Prometheus, Vol. 24, No. 4, December 2006

Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?[1]

SIMON BRONITT & JAMES STELLIOS

Abstract *This article reviews the expansion of federal telecommunications interception powers, focusing on the watershed reforms enacted in 2006. The new statutory frameworks governing interception of 'live' and 'stored communications' are compared and contrasted, with a particular focus on their impact on human rights such as privacy and the fair trial. The article identifies significant regulatory loopholes and deficiencies in this new system, casting doubt on the usefulness of adopting a 'balancing' model to guide either macro-level policy development or micro-level decision-making relating to individual warrants.*

Keywords: telecommunications interception and access; wiretapping; electronic surveillance; access to stored communications; federal and State law enforcement powers; law reform; human rights relating to privacy and the fair trial.

Introduction

In 2006, the federal Parliament amended the legislative scheme for the regulation of telecommunications interception and access in Australia. This is the most significant overhaul and expansion of these surveillance powers since the current regime was established by the *Telecommunications (Interception) Act 1979* (Cth) ('TI Act'). The changes were introduced to implement recommendations from a review by Anthony Blunn ('Blunn Report') in 2005.[2]

Prior to the 2006 amendments, the TI Act regulated the interception of communications passing over a telecommunications system, establishing broad prohibitions on interception and subsequent use of intercepted communications, with a range of limited exceptions where interception was permissible, for example, under a warrant for security and law enforcement purposes. While the original intention of the TI Act may have been to protect the integrity of the national telecommunications infrastructure, that intention has since been eclipsed by the

Prometheus ISSN 0810-9028 print/ISSN 1470-1030 online © 2006 Taylor & Francis
http://www.tandf.co.uk/journals
DOI: 10.1080/08109020601030001

rhetorical appeal to the idea that the legislation provides an important vehicle for the protection of privacy for those using the telecommunications system. Thus, the legislative scheme, as currently conceived, embodies a tension between the protection of privacy interests—as reflected in the overarching prohibition—and the national security and law enforcement objectives—as reflected in the exceptions. Accordingly, reforms which have expanded the legislative scheme have been seen as an exercise in 'balancing' the interests of privacy against 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 *Telecommunications (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 superficially similar to those under the original interception provisions in the TI Act, the scope of the TIA 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 who are likely to communicate with individuals involved with the serious offence under investigation).

This article will show that the 2006 amendments have fundamentally altered the legislative scheme. While previous amendments have resulted in incremental function creep favouring an expansion in interception powers for law enforcement and national security purposes, the 2006 amendments have resulted in a sea-change in regulatory design. The article will then demonstrate that the current 'balancing' approach, which has guided law reform as well as individual decisions to authorise interception, tends to suppress or marginalise privacy and fair trial interests in favour of providing government agencies with wide surveillance powers for the purposes of national security and law enforcement.

Telecommunications Interception: A History of Normalisation

Law reform in the telecommunications field is hardly unusual. The adage that technology outstrips law is true, explaining the almost constant pattern of revision of the TI Act since 1979. The scope of the warrant scheme has expanded significantly over time. Prior to the TI Act, the *Telephonic Communications (Interception) Act 1960* (Cth) criminally prohibited the interception of telephonic communications subject only to limited exceptions where a warrant had been granted 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 beyond drug offences, most recently to include terrorism offences in 2002. Although numerically small, interception powers have been critical in several recent investigations and prosecutions for terrorism.[3]

This tendency to 'function creep' and 'normalisation of extraordinary powers' has been long recognised in the literature in this field.[4] From its inception as primarily an investigative tool for federal drug offences, the powers have evolved into a national surveillance scheme for serious crime whether federal or State. Indeed, the bulk of interception activity now relates to State offences. The 2006 amendments continue this expansion of authorised interception with the introduction of device warrants and B-Party warrants.

