Submission No 133

Inquiry into potential reforms of National Security Legislation

Organisation: New South Wales Young Lawyers

Table of Contents

1. Preface

New South Wales Young Lawyers is a division of the Law Society of New South Wales. Members include law students, solicitors and barristers in their first 5 years of practice and/or under the age of 36. There are currently over 13,000 members.

The NSW Young Lawyers Public Law and Government Committee (**the Committee**) is responsible for providing a platform under which our members can discuss issues relevant to work in or with government departments, matters of constitutional and administrative law, and matters of public interest law. The Committee has a keen interest in the role of government in providing a framework that facilitates effective law enforcement. Equally, the Committee takes an interest in any law that might otherwise abrogate expectations of privacy, security and accountability that members of the public ought to expect from their public service.

The inquiry seeks to move forward a number of proposals that significantly expand already substantial powers held by intelligence services and law enforcement agencies along a number of aspects. The terms of reference are expansive and the limited time available to prepare a response has meant that the Committee has focused on Telecommunications Interceptions Warrants, Warrants under the ASIO Act, Cross-border/Agency cooperation, Data retention and evidentiary certificates.

2. Telecommunications Interception Warrants

The government asserts that there is an urgent requirement to overhaul the legislative framework in which these warrants are issued. The stated justification is that the technological landscape that underpins legislative assumptions has changed dramatically.

This description does not adequately evidence the amount of legislative time subsequently devoted to this act. Since its inception, the TIA Act has previously been amended by at least 64 other pieces of legislation, an average of almost twice per year. Changes to the warrants available under the TIA Act have been made in 2011[1] in 2010,[2] and in 2007, following from the Blunn Report.[3]

As noted in its 2011 report,[4] ASIO had direct input into the drafting process for the most recent amendments to this legislation, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011*. These warrants are also extensively used by state police forces and other government agencies, with a total of 3,495 requests for warrants having been made in the 2010-2011 year and only seven being refused or withdrawn.[5] Figures for (warrantless) authorisation to obtain access to telecommunications data are more extreme, with 243,631 requests made in the same period.

These particular amendments significantly expanded the scope law enforcement and intelligence agencies have to issue warrants in respect of telecommunications, introducing mechanisms such as controversial B-Party warrants[6]. No discussion has been provided on why these amendments have not been sufficient.

Currently four varieties of warrant are available under the TIA Act. In terms of accountability of intelligence agencies and judicial oversight, there are potential gains to be had in homogenising the thresholds for obtaining these warrants, as well as the time frames in which they must be issued. The ALRC has previously commented that there are a number of aspects of the Act which are problematic. These range from absent

---

[1] *Cybercrime Legislation Amendment Bill 2011* (Cth).
[2] *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 Number 2* (Cth).
[3] A Blunn, *Report of the Review of the Regulation of Access to Communications (2005) Australian Government Attorney-General's Department*.
[4] Report to Parliament, *ASIO for 2010-2011* (2011) 101.
[5] Report to Parliament, *Telecommunications (Interception and Access) Act 1979 for 2010-2011* (2011) 18.
[6] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and* Practice, Report No 108 (2008) 73.61 – 73.64.

definitions, to absent prescriptions in respect of privacy and regulatory oversight.[7] Additionally, in terms of retention of data, the ALRC previously recommended that s 79 of the *Telecommunications Interception and Access Act 1979* (Cth) be amended to provide that any record, including copies, gathered through interception be destroyed when no longer needed,[8] citing data security concerns.

[7] Ibid, 73.45.
[8] Ibid, 73.85.

3. Special Powers under the ASIO Act

The Discussion Paper outlines a number of proposals to 'modernise and streamline' ASIO's warrant provisions, contained in Division 2 of Part 3 of the ASIO Act. These proposals pose a range of questions and concerns, in particular regarding their breadth, impact on innocent third parties and accountability measures. Our key concerns are as follows:

References to 'computer' in section 25, (page 41)

The proposal to broaden the definition of 'a computer' in respect of computer access warrants poses a significant and disproportionate risk to the rights, in particular to the privacy, of innocent third parties. Extending the definition of computer to include computers on a premises or on a network would enable a single warrant to encompass a potentially large number of devices, many of which may have little or no substantial connection to the subject of the investigation. This over-reach could foreseeably occur in a variety of everyday circumstances, including where a subject is in shared accommodation, linked to a broader Wi-Fi network, or has a computer connected to a professional network such as in corporations or universities.

