Submission No 152

Inquiry into potential reforms of National Security Legislation

Organisation: Ms Stella Gray

Stella Gray

20 August 2012

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

This submission seeks to address specific points outlined in the discussion paper, *"Equipping Australia Against Emerging And Evolving Threats"*. I welcome the Parliamentary Joint Committee on Intelligence and Security offer to allow public consultations on this inquiry, as its scope concerns every Australian citizen.

It is important to make clear the angle that this submission is being written from. I have written this submission as an Australian citizen, who has no vested corporate, state or non-governmental organisation interests.

This inquiry must be considered specifically within its historical, legal and political context. Since 2001, there have been over 50 amendments enacted for anti-terror legislation in Australia.[1]

The argument for robust national security law should *not* be an argument for the abrogation of due process, i.e. reasonable suspicion demonstrated before a court in order to obtain a warrant.

Australia is now the only democratic nation in the world without a national human rights law such as a human rights Act or bill of rights.[2] Such an Act, when in effect, is the principal means for citizens to protect themselves from arbitrary, politicized and ideological abuses of power by the police and intelligence community.

In the last decade, the gamut of national security lawmaking in Australia has done away with the separation of powers principle. Two notable examples of this include the decision-making power of who proscribes organisations as terrorist ones and the execution of search warrants and warrantless searches coming under the control of the executive, away from the judiciary.[3] Australians were previously able to point to this doctrine as a way to differentiate our nation from that of a failed state. This is no longer the case.

The key policy-making trend since 2001, shared by Australia's allied nations, is the pre-emptive nature of national security law. While there is a need for sensible,

---

[1] Williams, G. 2011, 'A Decade of Australian Ant-Terror Laws', Melbourne University Law Review, vol. 35 no. 36, pp 36-76
[2] Ibid.
[3] ibid.

nuanced legislation that serves as a deterrent to those planning serious criminal acts, tipping the balance too far to one side makes everyone a suspect.

Justification for increased search and seizure powers is often promoted by authorities in a reflexive response to a threat *du jour* running through the news cycle, yet the issue of proportionality is seldom addressed with equal vigour.

Although this inquiry purports to simplify some of this vertical layering of law, the proposals instead indicate only a desire for expanded powers. *This discussion paper's references to the 'streamlining' of law appears to act as a euphemism for the law enforcement and intelligence community to increase its power with no clearly articulated safeguards.*

A consistent, repeated demand for increased investigatory powers raises the question: Precisely what is it about the techniques and practices of police and intelligence communities that are ineffective enough to justify their constant demands for broader powers?

The fundamental question that the terms of reference (TOR) refuse to answer is who will be monitoring those who monitor us? It's a common refrain, almost hackneyed to those who extol civil liberties, but the simple crux of this question remains inviolable in its meaning.

Responses to certain sections in the discussion paper

Under **section 1.1** is outlined a set of statistics to highlight the efficacy of communications intercepts in generating arrests and prosecutions. Yet these statistics omit the crucial key to this ratio: How many intercepts were conducted in order to make this number of arrests and prosecutions?

The TIA report (Australian Attorney-General 2011) stated
"In 2010□2011 there were 2441 arrests, 3168 prosecutions (2848 for serious offences) and 2034 convictions (1854 for serious offences) based on lawfully intercepted material.2 Law enforcement agencies made 91 arrests, 33 prosecutions and obtained 33 convictions based on evidence obtained under stored communications warrants. The number of warrants issued in the same period was a staggering **243,641**. This equates to a ratio of approximately 1000 warrants to each arrest. These statistics do not reveal how many warrants were issued per case. From this it is logical to infer that invasions of privacy were routine. Also not included are intercept statistics for ASIO, which were not included in this report.

Clearly there is imbalance of information available to the public here. Even if the ASIO intercept statistics were included in the figures above, not disclosing the number of arrests and prosecutions instigated by ASIO tells us nothing of the total

effectiveness of interception as a crime-fighting tool. It does, however, reveal a propensity for agencies to conduct 'fishing expeditions'[4].

Comment in response to Section 1.2 (page 15)
In reference to page 15, "Nation states *as well as disaffected individuals and groups,* are able to use computer networks *to view* or siphon *sensitive, private or classified information* for the purpose of espionage, political diplomatic or commercial advantage" While this statement is inclusive of bona fide espionage activity, it can also be practically applied to the general public when viewing documents released by media organisations such as Wikileaks. By this definition, thousands of Australians have already conducted espionage by looking at this published material on their computers.