However, even more significantly, the 2006 amendments go beyond function creep: the amendments are a watershed in the history of interception law in Australia, heralding a major conceptual shift albeit under the guise of technical improvement. Under these reforms, the scheme moved beyond 'live' interception to include access to stored data. In simple terms, a warrant scheme originally devised to permit interception of communications has been extended into a power to search and seize stored communication data. The question arising is whether this new form of covert search warrant justifies a different regulatory scheme. As we explore below, there is a contestable policy assumption that the access to stored communications does not require the same regulatory approach as interception, with the TIA Act containing both loopholes that permit so-called 'overt access' to stored communications, and a more permissive approach to the use and purposes for which warrants are granted.

The Legal Framework Governing Telecommunications Interception

The warrant system

The TI Act sets out a number of exceptions to the prohibition on interception, most significantly legalising interceptions done 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.[5] Part 2.5 warrants may be issued by federal judges and Administrative Appeal Tribunal (AAT) members to federal[6] and State law enforcement agencies to intercept telecommunications made in connection with the investigation of specified federal and State offences. State agencies[7] may apply for Part 2.5 warrants where they have been declared to be eligible by the federal Attorney-General. 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 latest Annual Report by the Attorney-General to Parliament on the operation of the TI Act reveals that two-thirds of Part 2.5 warrants were issued to State rather than federal agencies, leading to the conclusion that this is primarily a national rather than federal law enforcement activity.[8]

While the prohibition on the interception of communications and subsequent use of the intercepted information (which is subject to exceptions including a warrant authorising interception) appears prima facie prohibitory and limiting, the system poses few real constraints on the use of these powers. It should also be noted that there have been no prosecutions for illegal interception and use of material (whether by law enforcement agencies or others). It would be optimistic and naïve to think that all interception activity in Australia occurs within the warrant system.[9]

The 2006 amendments have changed the legislative scheme in at least three significant ways. First, the legislation now allows security and law enforcement agencies to seek device specific warrants. Secondly, security and law enforcement officers also have access to B-Party warrants. Thirdly, there is a new regime for the regulation of access to stored communications. The first two of these changes will

be considered in this section of the paper. The third change will be considered in the next section.

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.[10] Service warrants are issued in relation to a particular 'telecommunications service' where the intercepted information is likely to assist in connection with the investigation of a serious offence in which the particular person is involved. Interception is based not upon reasonable suspicion that the person has committed or will commit serious offences, but rather the statutory threshold is satisfied by mere *involvement* in those offences—a broader category where the subject is typically described as a 'person of interest'. Where a person of interest is using more than one telecommunications service, there is provision for the issue of a named person warrant, which authorises the interception of multiple telecommunications services in relation to a particular person of interest.

Device warrants

The recent amendments in 2006 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'—e.g. 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'.[11]

There has been some controversy as to whether communications technology has developed to a point which would allow devices to be identified with sufficient precision, with concern expressed over the potential impact upon the privacy of innocent persons where the device identification cannot be determined with such precision.[12] The Blunn Report, giving rise to the 2006 amendments, 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'.[13] 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'.[14] Likewise, the Senate Committee reviewing the Bill during its passage through Parliament was not entirely convinced that 'the device being targeted under the warrant was able to be certified as uniquely identifiable'.[15] 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 identity of the source of telecommunications would take some time,[16] and operational needs, it would seem, justified any potential impact on the privacy of innocent parties.

B-party warrants

Warrants under Part 2.2 and Part 2.5 are now available not only in relation to a person of interest but, following the 2006 amendments, also in relation to a person who is entirely innocent of any involvement in criminal activity. This so-called 'B-Party' is someone who uses a telecommunications service to communicate with a person of interest. There must be a connection between the use of the innocent third party's telecommunications service and the security or law enforcement objective, but the B-Party thresholds in the TIA are low: warrants may be issued where it is 'likely' that monitoring the communication of a B-Party or services used by third parties will intercept communication by a person of interest, which in turn is one which is 'likely' to assist in an investigation or security intelligence-gathering.[17]

The circumstances that trigger the issue of a B-Party warrant are broad, and once the warrant has been issued under either Part 2.2 or Part 2.5 of the TIA Act 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 intercepted communication, 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 might be the suspected person's medical practitioner or religious leader, and the intercepted communication might include communication by the medical practitioner with other patients or by the religious leader with other members of the religious community.