Such concerns were previously raised in relation to the initial introduction of B-Party warrants some years ago, with Senator Ludwig noting "it is not only the B-Party but also the C, D E and F parties who may at some point end up talking to B and, therefore, being captured'. The result is that potentially not just one, but a great many non-suspects to be caught in the B-Party warrant process".[9]

The existing definition provides sufficient precision and clarity to ensure that accountability is maintained throughout the warrant issuing process and in the exercise of ASIO's powers whilst also providing ASIO with targeted investigative capabilities.

Variation of a warrant (page 41-42)

The proposal to create a process by which ASIO may seek the variation of a warrant leaves open many important questions. Without these questions being answered the proposal is unsupportable. Based on the information in the Discussion Paper a new warrant must be maintained when there is a significant change of circumstances. It is not explained what constitutes a 'significant' change. It can be taken, however, that in order to maintain accountability a significant change in circumstances ought to justify the review of the warrant that would be undertaken in the context of seeking a new warrant.

[9] Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006) [4.62].

The Discussion Paper says any amendment to enable warrant variation would maintain *'appropriate accountability'*, without explaining what accountability measures would be in place. The present requirement that ASIO seek a fresh warrant following a significant change in circumstances already provides an avenue of accountability. In order to maintain accountability and ensure that an existing warrant did not endure inappropriately following a significant change in circumstances, any variation of a warrant as proposed would call for a level of accountability whereby the entire basis of the warrant would be reviewed in light of present, past and altered circumstances. This level of accountability is achieved under the existing provisions.

Duration of a warrant (page 42)

We are concerned about the proposal to extend ASIO search warrants from 90 days to six months. 90 days is a considerable period of time for ASIO to undertake its search. The powers exercised under a search warrant are particularly intrusive invasions into the privacy of the subject and, in all likelihood, innocent third parties. The circumstances of the case may change in the 90 day period. It is entirely appropriate that search warrants are not extended beyond the 90 day period. At the end of the 90 days ASIO may still apply for a fresh warrant, thus maintaining an ongoing accountability measure and ensuring the currency of the warrant and its basis.

Renewal of warrants (page 42)

The process by which ASIO must seek a fresh warrant rather than merely renewing an existing warrant provides a key accountability mechanism, ensuring that ASIO exercises its powers in a timely and efficient manner, and that the basis on which the warrant was originally issued (including adherence to legal threshold supported by an intelligence case) continues to apply. Again, the Discussion Paper does not explain the oversight or accountability measures that would apply to a renewal scheme. The rights that may be infringed under the broad array of ASIO warrants are sufficiently important to call for a strong accountability measure, such as the existing need to re-apply for a warrant upon its expiration. The risk posed to rights by the secrecy and breadth of ASIO warrants deserves strong protection, regardless of the administrative inconvenience to ASIO in needing to re-establish their justification for the warrant.

Authority for acts necessary to execute a computer access warrant (page 48)

The government proposes to amend s 25A of the ASIO Act to remove the prohibition on ASIO *'doing anything that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer'* to the extent that such activities are necessary to execute the warrant. The protection afforded to individuals by the s 25A

prohibition is a significant one. The privacy rights of a person subject to a warrant are already being substantially interfered with. Enabling ASIO to affect the contents of a person's computer or their (or others') use of it presents a troubling further interference with the rights of that person. When considered in the context of other proposals, this proposed amendment could extend to the computers of innocent third parties, even on a large scale. The proportionality test does not present nearly high enough a standard to maintain accountability and necessity, or to counter-balance the risk posed by the removal of this important protection.

We see no reason to remove the prohibition. If the prohibition were to be removed it should be subject to a very high standard, and presented as a last resort mechanism with strict time and action restraints and oversight of the highest level.

Use of third party computers and communications in transit & incidental entry (page 50)

The proposals to enable the use of third party computers and enter third party premises pose similar issues. These proposals present substantial increases in the breadth of ASIO's powers with respect to innocent third parties. The proposal does not specify which third parties could be covered by such a power, whether there would be limits of proximity or otherwise in this respect. The proposal does not specify whether a warrant or any other kind of formal procedure would be necessary to enable ASIO to exercise the proposed powers. The proposal does not outline any threshold considerations before the third party premises or technology could be accessed. In short, the proposal describes increasing ASIO's powers to enter the premises, use the computers and intercept communications of innocent third parties with no warrant and no demonstrable oversight or applicable standards or thresholds.

This proposed increase in ASIO's powers ought to be viewed in light of other proposals which could see ASIO granted access to entire networks of computers, affect the contents of computers and hold search warrants for six months instead of 90 days. Together these proposals would greatly increase ASIO's capabilities to infringe the rights and privacy of innocent third parties, in a foreseeably far-reaching manner. The countervailing accountability mechanisms are not clear. Again, in its proposal, the government says that '*appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme*' without describing at all what such measures would consist of. The necessity for secrecy and the great breadth of ASIO's powers heightens the importance of oversight and accountability mechanisms. Until such mechanisms can be explained and debated, and it can be demonstrated that they

are sufficiently strong to counterbalance the risks these powers pose, the proposals ought not be adopted.

