue warrants: *ibid*.

¹¹¹ See Senate Legal and Constitutional Legislation Committee, above n 8, para 3.55.

+61 2 61253971

The First Workshop on the Social Implications of National Security

judges. McHugh J
when the judges ...
part of the criminal
daily work.¹⁰⁸

and the Family
case to participate
ently, Parliament
The most recent
are still formally
ourt judges were

observations about the role of AAT members in the process, it recommended that a future review of the legislation 'should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime'.¹¹² The Democrats put forward a stronger position during the Senate debates, saying that they did not support having the AAT as an issuing authority: '[w]e believe, not only from looking at the statistics, that it is lowering a threshold. It is making it easier for warrants to be issued or obtained.'¹¹³ The fact that AAT members have, at least on one occasion, met with law enforcement agencies to discuss 'generic issues'¹¹⁴ tends to give the impression that AAT members do not see themselves as part of the checks and balances on law enforcement.

Thus, the reality of the warrant system does not reflect the perception: the percentage of warrant cases involving the involvement of judges is now significantly reduced.

Court Judges,
Issue Warrants
1979: Report for the

Table 3 - Number of Warrants Issued in 2003-2004 Reporting Year by Federal Court Judges, Family Court Judges, Nominated AAT Members and Federal Magistrates (information taken from the *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004, Table 31*).

AGENCY	ISSUER			
	FAMILY COURT JUDGES	FEDERAL COURT JUDGES	NOMINATED AAT MEMBERS	FEDERAL MAGISTRATES
AUSTRALIAN FEDERAL POLICE	9	29	592	30
INDEPENDENT COMMISSION AGAINST CORRUPTION	0	0	31	0
AUSTRALIAN CRIME COMMISSION	0	11	379	0
NEW SOUTH WALES CRIME COMMISSION	0	0	824	0
NEW SOUTH WALES POLICE	0	0	6	457
POLICE INTEGRITY COMMISSION	0	0	55	7
SOUTH AUSTRALIA POLICE	0	13	113	0
VICTORIA POLICE	0	0	269	0
WESTERN AUSTRALIAN ANTI-CORRUPTION COMMISSION	18	0	0	0
WESTERN AUSTRALIAN CORRUPTION AND CRIME COMMISSION	7	0	0	0
WESTERN AUSTRALIA POLICE	145	0	33	0
TOTAL	179	53	2302	494

process is more
arily from AAT
of the warrants
ed, when 91 per
AAT members
s to the Senate
e any negative

tions over the warrant
r exercising the power
al and Constitutional
nre of Public Law) 4.
lity and independence
tegrity. This has been
Attorney General for the
changes that threatens
future Court were to
in *Grollo*.

pared to participate as

¹¹² Senate Legal and Constitutional Legislation Committee, above n 8, Rec 25, para 4.112. This recommendation was supported by the Supplementary Report of the Democrats.

¹¹³ Commonwealth of Australia, *Parliamentary Debates, Senate*, 30 March 2006, 37.

¹¹⁴ Sherman, above n 100, 11.

+61 2 61253971

4.5 Civil remedies

Part 2-10 of the TIA Act creates a civil remedy in favour of an aggrieved person in circumstances where there has been an interception in contravention of s 7(1), or a communication of information in breach of s 63. An individual is an 'aggrieved person' for these purposes if the person was a party to the intercepted communication or the communication was made on the person's behalf (s 107A). An application for such a remedy may be made to the Federal Court of Australia or a court of a State or Territory, or to a criminal court that has convicted a person of a breach of ss 7(1) or 63. The new Part 3-7 creates an identical mechanism for civil remedy in relation to the accessing of a stored communication in contravention of s 108(1), or the communication of information in contravention of s 133.