An obligation to minimise privacy intrusions in B-Party warrants would undoubtedly place a regulatory burden on security and law enforcement agencies. However, in cases where the surveillance does not relate to a person who is suspected of a crime, from a human rights perspective, any intrusion into privacy should be demonstrably necessary and proportionate. A minimisation scheme similar to the one used under the US federal wiretapping law would have been one model that could address these human rights concerns.[18]

The significant potential for privacy intrusion under B-Party warrants attracted considerable attention in the Blunn Report and during the Senate Committee review of the amendments. Blunn had recognised that the legislation as it stood before the amendments might be wide enough to authorise B-Party warrants, and recommended that the legislation be amended to make it clear that they could only be used in controlled circumstances to protect privacy and avoid 'fishing expeditions'. The Senate Committee recognised the need for security and law enforcement officers to have access to B-Party warrants, but was concerned about the potential privacy invasion. As a result, the Committee recommended various amendments to confine the scope of B-Party warrants, including that there should be stricter supervision of destruction of non-material content; and that certain communications be exempted from B-Party warrants (e.g. 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).[19] The Committee also recommended more detailed parliamentary reporting requirements. Of these

recommendations, only the enhanced reporting requirements were adopted by the government in its Senate amendments.

The Legal Framework Governing Access to Stored Communications

The 2006 amendments introduced provisions for the protection of stored communications. The introduction of these provisions followed a protracted attempt by the government in 2002 and 2004 to amend the TI Act to deal with stored communications. Following continuing disagreement between the Attorney-General's Department and the Australian Federal Police (AFP) on the proper scope of the powers under the Act, the Senate Legal and Constitutional Legislation Committee recommended in 2004 an independent review of the position, and that the status quo be maintained until that review was undertaken.[20]

The Blunn Report 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 procedures, and the storage and disposal processes.[21] Blunn recommended that a warrant scheme should be enacted with similar elements to those existing for interceptions, including access by warrant issued by independent issuing authorities.[22] Importantly, Blunn was of the view that the 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.[23]

Purporting to implement these Blunn recommendations, s 108 of the TIA Act prohibits the accessing of stored communications without the knowledge of either the intended recipient or the sender of the communication. 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.[24] 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. so-called 'overt access', which is discussed below) 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).[25]

Stored communications warrants

There is a range of exceptions to the criminal prohibition on accessing stored communications, primarily relating to access under an interception warrant[26] or a stored communications warrant.[27] 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.[28] As the Explanatory 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.[29]

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 that the information likely to be obtained by accessing the stored communication 'would be likely to assist in connection with the investigation by the agency of a serious contravention in which the person is involved'.[30]

Curiously, despite what might be a more significant impact on privacy when compared to interception of live communications, stored communications warrants are issued by a wider range of issuing authorities; they are available to a broader group of agencies (not only do they include law enforcement agencies, but they also include agencies that enforce pecuniary penalties or administer revenue laws like the Australian Taxation Office, Australian Securities and Investments Commission and Australian Customs Service) and they are available in relation to a lesser range of offences and civil penalties. 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 equivalent stored communications provisions. Additionally, reporting requirements for stored communication warrants are less stringent.

The broadening of the stored communications access regime and the relaxation of various thresholds in relation to stored communications warrants 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. 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'.[31] However, there are at least three difficulties with this distinction. First, 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. Secondly, the assumption that stored communication is more 'considered' does not hold as a general rule: a point which generated discussion during the Senate Committee process and was further developed in the Senate debate on the Bill.[32] The opposition to such a distinction was well illustrated by Senator Stott Despoja's comments during the course of the Bill through Parliament: '[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, in this day and age, is ridiculous'.[33]

Thirdly, in any event, even if one were to accept the 'spontaneous/considered' communication 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.[34] Clearly, as the Blunn Report concluded, the mode of expression does not alter the reasonable expectation of privacy in respect of such personal communications.[35] 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 pertinent distinction in this context is between covert and overt searches, and the guiding test should be the impact on individual privacy.[36] Given the significant impact of covert access on privacy, and considering that the wider group of enforcement agencies had access to covert access methods, the Committee recommended that: (i) enforcement agencies able to access stored communications should be limited to those eligible under the interception provisions;[37] (ii) states enact complementary legislation as a precondition to being entitled to apply for a warrant;[38] (iii) warrants be limited to criminal offences;[39] and (iv) issuing authorities be limited to those under the interception provisions.[40]