Authorisation Lists

It is suggested in the Discussion Paper that in order to overcome operational inefficiencies the Director-General could approve classes of people to execute a warrant. There are, no doubt, many potential reforms that would operate to improve the operational efficiencies of ASIO. Whilst improving efficiencies and the efficacy of ASIO is, at a general level, to be encouraged, often they will come at a cost elsewhere in society. The Joint Committee should ensure that shortcuts to achieving ASIO's objectives are carefully considered and properly justified.

This suggestion of "classes of people" to execute a warrant appears to The Committee to be an example of such a shortcut. There will be obvious accountability issues as well as a partial defeat of the basis for having an "approved officer" in the first place. Approving classes of officers would need to be justified as to why it necessary to depart from the existing framework and safeguards.

4. Intelligence Service Cross-border/Agency Cooperation

In addition to the legislative instruments specifically discussed in the terms of reference, and in this submission as per the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011,* Australia has acceded to the *Council of Europe Convention on Cybercrime*,[10] which provides an important framework for cross-border cooperation, both in respect of how Australian law enforcement and intelligence services may interact with overseas intelligence services, and with regard to how private enterprise may have to behave in interacting with such agencies.

In the UK, this convention has been the basis upon which the Home Office has issued a voluntary code of conduct under which telephone and internet service providers retain some data. The legislation enabling the Convention in the UK also provides that if the Secretary of State is unconvinced of the efficacy of such a voluntary program, then the Code may be made mandatory.[11] The code has not subsequently been made mandatory and requires only a small subset of data be kept for up to 12 months, principally consisting of subscriber information that would be necessary for billing.

A voluntary code may help to formalise the existing level of cooperation generally afforded by private enterprise to intelligence agencies in Australia, as well as providing customers with a better idea of what information is being retained by telecommunications and internet services providers and to what ends it may be furnished to government bodies.

[10] *Council of Europe Convention on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004).
[11] *Anti-Terrorism, Crime and Security Act 2001* (UK) Part 11.

5. Data Retention Schemes and Cooperation between Intelligence Services and Private Enterprise

Data retention is broached under clause 15c of the Terms of Reference and in further detail at page 25 of the Discussion Paper. While there appears to have been little mainstream media attention given to these proposals, the prospect of a data retention regime has attracted some criticism.[12]

The proposed regime would require Carriage and Carriage Service Provides (**C/CSPs**), such as internet service providers and, potentially, "cloud computing providers" (which may include social networking services, such as Facebook or Twitter), to maintain large amounts of data for up to two years. For this to be of any utility to law enforcement, it fundamentally must connect to a subscriber to any of these services and to assist in identifying a party.

The privacy and security implications of this are significant. In recent months, companies including Yahoo,[13] LinkedIn,[14] Twitter[15] and AAPT[16] have all experienced serious data breaches, where user account data or other personal information has been disclosed.

The AAPT data breach is of particular interest, not just because the target of the attacks was an Australian ISP, but because the attacks were purportedly undertaken in response to government's present stance in favour of data retention laws.[17] Maintaining an ISP or any other large, technically sophisticated service online is difficult enough. The purported benefits of retaining this data must be weighed against:

- The privacy costs to users of any service maintaining such records,
- The difficulties in enforcing the maintenance of any records for services that operate outside the Australian jurisdiction; and

---

[12] Mark Newton, *The Surveillance State Tunes In* (2012) New Matilda <http://newmatilda.com/node/12166> at 13 August 2012; Bernard Keane, *Government Unveils Huge Wishlist of New Surveillance Powers* (2012) Crikey <http://www.crikey.com.au/2012/07/10/government-unveils-huge-wishlist-of-new-surveillance-powers/> at 13 August 2012.

[13] Ellen Messmer, *Update: Yahoo's massive data breach includes Gmail, Hotmail, Comcast user names and passwords* (2012) Network World <https://www.networkworld.com/news/2012/071212-yahoo-breach-update-260855.html> at 13 August 2012.

[14] Jim Finkle, *LinkedIn suffers data breach* (2012) Reuters <http://www.reuters.com/article/2012/06/06/net-us-linkedin-breach-idUSBRE85511820120606> at 13 August 2012.

[15] Matthew Schwartz, *Twitter Downplays Breach That Exposed Passwords* (2012) Information Week <http://www.informationweek.com/news/security/attacks/240000060> at 13 August 2012.