Comment in response to Section 1.5 Fundamentals of the current Act [TIA] (Page 17)

This section states that multiple amendments to the TIA have "*been able to accommodate emerging threats and changes in criminal behaviour because the legislation does not limit the concept of interception to a particular technology (such as telephone).* ***By couching the Act this way the currency of the legislation has been maintained through amendments that have clarified the application of the Act..."***

This line of reasoning demonstrates that the TIA already provides authorities with full access to communications when they are requested.
A subsequent excerpt reads: *Much of the need to amend the TIA Act stems from the contextual foundations of the Act. Many of those foundations no longer apply, creating significant challenges for agencies to maintain current investigative capabilities.* The foundations that 'no longer apply' are not explored in detail. Hence, this justification remains vague and ill defined.

The basic essence of the TIA is to ensure that interception of communications is the exception, not the norm. With nearly 250,000 interception warrants issued between 2010-2011 alone, demands from the police and intelligence community to make the interception process easier only serves to normalise total surveillance of Australian citizens.

Comment on Section 2.1 – Identifying communications
(Page 21)

This section stresses the issue of accurately identifying a user on an internet-based network. Although the paper states the *"TIA is based on an assumption that there is a unique, non□ambiguous identifier, such as a phone number, linking the target of an interception warrant to the service (or device) to be intercepted",* multiple amendments to the TIA have enabled interception activity to operate beyond the

[4] Dorling, P. (2012) Police spy on web, phone usage with no warrants, 'Sydney Morning Herald', accessed 17 August 2012 <http://www.smh.com.au/technology/technology-news/police-spy-on-web-phone-usage-with-no-warrants-20120217-1tegl.html#ixzz24589oFKv>

1970s-era scope of the analog telephone. This ability is acknowledged in the discussion paper in Section 1.5 (see above). The wording in Section 2.1 also demonstrates that the police and intelligence community see a problem with the encryption of everyday communications and the use of VPNs (virtual private networks which anonymise IP addresses), which are used legitimately by individuals and businesses every day.

Responses to Proposals Outlined In The Terms of Reference

Section C. 15. Modernising the Industry assistance framework
(a) Establish an offence for failure to assist in the decryption of communications

This proposal, along with the data retention proposal discussed below, is highly worrisome.
Many web services (email, cloud storage such as Apple's iCloud, or Dropbox) are useless without effective encryption. The only way for encryption to be effective is if the service provider is unable to decrypt your content without your involvement. Hence, this proposal raises the prospect of police and intelligence agencies demanding built-in leeway for forced decryption, which will fundamentally alter the entire online security landscape. This proposal is also highly illiberal as it is prone to abuse. It can be deployed against journalists, lawyers and others who enjoy some form of professional privilege with their clients (or sources). I cannot support this proposal.

Section B.
9 *a. Implement detailed requirements for industry interception obligations*
b. Extend the regulatory regime to ancillary service providers not currently covered by the legislation
c. Implement a three‐tiered industry participation model

See also: *Access to communications content and communications data* (page 21)

And:

Section C. 15. Modernising the Industry assistance framework
(c) Tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

"…Whereas telecommunications services were once provided by a single carrier, in many cases now each communication event typically involves a number of service providers…many application service providers operate from offshore making the provision of assistance to Australian agencies challenging."

These arguments are based on the idea that cloud-based computing services, as well as social media networks such as Google, Facebook, Twitter et al are currently off

limits to authorities but should not be. There are several specific problems with this thinking.

- Firstly, this brings internet companies such as Google under the same umbrella as telecommunication service providers such as iiNet and TPG.

- Extension of TIA requirements to such internet companies is known as 'creating backdoors', the deliberate creation of vulnerabilities in a system allowing regular authentication to be bypassed. This is a significant alteration to the architecture of internet networks and will certainly be exploited by hackers[5].

- Internet companies would need to be regulated same way as CSPs, which is not tenable if many of these companies are owned and operated outside of Australia.

- This has great potential to discourage foreign companies from providing services to Australians if the administrative and technical burden of TIA compliance is too high.

- It is also likely that extension of the TIA to such companies would then prohibit the use of their services if they do not comply with Australian law enforcement standards.