The government did not seek to implement these recommendations, and did not support 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 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.[41]

However, given the discussion above, if a transmitted communication is *different in nature* to a communication whilst in transmission so as to justify the relaxation of safeguards in relation to the former, that rationale is yet to be provided.[42]

'Overt access' to stored communications: a regulatory loophole

The TIA provisions governing stored communications contain similar prohibitions and reporting requirements as those contained in the interception provisions, although with important differences. A key difference is that the TIA prohibits only accessing stored communication *without the knowledge of either the intended recipient or the sender of the communication.*[43] It is sufficient to have knowledge for these purposes if a written notice has been given to the person.[44] This 'knowledge' exclusion seeks to preserve so-called 'overt access', though it should be noted this is based only on notification to one party (rather than all parties, including both senders and recipients) to that stored communication.[45] Thus, for example, notification to *any* recipient of a communication will relieve officials from the legal obligation to seek a warrant in relation to accessing that stored communication. Under these circumstances, the privacy interests of senders and recipients need not be subject to further consideration, and the actions of the law enforcement officials are not subject to independent review. It is conceivable that this aspect of the new law permitting access to stored communications where one party is notified will operate as a regulatory 'loophole'.

In the United States, a similar practice permitted under the federal wiretap legislation is known as 'consensual monitoring', and stands outside the warrant

scheme.[46] A similar feature in the Australian law governing surveillance devices permits 'participant monitoring' in some jurisdictions, though this form of warrantless surveillance has attracted significant criticism from both academics and the New South Wales Law Reform Commission.[47] From a privacy standpoint, this type of law enforcement conduct is problematic: it is doubtful whether notification to one party modifies the other party's reasonable expectation of privacy in their communications. Moreover, there is also a fundamental conceptual question as to whether mere knowledge that a stored communication is being accessed should be construed as a meaningful consent, express or implied, to that access.

Balanced Public Policy or Balancing Away Privacy Interests?

The various developments since the enactment of the TI Act have placed considerable pressure on privacy in a way not initially contemplated. The regulatory landscape has shifted to such an extent that there is no longer a position that resembles a 'balance' between competing interests of law enforcement and privacy rights. In earlier work we have called for legislative reform that places rights protection—which extends beyond privacy to include fair trial rights—at the centre of regulatory design.[48] The response to such calls initially 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'.[49] 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'.[50] However, 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'.

There is a growing recognition that a balancing approach in the context of law enforcement is problematic, both at the *macro-level* of the law reform or at the *micro-level* of weighing of interests in judicial decisions (whether to grant warrants or to exclude improperly obtained evidence).[51] Although a persistent idea in all areas of policy development, balancing models rarely achieve an accommodation or equilibrium between competing interests. In other contexts, criminal justice scholarship has pointed out that 'balancing' tends to prioritise the interests of crime control over due process.[52] The New South Wales Law Reform Commission had initially taken the balancing approach in its consideration of privacy issues in relation to surveillance laws, arguing that privacy interests must be weighed against legitimate societal interests in preventing and prosecuting crime.[53] It subsequently revised that approach following further research, concluding that the balancing approach was 'inherently flawed'.[54]

Macro-Level Balancing: An Unbalanced Approach to Law Reform?

In the context of the 2006 reforms, it seems that at each turn privacy interests were balanced away in favour of security and law enforcement—whether it was the adoption of device warrants notwithstanding technological difficulties of precise identification, the creation of B-Party warrants with their profound implications for innocent third parties, or the lowering rather than raising of the thresholds for issuing and reporting stored communications warrants. At every moment where a

balance had to be struck through the legislative process, the end result was that interests of security or law enforcement outweighed privacy interests. Structured as a binary equilibrium between privacy and the needs of national security and crime control, the reform process overlooked other significant due process considerations at stake such as the fair trial. In this context, a fundamental rule of law (and attribute of the right to a fair trial), namely lawyer–client privilege, seemed to play no role in limiting the scope of interception or access warrants.[55]