[16] Hamish Barwick, *Melbourne IT launches investigation into AAPT data breach* (2012) Tech World <http://www.techworld.com.au/article/431931/melbourne_it_launches_investigation_into_aapt_data_breach/> at 13 August 2012.

[17] Hamish Barwick, *Anonymous releases some AAPT data* (2012) CIO <https://www.cio.com.au/article/432044/anonymous_releases_some_aapt_data_/> at 13 August 2012.

- Any complications that may arise where other parties obtain access to such records as may impact law enforcement or intelligence investigations.

The concerns previously noted in respect of the *Telecommunications (Interception and Access) Act* are applicable to this scheme. Long term storage of data for no demonstrable purpose is costly, insecure and ill advised without further detail, particularly as to oversight and security requirements.

More broadly, there are also issues of procedural fairness in relation to production of evidence held by third parties for criminal purposes. If a third party (for example, Facebook or Twitter) is subpoenaed to produce information under existing regimes, their interests in how the proceedings should be conducted are very different to the interests of the person or people whose data is being produced.

As in *Norwich Phramacal*[18] style proceedings, the main interest of the C/CSP is in mitigating legal costs and extricating themselves from any proceedings as early as possible. Elsewhere, it has been suggested that the eventual target ought to have the benefit of being able to make submissions or otherwise be involved in the matter.[19] Such issues may be exacerbated if the accused party does not have access to evidence to be used against them.

We strongly recommend against a mandatory data retention scheme without further specifications provided about the particular nature of data to be retained. As noted, a voluntary code has been effective in the UK and would potentially help to provide the public with a better understanding of the existing level of cooperation between private enterprises and intelligence services, in lieu of any reconsideration of what information is already provided by C/CSPs to government agencies.

[18] *Norwich Pharmacal Co. & Others v Customs and Excise Commissioners* [1974] AC 133.
[19] Kimberlee Weatherall, "A Very Dynamic Issue: International Developments in Privacy in the Last 12 Months", ANU Public Law Weekend, Canberra, 2 November 2002, 7.

6. Evidentiary Certificates and Indemnities from legal action for ASIO officers

Evidentiary Certificates

This proposal is found in the Discussion Paper at page 51. The proposed basis for reform in this respect is to "provide a legislative basis for assisting ASIO to protect the identity of officers and sensitive capabilities involvied (sic) in the execution of warrant powers". The substance of the proposal appears to be to enact a provision (presumably in the ASIO Act) in similar terms to the evidentiary certificate provisions in the *Telecommunications (Interception and Access Act) 1979* and the *Surveillance Devices Act 2004*. The general purpose for these provisions is to prevent officers or employees from having to give evidence in court, where to do so would be disruptive to the efficacy of the agency involved and potentially dangerous to the officer or employee.

Evidentiary certificates represent a societal challenge whereby the ability of the agency to discharge its functions for the public benefit is in competition with the traditional notion of a judicial process and aspects of procedural fairness.

As the discussion by the NSW Court of Criminal Appeal in *R v Cheiko* (2008) 75 NSWLR 323 makes clear, there is a distinction to be drawn between the types of facts sought to be proven by the evidentiary certificate. Thus there is evidence of "formal matters of technical evidence" on the one hand and ultimate facts and issues, or "elements of the offence", on the other. Notwithstanding any constitutional limitations with the latter sort, there is on any view a confronting infringement on the nature of the judicial process itself, as well as on the procedural fairness to the defendant, if an element of an offence is determined by a party to the proceeding. The Joint Committee should be careful to ensure that the reforms are drafted in a way such that ultimate facts are not to be the subject of an evidentiary certificate, and that the content of such a certificate would be limited to facts removed from a fact in issue.

The evidentiary certificate provision(s) sought to be introduced should not be drafted in a way that prevents a defendant from challenging the accuracy of anything said or relied on in the intercepted communication. Furthermore the certificate should not operate to preclude a defendant from being able to provide evidence inconsistent with the Crown's case in respect of the interception, or indeed any evidence that would undermine a fact in a certificate. Importantly the evidentiary certificate should not operate to preclude the operation of s 137 of the *Evidence Act*, which would apply where the probative value of a certificate is outweighed by the unfair prejudice it would cause to a defendant. It may be that an evidentiary certificate goes to the exercise of the court's discretion in this regard,

but there will be other factors influencing the exercise of the court's discretion. Although national security will be carefully considered by the court, a certificate in this context should not be able to dictate an outcome in the face of inconsistent or doubtful evidence.