- Telecommunications services will become significantly more expensive, which is likely to deprive people of lower socio-economic backgrounds with connectivity.

- This will unnecessarily impose on the millions of citizens who use such services without criminal intent.

Recent developments in 2012 do not inspire confidence in CSPs' data security practices. The intrusion into AAPT's network to obtain customer data illustrates that industry best practice does not exist. Servers hosted with third-party providers are often paid for and forgotten about – with data still remaining on them. Such 'lost' servers can be easy prey for hackers.[6]

Another problem with this TIA proposal is that it uses phone interception as a model for web interception. A web browser hops through multiple IP addresses before reaching its destination to the page a user is navigating to. A web user is not in control of every IP address their web browser visits[7]. Dozens of analytic trackers (measuring page view statistics) and advertising servers all run in the background on many websites that people frequent daily. That is a lot data that CSPs will need to be trusted to store, and a lot of data that law enforcement will need to sift through every time they are suspicions of someone. Adding to this problem are compromised web servers

[5] Emspak, J. (2012) FBI surveillance backdoor might be open to hackers, Technolog, MSNBC, accessed 19 August 2012 http://www.technolog.msnbc.msn.com/technology/technolog/fbi-surveillance-backdoor-might-be-open-hackers-947887

[6] Sharwood, S. (2012) The policy that helped Anonymous hack AAPT, 'The Register', accessed 17 August 2012 <http://www.theregister.co.uk/2012/08/07/how_anonymous_hacked_aapt/>

[7] Chirgwin, R. (2012) The asymmetry implicit in Internet data retention, 'The Register' accessed 12 August 2012 <http://www.theregister.co.uk/2012/07/31/anonymous_go_bloody_home/>

that users may inadvertently be directed to via malware. Another compounding factor is that much web traffic data is 'non-human' (as high as 51 per cent). [8]
The amount of data 'noise' is astronomically high.

The other issue this raises is the integrity of law enforcement data systems themselves. Data is proliferative matter; databases usually beget more databases, which create the perfect conditions for (accidental and deliberate) leaks and intrusions to occur. One example is the Victoria Police LEAP data incident, where "data relating to a substantial number of people was sent electronically by Victoria Police and/or its contracted service provider IBM to an individual employed in Corrections Victoria who had no proper interest in receiving it" [9]

Mass surveillance via data retention also contravenes the following Articles of the United Nations Declaration of Human Rights:

- Article 12 the Right to Privacy
- Article 19 Freedom of Expression
-Article 20 Freedom of Association

Creating law to enable complete access to everyone's communications will create many false positives in relation to data mining; it will create unnecessarily detailed profiles of every individual citizen regardless of whether they are under investigation or not; it will also have a 'chilling effect' on political speech and public discourse.

Pre-emptive surveillance of an entire population does away with the legal principle of the presumption of innocence. Any serious consideration of implementing such a system, in a democratic country such as Australia, should be anathema to policy makers.

Section A
4. Modernising the TIA Act's cost sharing framework to align industry interception assistance with industry regulatory policy
(Page 24)

"The current requirements are predicated on the existence of one or few industry players and assume that all are resourced on a similar basis and have a similar customer base. This does not reflect industry practice which better suits a tiered model that supports comprehensive interception and delivery capability on the part of larger providers, a minimum interception and delivery capability on the part of medium providers and only reasonably necessary assistance for interception on the part of smaller providers."
A tiered interception-compliance model may simply encourage people to flock to smaller CSPs to evade surveillance, thereby negating the structure of this model.

---

[8] Grandoni, D. (2012), 'Non-Humans' Account for 51% of All Internet Traffic (in italics), 'The Atlantic Wire', accessed 19 August 2012, <http://www.theatlanticwire.com/technology/2012/03/non-humans-account-51-all-interent-traffic/49967/>
[9] Privacy Victoria (2005) *Investigation of Security of LEAP Data*, accessed 18 August 2012 <http://www.privacy.vic.gov.au/privacy/web2.nsf/files/investigation-of-security-of-leap-data>