The case for reform underlying the TIA Act was most vigorously scrutinised by the Senate Committee. During the Bill's passage through Parliament, the Committee displayed impressive comprehension of the legislative scheme and the issues arising from the proposed amendments despite the significantly condensed period for consideration. Adopting the balancing approach itself, the Committee produced a bi-partisan 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. The Democrat's Supplementary Report dissented only in the sense that it sought further privacy protection within the legislative scheme. Unsurprisingly, in the current climate, the Committee's concerns were addressed only in a limited way. The only privacy enhancing recommendation accepted by the government was to strengthen the reporting requirements for B-Party warrant statistics.[56] Both 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 of the Senate Committee!

At the macro-level, the problem with the balancing approach is that the interests in competition are not commensurable—a key fallacy is that enhancing privacy protection or due process values *necessarily* impedes law enforcement. As Lucia Zedner points out:

> Typically, conflicting interests are said to be 'balanced' as if there were a self-evident weighting of or priority among them. Yet rarely are the particular interests spelt out, priorities made explicitly, or the process by which a weight is achieved made clear. Balancing is presented as a zero-sum game in which more of one necessarily means less of the other … Although beloved of constitutional lawyers and political theorists, the experience of criminal justice is that balancing is a politically dangerous metaphor unless careful regard is given to what is at stake.[57]

In the face of an empirical vacuum in relation to these questions of (in)effectiveness, significant reform must be resisted—expansion of police powers must be evidence-based and incursions into rights like privacy must be necessary and proportionate. Fundamental fair trial rights like the right to legal counsel (upon which the lawyer–client privilege rests) must not be overlooked.

Most importantly, the recent experience of reform leading to the TIA Act demonstrates the inadequacy of our system of parliamentary democracy for considered public policy development—politicians and indeed governments will often be held hostage to an 'uncivil politics of law and order'[58] in which standing up for liberal principles against reforms which law enforcement claim are essential is untenable. Clearly, such matters should be referred to an independent law reform

commission—indeed, this federal Act clearly falls within the purview of the Australian Law Reform Commission (ALRC). The ALRC is much better placed than Parliament to conduct independent research, and to rigorously test competing interests and rights at stake.[59] Only through such a process can legislation be devised that would maximise privacy and due process protection *and* ensure that the powers of investigation are both necessary and proportionate.

Micro-Level Balancing: Warrants—Judicial Safeguard or Rubber Stamp?

The warrant system in Australia is often presented as an important safeguard for the protection of privacy interests. Prior to the recent 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 taken into account in the warrant process only in relation to 'Class 1' offences. We had previously observed this approach 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 arguments that the privacy interests become of greater rather than of lesser significance.[60] Recognising the need for privacy interests to be considered in all warrant applications, the 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 reviewing the Bill.[61]

Thus, following the recent amendment, privacy protection appears to be enhanced: it is now a factor to be taken into account in the issuing of *all* Part 2.5 interception warrants and stored communications warrants. Furthermore, although not a factor expressly to be taken into account by an issuing authority in relation to Part 2.2 warrants, arguably the legislative scheme does not expressly prevent consideration of privacy considerations.

There are, however, some problems with seeing the warrant system as providing an effective bulwark against arbitrary intrusion into privacy. First, as the Blunn Report recognised, rarely if ever would privacy concerns outweigh law enforcement or security objectives.[62] This observation is supported by the experience with Part 2.5 warrants. The statistics clearly show that a negligible percentage of applications are refused or withdrawn.[63] This is especially the case since the issuing process is *ex parte*—no-one represents the interest of the persons subject to surveillance. Privacy concerns are magnified in relation to B-Party warrants where the persons targeted may not be involved in any respect with criminal behaviour. Although issuing authorities might place limitations on warrants so as to protect privacy of such innocent persons, there does not seem to be a significant practice of imposing warrant conditions, and it is impossible to tell whether those conditions are motivated by privacy concerns.