It is one thing for a civil remedy to be created, it is quite another for it to be effective. The covert nature of the process of applying for a warrant will mean that it is only when the information becomes public, for example through a prosecution or enforcement process, that a person may become aware that he or she is an aggrieved person. Thus, innocent persons whose communications have been intercepted or accessed in contravention of the Act, and who are not later the subject of criminal prosecution or another enforcement mechanism, are unlikely to know whether they were aggrieved persons and entitled to a remedy under the Act. This issue surfaced during the Senate Committee inquiry, particularly in relation to B-Party warrants. The very nature of the B-Party warrant is that the subject of the warrant is likely to be an innocent party who may never be informed of an interception. The lack of such knowledge greatly reduces the effectiveness of the remedy. The point was made during the course of the Senate Committee hearings, in the context of a discussion of the possibility of seeking a review by the Ombudsman or the Inspector-General of Intelligence and Security ('IGIS') of an interception. In its Report, the Senate Committee said:

It is theoretically open to any person adversely affected by the B-party warrant provisions to notify the Ombudsman, in the case of an agency, or the IGIS in the case of an ASIO warrant. However, the nature of the provisions and the covert nature of the surveillance makes it most unlikely if not impossible for such notification to occur. As the Committee Chair noted in the public hearing:

I am not entirely persuaded that one can complain to the Ombudsman or the IGIS about a telephone intercept that one does not know about.¹¹⁵

These comments are equally applicable to the likelihood of seeking a civil remedy.

¹¹⁵ Senate Legal and Constitutional Legislation Committee, above n 8, para 4.101.

+61 2 61253971

The First Workshop on the Social Implications of National Security

As Senator Stott Despoja said during the Senate Debate:

Similar to stored communication warrants, we believe the ability of an aggrieved person affected by a B-party warrant to access civil remedies under the Telecommunications Act is ineffective. Where a person has their communications unlawfully invaded or where material used from that interception is unlawfully recorded, they have no ability to seek redress because they will be completely unaware that the warrant has been exercised.¹¹⁶

In 1994, a review by Pat Barrett into the long term cost effectiveness of telecommunications interception recommended that 'agencies should be required to notify any innocent person whose telephone service has been intercepted of the fact of interception within a period of 90 days of cessation of the interception.'¹¹⁷ As Barrett noted, there are notification mechanisms in the United States and Canada. Barrett's recommendation was not implemented by the government, but was raised again in a number of submissions to the Senate Committee.¹¹⁸ Following the Democrats' unsuccessful attempt to introduce an amendment in the Senate, which would have required notification of a warrant in the case of stored communications warrants and B-Party warrants, the following exchange took place between Senator Ellison and Senator Stott Despoja as to the operation of the civil remedy provisions:

Senator Ellison: ... If there was a warrant executed which involved a B party and nothing was ever done in relation to the information concerning the B party, where would the harm be to the B party? You would have harm only if there were some action taken or they were prejudiced in some fashion. There would be a possibility of that occurring if you were to have proceedings in a court and that was all brought out. But, otherwise, it would never be acted upon. It could remain something which was of no consequence. ...¹¹⁹

Senator Stott Despoja: I am not talking about harm. The bill provides for civil remedies if there is an aggrieved person. I am wondering how that person finds out that they are aggrieved or that some harm has been done to them. What I am tackling in this amendment is the issue of notification

¹¹⁶ Commonwealth of Australia, *Parliamentary Debates*, Senate, 28 March 2006, 87-88. The Senator had earlier said that she thought it 'a little amusing that the government has included in the bill a section for civil remedies when the entire operation of the warrant is covert': at 86.

¹¹⁷ Pat Barrett, *Review of the Long Term Cost Effectiveness of Telecommunications Interception* (1994) Rec 7, para 4.32.

¹¹⁸ Electronic Frontiers Australia, above n 17, para 94; Australian Privacy Foundation, above n 26, para 18.

¹¹⁹ Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 March 2006, 18.

+61 2 61253971

that a warrant has been issued. ...¹²⁰

Senator Ellison: Under our law, any action has to be based on a case which demonstrates some disadvantage or harm. If a person never knows that they have been discriminated against – and this is across the board – they cannot bring the action.¹²¹

Senator Ellison's response that knowledge of harm is necessary for an action to be brought is self-evident, but it really misses the point. The TIA creates a civil remedy in circumstances where there has been an interception or access, or subsequent communication, in contravention of the statutory prohibitions. It is not a question of what harm may result once the information is publicly revealed as the Senator seemed to suggest. The relevant harm giving rise to the statutory claim is the unlawful interception or access or subsequent communication. If an aggrieved party is unaware of the circumstances giving rise to the remedy, then it is an ineffective one. The responses by Senator Ellison suggest either that, in the condensed period for debate, the Senator misunderstood the nature of the civil remedy provisions under the Act, or that the importance of maintaining the covert nature of the warrant process for security and law enforcement purposes outweighs the provision of an effective remedy to an aggrieved person. The second explanation is more likely. As the Senator said in one of his replies to Senator Stott Despoja, '[t]he fact is that if you notify people that you have a warrant against them you will destroy the whole regime this legislation is creating'.¹²²

4.6 Enhancing security and law enforcement tools but leaving privacy protection behind

The 2006 amendments were described by the Attorney-General as 'enhanc[ing] interception powers and privacy protections'.¹²³ The changes, it was said, were designed to keep pace with technological change and 'ensure law enforcement and security have the investigative tools to continue to fight against serious crime and terrorist activity'.¹²⁴ While the amendments do enhance interception powers, they do not, to any significant degree, enhance privacy protections.