Section C, part 16
(a) Instituting obligation on the Australian telecommunications industry to protect their networks
[Page 32-39]
As digital infrastructure becomes more ubiquitous, some form of obligation on the telecommunication industry to protect against intruder and data loss threats is essential. However, an independent audit process should be established to handle this function. CSPs should be deterred from leaving their networks and data unsecured; there should also be a requirement obliging CSPs to report data breaches to their customers within an acceptable time frame. However (as referred to elsewhere in this submission), the dilemma inherent in the government's proposals is the obvious intent to mandate a data retention policy, which would create more possibilities for data breaches, would in turn negate the efficacy what is proposed for industry obligations here. It is nonsensical to create a law punishing CSPs when data is 'accessed and published' when concurrently requiring CSPs to store data beyond their everyday business requirements in the first place.
Section A pt. 2.a Reducing the numbers of agencies eligible to access comms information
(Page 24)

The paper lists here some of the agencies and bodies that have intercept powers (e.g. ASIC, ACCC, Centrelink). Then it states:
"Consideration is also being given to reducing the number of agencies able to access communications information on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so."
I support this proposal. Reducing the number of government agencies which have access to individuals' private communications, reduces the ability to abuse the TIA. However, there is insufficient detail here on which agencies are being considered for reduction in such powers.

Section A pt. 3 – Simplifying information sharing provisions (Streamlining and reducing complexity in the law)
(Page 25)

The paper highlights barriers to effective information sharing between agencies under the TIA in this section. This is a critical grey area where legislators must tread carefully.
It is fair and reasonable to assume that if an agency obtains evidence of a crime that is outside their jurisdiction to pursue, they should be able share that evidence with the relevant agency. However, they should only share the evidence relevant to the crime in question. If agencies were allowed to share the entirety of communications intercepted under the original warrant, this would be a clear case of overreach, and has severe implications for citizens' privacy. It is crucial that all information gathered from warrants remains stored separately as a privacy safeguard. If this aspect of information sharing is not treated with precision, there will be a temptation to create a central database accessible by all agencies, which is a security and privacy risk in itself.

Section A pt. 2 (a) Standardisation of warrant tests and thresholds
(Page 24)
The government proposes making changes to the penalty thresholds that law enforcement agencies abide by when determining which investigations require communications intercepts. Reducing the penalty threshold from 7 years to anything lower will give law enforcement free reign to conduct invasive interceptions for minor offences. I do not support this proposal.

Section A pt. 1 (c) Mandatory record-keeping standards
(Page 26)

The importance of record-keeping standards being upheld by agencies with TIA powers is justifiably emphasized here. I support this proposal.

Section A
1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the TIA Act.
(d) Oversight arrangements by the Commonwealth and State Ombudsman
(Page 26)

"…Many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate." This indicates the government sees current safeguards against abuse and corruption by police and intelligence agencies as too stringent, which is disingenuous.
Further to this, the government states: *"Consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes."* The question here is: Who is to conduct such evaluations? If the emphasis is on allowing a government minister to determine 'proportionality' with lesser or no regard to 'process', this effectively diminishes any effective oversight function.

The following practices are permissible under current federal legislation:
- Detention of suspects by ASIO on mere suspicion of committing an offence
- Detainees held by ASIO have no right to choose their own legal representatives
- Under The ASIO Act 1979 (Cth) makes it a serious offence to publicly identify ASIO officers or agents, which means detainees are unable to take ASIO or one of its officers to court for torture prolonged interrogation and other abuses

It is within this existing framework that Justice Adams ruled in 2007 that ASIO's treatment of Izhar Ul-Haque during his 2003 interrogation was a "gross breach of the powers given to the officers under warrant"[10].

[10] R v Ul-Haque [2007] NSWSC 1251

Although some of the laws referenced above are subject to the review of other current inquiries, these examples highlight the fact that there are weak accountability mechanisms in place for Australia's intelligence services.

In order for Parliament to conduct a fully reasoned argument about oversight arrangements as referred to in the Terms of Reference of this inquiry, such laws described above would need to be repealed in the first instance.

ASIO Legislation Reform

Section A.5.a-b (from ToR) Page 41 in Discussion paper

- Proposed changes to 'computer' in section 25A of the ASIO Act

In this section the paper states:

"If there are multiple computers on a premises, and it is only discovered upon entering the premises for the purpose of executing a warrant that a particular computer is not connected to the computer system specified in the warrant, it would be necessary to seek another warrant…A possible solution to this issue could be to amend the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network."