There are mechanisms which could be incorporated into the current legislative scheme which would allow for a stronger recognition of privacy interests. In the State of Queensland, a Public Interest Monitor (PIM) has the role of appearing at the hearing of applications for surveillance device warrants to examine witnesses and make submissions on the appropriateness of granting the application.[64]

During the course of the Senate debate, the Democrats suggested that a PIM, based upon the Queensland model, be incorporated. However, no amendment to introduce a PIM was pressed. The Commonwealth Attorney-General recently suggested that the use of the PIM in Queensland warrant hearings would be inconsistent with the national regime and thus would be unacceptable to the Commonwealth.[65]

A second reason for not placing too much reliance on the warrant system is the increasing marginalisation of the role of judicial officers. Judicial involvement in the warrant process is often presented as an essential oversight function. However, as noted above, there is no judicial involvement in the issuing of Part 2.2 warrants for national security purposes. Even in relation to Part 2.5 warrants, judicial involvement is increasingly limited. This is partly for constitutional reasons, as the issuance of a warrant is seen as an exercise of executive power which cannot be exercised by a federal court. Judges can however consent to exercising the power in their personal capacity provided that the function does not undermine the integrity of the judiciary.[66] 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.[67] Consequently, Parliament amended the TI Act to allow members of the AAT to issue warrants. The most recent statistics show that AAT members represent 37% of the issuing authorities.[68]

Further diminishing the judicial role in the warrant process is the fact that law enforcement agencies are seeking warrants primarily from AAT members. Despite representing 37% of the available issuing authorities in the 2004/5 period, AAT members issued 93% of the warrants issued.[69] The increased use of AAT members to issue warrants was noted by the NSW Council of Civil Liberties to the Senate Committee.[70] Although the Committee was careful not to make any negative 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'.[71] 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'.[72]

Conclusion

The Attorney-General has described the 2006 amendments as 'enhanc[ing] interception powers and privacy protections'.[73] The reforms, 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'.[74] While the reforms do enhance interception powers, we believe that these measures do not, to any *significant* degree, enhance privacy protections.

On the contrary, 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 subordinate privacy interests. The advent of device and B-Party warrants constitutes a significant threat to the privacy of innocent persons. They combine with a new scheme of access to stored communications that lowers the threshold for gaining access to those communications when compared with the interception of live communications. Preserving access to stored communications without warrant where one party has been notified is a significant regulatory

loophole with profound implications for privacy rights. On the face of the reforms, the only significant measure purporting to enhance privacy was the removal of the distinction between Class 1 and Class 2 offences and 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 practical terms, this change is likely to have a minimal impact on privacy protection.

The government maintained consistently that the Blunn Report and Senate Committee recommendations will 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'.[75] The 2006 reforms, however, reinforce our previous concern that the regulatory landscape has changed to such an extent that there is no longer a position that resembles a 'balance'.[76] More fundamentally, we question whether promoting this balance—both at the macro-level of policy development or micro-level of warrant authorisation—is an appropriate and effective principle to guide us in this field.

Notes and References

1. This article is adapted from the conference paper 'Regulating telecommunications interception and access: a sea-change in surveillance laws', in Michael and Michael (eds), *Social Implications of Information Security Measure on Citizens and Business*, University of Wollongong Press, 29 May 2006. This research forms part of a wider ARC funded project monitoring legal changes post-9/11 (DP 451473) 'Terrorism and the Non-State Actor after September 11: The Role of Law in the Search for Security'. The authors would like to thank Niamh Lenagh-Maguire for her excellent research and editorial assistance.
2. Anthony Blunn, *Report of the Review of the Regulation of Access to Communications*, 2005.
3. A recent review of the federal terrorism laws noted that TI warrants for terrorism-related offences had been issued more than 20 times since 2002, with one operation leading to the arrest of 19 terrorist suspects in NSW and Victoria: *Report of the Security Legislation Review Committee*, 2006. Available at: http://www.ag.gov.au/slrc.
4. S. Bronitt and J. Stellios, 'Telecommunications interception in Australia: recent trends and regulatory prospects', *Telecommunications Policy*, 29, 2005, p. 875.
5. *Telecommunications (Interception and Access) Act 1979* (Cth), Part 2.2.
6. Federal law enforcement agencies are the Australian Federal Police and the Australian Crimes Commission: see definition of 'Commonwealth agency', *Ibid.*, s 5.
7. The definition of 'eligible authority' in s 5 covers State police forces and other listed State crime and corruption agencies.
8. *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2005*, Table 1.
9. The Commonwealth Ombudsman plays an important oversight role in relation to TIA undertaking periodic compliance audit of interception records to ensure agency compliance with the Act. However, no system of audit is entirely fail-safe as revealed in the 1986 Stewart Royal Commission that incidentally uncovered widespread wiretapping by NSW police in flagrant breach of the requirements of federal law: see P. Grabosky, *Wayward Governance: Illegality and its Control in the Public Sector*, AIC, Canberra, 1989, p. 47.
10. See *Telecommunications (Interception and Access) Act 1979* (Cth), 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).
11. *Ibid.*, ss 9A(3) and 46A(3). The Second Reading Speech 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'.