Although not explicitly foreshadowed in the discussion paper, to the extent that reforms are intended to protect the physical identity of ASIO officers in court (for example, in the sense presented in *BUSB v R* (2011) 248 FLR 368), any reform in The Committee's view should go no further than the approach taken in that case. Given that *vive voce* evidence brings with it different principles, any reform should maintain a discretion to the court to deal sensibly with the substance and presentation of the evidence. As that case demonstrates, the concomitant infringement on the open court principle can be dealt with by the traditional categories of exceptions to that principle and no further reform is necessary. The court will have the discretion, whether inherently or by way of existing statute, to make suppression order or screening orders as appropriate in the case. As indicated by Spigelman CJ in that case, ASIO officers will be entitled to special treatment in appropriate circumstances.

It is also important to bear in mind the circumstances in which an evidentiary certificate is sought. It is not clear how far beyond the execution of a warrant the proposed reforms will go. For example, it would be of concern if certificates were proposed to operate in relation to a serious criminal trial to preclude not only the defendant but the court from access to relevant documents. In this context there is no reason to doubt that the existing law is sufficient. The reasoning by the High Court in *Alister v R* (1983) 154 CLR 404 highlights that the court should not be seized of an opportunity to balance the prejudice to a person's liberty with the national security threat asserted. But even in this balancing exercising, it is settled that the government's assertion of national security will be one carrying great weight; *A v Hayden* (1984) 156 CLR 532.

Indemnities from legal action

At page 46 of the Discussion Paper it is suggested that ASIO officers or "human sources" are potentially exposed to civil and criminal liability in the course of their work. At a broad level there is nothing problematic with this statement: it is consistent with the well established rule that officers of the executive are subject to law. The discussion by the High Court in *A v Hayden*, particular the judgment of Brennan J (see also *Ridgeway v The Queen* (1995) 184 CLR 19 at 44), demonstrates the importance of this rule, although a reminder is necessary as the Executive may at times feel frustrated "by laws which affect the fulfilment of their policies".

The Discussion Paper highlights a deficiency in the current framework in that there is presently the potential for ASIO officers to commit an offence in the course of the legitimate discharge of their duties, such as in the example of intentionally providing training to a terrorist organisation. It is clear that it would be entirely reasonable and proper to remedy deficiencies of this character. However it is not clear to what degree the reforms will be of this character. Exemptions from prosecution from other laws – whether civil or criminal, Commonwealth, State or Territory – may not be reasonable and may operate to offend the fundamental rule outlined above.

If a scheme similar to that under the *Crimes Act 1914* were introduced, The Committee would support the adoption of the procedure and safeguards in that Act. Thus, any exemption would, of course, be strictly limited to conduct in the course of, and for the purposes of, the authorised intelligence operation, and where the scope of authorised intelligence operation is circumscribed by the formal authority to conduct the operation. For example, unreasonable conduct or manifestly reckless conduct would arguably not be in the course of, or for the purposes of, the authorised intelligence operation, and the ASIO officer would be liable for such conduct in this example.

A similar point is to be made about the proposal in the Discussion Paper to introduce authorised intelligence operation certificates, "which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months)".

The operation of any certificate in this context should be consistent with the regime for controlled operations in the *Crimes Act 1914.* That is, a certificate should not be able to specify conduct or exemptions that would circumvent limitations of the sort provided in the *Crimes Act 1914* and the conduct stated in a certificate must be consistent with the functions of ASIO. In this regard The Committee would support the proposal that any reform specify conduct that cannot be authorised. Further, although it is not clear precisely how a certificate would operate in this context, we would assume that the certificate would only go to detailing the nature of the intelligence operation and a specified officer's involvement in that operation.

In terms of the specified period, the Joint Committee should aim to make clear why 12 months is a justified period, given the shorter periods provided in the *Crimes Act 1914*; see, for example, ss 15GG and 15GH.

7. Conclusion

In conclusion, The Committee supports a position that provides law enforcement agencies and intelligence service with the appropriate tools to conduct their work (particularly in relation to civil and criminal liability of intelligence officers, and in relation to evidentiary certificates). However, such a position is not one that needs to provide unnecessary intrusions into private lives of members of the public, with little oversight, increased costs on private enterprise to comply with regulatory incursions and no analysis of additional departmental costs that would be required.

Reform of this kind has been a legislative priority for a decade. It should be clear that a piecemeal approach has not met expectations. The relative costs and utility of further legislation ought to be weighed carefully, particularly in the wake of the recently announced COAG Review of Counter-terrorism legislation.[20]

[20] *COAG Review of Counter-terrorism Legislation* (2012) Council of Australian Governments <http://www.coagctreview.gov.au/Pages/default.aspx> at 13 August 2012.