This proposal does not define how it would ensure that ASIO does not inadvertently access computers on a network that are not the target of a warrant. Now that cloud and 'virtualisation' services are becoming increasingly ubiquitous, this is an important distinction to make. I cannot support this proposal with its current wording.

Variation of a warrant
Section A.5. a - b (Page 41)

Here the proposal states, *"A variation provision may be appropriate to ensure sufficient operational flexibility while maintaining appropriate accountability."* The rationale given here is because a *"new warrant is required in every instance where there is a significant change in circumstances."* Similar to the proposal for search six-month durations of search warrants, this provision paves the way for overreach and abuse by ASIO, when considered in the context of the minimal oversight ASIO already has. I do not support this proposal.

Duration and renewal of warrants – section A, 5 (b) (page 42)

---

http://www.lawlink.nsw.gov.au/scjudgments/2007nswsc.nsf/aef73009028d6777ca25673900081e8d/d9a9080227820bddca257389007c91e4?OpenDocument

In this section, the government is proposing two things: 1) Increase search warrant periods from 90 days to 6 months to make it "consistent with other warrant powers" in the ASIO Act; and 2) indefinite renewal of all warrants.
Currently, the following sections in the ASIO Act allow up to six months per warrant:
26B. Tracking device warrants relating to persons
26C. Tracking device warrants relating to objects
25A. Computer access warrant
The legislative milieu for ASIO warrants is already heavily weighted towards the longest periods possible for ASIO officers to obtain evidence. Six-month warrants in the abovementioned categories already provide ample time for evidence gathering. In the proposal, it is apparent that ASIO sees re-applying for a search warrant every 28 days as an inconvenience.

However, the warrant process is an accountability mechanism; ASIO's need for obtaining unfettered access to someone's premises and belongings should be restated frequently to prevent abuse of the law. A six-month search warrant as proposed here is unacceptable.

Section 7. Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies (pg. 45)

Here the proposal states: *Paragraph 6B(e)(ii) could be amended to remove the word 'such', so as to avoid any doubt that DIGO is enabled to provide Commonwealth and State authorities, and other approved bodies, assistance in relation to the production and use of both non intelligence and intelligence imagery and geospatial products.* This would enable ASIS, DSD and DIGO to collect intelligence on Australian citizens whenever the agencies are cooperating with ASIO in the performance of its functions. This proposal is does not include any provision to prevent the abuse of power by these agencies whilst working in concert. This proposal cannot be supported with the current level of accountability it demands of these agencies.

Section 12 – Clarify ASIO's ability to cooperate with the private sector
(Page 49) This section lacks detail in the discussion paper; therefore I reserve stating support for this without further elaboration on the government's intent.

Section 13 (page 49) Amend the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act
This proposal recommends amending the ASIO Act to enable ASIO officers to report offences committed by other ASIO officers to law enforcement. This proposal is good common sense and has my full support.

Section 17. A (page 50) Use of third party computers and communications in transit
The government proposes allowing ASIO to use third party computers in order to conduct surveillance on a suspect without being detected. I do not support this proposal, as safeguards against abuses of privacy have not been articulated fully. For example, would such a practice be conducted with the knowledge and consent of the

owner of the third-party computer? By design, this proposal is asking to allow ASIO to abuse the privacy of third parties in order to conduct investigations.

Section 17. B (page 50) Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant

Here the government is asking for clarification on whether current law allows ASIO to enter a third party's premises for the purpose of executing search warrant. This proposal raises significant privacy concerns. For instance, the use of surveillance devices in such a situation could mean a device will also record third party communications, which have nothing to do with ASIO's investigation. Coupled with the prospect of six-month search warrants, this provision would be open to abuse and overreach.

As it is clear the argument here is for actually allowing for such incidental power, I reject such a proposal.

Section 10 Amending the ASIO Act to create an authorised intelligence operations scheme (page 46)

This is requesting permission for ASIO to commit crimes in order to solve them (or gather intelligence). Even with an anti-entrapment provision, this is not a law that should be found in any healthy democracy.

Section B, 11 (c) Enable the disruption of a target computer for the purposes of a computer access warrant (page 48)

Subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons.

It must stay this way. Such a provision will foster the planting, tampering and destruction of evidence, and will allow ASIO to store malware on computers. I cannot support any aspect of this proposal in any hypothetical scenario.

Thank you for taking the time to read this submission.

Stella Gray