12. See submissions of Electronic Frontiers Australia, noted in Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Bill 2006,* para. 4.118.
13. Blunn, *op. cit.*, para. 3.2.2.
14. *Ibid.*, para. 3.3.5.
15. Senate Legal and Constitutional Legislation Committee, *op. cit.*, para. 4.122.
16. *Ibid.*, para. 4.125.
17. *Telecommunication (Interception and Access) Act 1979* (Cth), s 9(1)(a)(ia) and (b) for national security purposes; s 46(1)(d)(ii) for law enforcement purposes.
18. 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'.
19. Senate Legal and Constitutional Legislation Committee, *op. cit.*, Recs 22–24.
20. See the Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment Bill 2004*, 2004a; Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*, 2004b.
21. Blunn, *op. cit.*, para. 1.8.1.
22. *Ibid.*, para. 1.6.1.
23. *Ibid.*, para. 1.6.3.
24. *Telecommunications (Interception and Access) Act 1979* (Cth), s 5(1).
25. *Supplementary Explanatory Memorandum, Telecommunications (Interception) Bill 2006* (Cth), s 2.
26. *Telecommunications (Interception and Access) Act 1979* (Cth), s 108(2)(b).
27. *Ibid.*, s 108(2)(a).
28. *Ibid.*, s 108(3).
29. *Explanatory Memorandum, Telecommunications (Interception) Bill 2006* (Cth), 10.
30. *Telecommunications (Interception and Access) Act 1979* (Cth), s 116.
31. Blunn, *op. cit.*, para. 1.4.2.
32. See, for example, Evidence to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 15 March 2006, Professor George Williams, pp. 28, 31.
33. Commonwealth of Australia, *Parliamentary Debates*, Senate, 28 March 2006, p. 85.
34. See Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, March 2006, New South Wales Council for Civil Liberties, p. 3; Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, March 2006, Australian Privacy Foundation.
35. Blunn, *op. cit.,* para. 1.6.3.
36. Senate Legal and Constitutional Legislation Committee, *op. cit.*, para. 3.39.
37. *Ibid.*, Rec. 2, para. 3.42.
38. *Ibid.*, Rec. 6, p. 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).
39. *Ibid.*, Rec. 3, para. 3.43.
40. *Ibid.*, Rec. 5, para. 3.60.
41. Commonwealth of Australia, *Parliamentary Debates*, Senate, 29 March 2006, p. 42.
42. 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.*, p. 43). 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 suggests that more stringent measures be put in place for stored communications warrants.