On the contrary, as the discussion in Part 2 demonstrates, at every point that a policy choice was to be made between security and law enforcement, on the one hand, and privacy, on the other, the government chose to sacrifice privacy interests. When introducing device warrants, it was recognised that technology would need to

¹²⁰ Ibid.

¹²¹ Ibid 19. The debate continued in similar terms over three pages of the Senate Hansard: at 18–20.

¹²² Commonwealth of Australia, *Parliamentary Debates, Senate*, 30 March 2006, 20.

¹²³ The Hon Philip Ruddock MP, *Enhanced Interception Powers and Privacy Protections*, (Press Release, 30 March 2006)

¹²⁴ Ibid.

+61 2 61253971

be developed before it confidently could be said that privacy interests of non-suspects would not be affected. Nevertheless, it was accepted by the Senate Committee that operational requirements of law enforcement and security warranted the amendment. The B-Party amendments were recognised during the Senate Committee process as impacting significantly on the privacy interests of innocent third parties. Opposition and Democrat amendments designed to limit the extent of the privacy intrusions were not accepted by the government. The broader stored communications scheme with relaxed thresholds was justified on a contested distinction between real-time and stored communications. Opposition and Democrat amendments designed to restore parity of privacy protection were not supported by the government. The relaxed reporting requirements in relation to stored communications were defended by the government from amendment on the basis that more detailed reporting would have an 'operational impact' on law enforcement objectives. The concern expressed by the Ombudsman about the capacity of his office to inspect and report under the stored communications scheme within the prescribed period was not seen as a 'compelling reason' to extend those periods.

On the face of the amendments, the only significant measure designed to enhance privacy was the removal of the distinction between Class 1 and Class 2 offences and, consequently, the requirement that authorities issuing Part 2.5 warrants take account of privacy interests in all cases. However, as the Blunn Report recognised, where law enforcement needs are shown, privacy considerations are unlikely to preclude the issue of a warrant for any of the offences previously described as Class 1. Thus, in operation, the amendment is likely to have a minimal impact on privacy protection.

The government consistently maintained that the Blunn Report and Senate Committee recommendations would be the subject of ongoing consideration to ensure that the regime 'continues to achieve an appropriate balance between privacy and appropriate access for investigation of serious criminal conduct'.¹²⁵ The 2006 amendments, however, reinforce our previously stated concern that the regulatory landscape has changed to such an extent that 'there is no longer a position that resembles a "balance"'.¹²⁶ Even if the 'balancing' metaphor is adopted, there would need to be substantial amendments to the legislative scheme to take account, at the very least, of the privacy concerns set out by the Senate Committee.

5 Concluding observations

The TIA Act was originally designed to protect wire-based national telecommunications infrastructure from unauthorised interception and to ensure

¹²⁵ Ibid.

¹²⁶ S Bronitt and J Strellios, above n 42, 887

+61 2 61253971

The First Workshop on the Social Implications of National Security

access for national security and law enforcement purposes. However, the legislative assumptions and regulatory context have significantly changed since its original enactment. Changes in technology and patterns of criminal activity, and the increased attention on national security, have all placed pressure on government to provide enhanced legislative tools for national security and law enforcement. When these pressures are combined with the reduced judicial involvement in the warrant process and the largely illusory operation of the civil remedy provisions, the impact on privacy has been substantial.

These privacy implications are not merely the product of academic interest. Many of the fundamental privacy concerns were clearly expressed in the Blunn Report and the bipartisan report of the Senate Committee. The government has committed to reviewing their recommendations as part of an ongoing review of the legislation. We would renew our 'call for legislative reform that places rights protection at the centre of regulatory design',¹²⁷ but the implementation of the Senate Committee recommendations would be a useful start.

¹²⁷ Ibid 888.