43. *Telecommunications (Interception and Access) Act 1979* (Cth), s 108. The amending provision originally referred only to the knowledge of the recipient, but was amended in the Senate following somewhat confused debate: Commonwealth of Australia, *Parliamentary Debates*, Senate, 29 March 2006, p. 86; 30 March 2006, p. 3.
44. *Telecommunications (Interception and Access) Act 1979* (Cth), s 108(1A).
45. See Commonwealth of Australia, *Parliamentary Debates*, Senate, 29 March 2006, p. 86.
46. The federal electronic surveillance statutes have been codified at 18 USC 2510. Section 2511(2)(c) of Title 18 provides that 'It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has give prior consent to such interception'. This practice has been held not to violate the Fourth Amendment: *United States v White*, 401 US 745 (1971).
47. New South Wales Law Reform Commission, *Surveillance: An Interim Report,* Report No. 98, 2001.
48. Bronitt and Stellios, 2005, *op. cit.*, p. 887.
49. Blunn, *op. cit.*, p. 5.
50. *Ibid.*, para. 7.
51. For a review of the law relating to undercover policing that critiques the balancing approach, see S. Bronitt, 'The law in undercover policing: a comparative study of entrapment and covert interviewing in Australia, Canada and Europe', *Common Law World Review*, 33, 1, 2004, p. 35.
52. A. Ashworth, 'Crime, community and creeping consequentialism', *Criminal Law Review*, 43, 1996, pp. 220–30; S. Bronitt, 'Electronic surveillance, human rights and criminal justice', *Australian Journal of Human Rights*, 3, 2, 1997, p. 183. For recent essays critiquing the deployment of the balancing approach in the context of special laws to advance the war on terror, see J. Waldron, 'Security and liberty: the image of balance', *The Journal of Political Philosophy*, 11, 2, 2003, p. 191; L. Zedner, 'Securing liberty in the face of terror: reflections from criminal justice', *Journal of Law and Society*, 43, 4, 1995, p. 507.
53. New South Wales Law Reform Commission, *op. cit.*
54. *Ibid.*, para. 2.4.
55. The legal issues surrounding this issue are discussed in Bronitt, 1997, *op. cit.*, pp. 201–3.
56. See Senate Legal and Constitutional Legislation Committee, *op. cit.*, 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, pp. 1–2.
57. Zedner, *op. cit.*, pp. 510–1.
58. The phrase 'uncivil politics of law and order' was used before 9/11 to describe the trend to drive criminal justice reform in Australia by reference to law and order commonsense rather than informed expert opinion or available data: R. Hogg and D. Brown, *Rethinking Law and Order*, Pluto Press, Annandale, 1998, Ch. 1.
59. Since finalising this article for publication, the ALRC has commenced wide-ranging review of privacy. In its Issues Paper (IP 31), *Review of Privacy* (September 2006) the ALRC poses the important question whether the *Telecommunications (Interception and Access) Act 1979 (Cth)* provides 'adequate and effective protection for the use, disclosure and storage of personal information'?
60. Bronitt and Stellios, 2005, *op. cit.*, p. 885.
61. Senate Legal and Constitutional Legislation Committee, *op. cit.*, para. 5.9.
62. Blunn, *op. cit.*, para. 6.4.
63. See *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2005*, Table 1. For the year ending 30 June 2005, only six of the 2,889 applications were refused or withdrawn.
64. *Queensland Police Powers and Responsibilities Act 1997* (Qld), s 159.
65. See The Hon Phillip Ruddock MP (Attorney-General), *Queensland Government Wrong on Interception Amendments*, Press Release, 17 July 2006. It should be noted, however, that this

opposition was not previously applied to the federal scheme for imposing control orders for the purpose of protecting the public from terrorist acts. Under the federal legislation, the PIM in Queensland is permitted to make submissions to the issuing court where the person subject to the order is a Queensland resident or the issuing court is located in Queensland: *Criminal Code 1995* (Cth), s 104.14.

66. *Grollo v Commissioner of Australian Federal Police* (1995) 184 CLR 348.
67. See *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004*, para. 4.45.
68. *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2005,* Table 28. 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.
69. *Ibid.*, Table 29.
70. See Senate Legal and Constitutional Legislation Committee, *op. cit.*, para. 3.55.
71. See *Ibid.* Rec. 25, para. 4.112. This recommendation was supported by The Democrats' Supplementary Report.
72. Commonwealth of Australia, *Parliamentary Debates*, Senate, 30 March 2006, p. 37.
73. The Hon Philip Ruddock MP, *Enhanced Interception Powers and Privacy Protections*, Press Release, 30 March 2006.
74. *Ibid.*
75. *Ibid.*
76. Bronitt and Stellios, 2005, *op. cit.*, p. 887.