Submission No 50

Inquiry into potential reforms of National Security Legislation

Name: R Batten

Organisation: Private capacity

15 August 2012

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

Inquiry into potential reforms of National Security Legislation

I am pleased to submit the following document for consideration by the committee as part of its inquiry into possible reforms of Australia's National Security Legislation. I have structured this submission around the contents of the discussion paper published by the Attorney-General on the topic and included in the terms of reference for this inquiry. In the following pages I have addressed each of the proposals contained in that discussion paper I consider to be of import and provided the committee with my opinions. The discussion paper was quite extensive and included a large number of proposals, many of which are of little consequence and relate only to improving the efficiency of the relevant government agencies. As such, I have not attempted to address every single proposal in the paper – where a proposal is not discussed in this document it can be assumed that I either support the proposal or do not have an opinion one way or the other.

The views expressed in this document are my own personal opinions and I do not claim to represent any organisation. I currently work in the ICT professions.

Summary of opinions

I found it difficult to clearly support or object to a number of the proposals contained in the discussion paper as I found many points overly vague concerning key details that could prove pivotal to the appropriateness of the proposed changes. As such, when discussing each proposal I have attempted to outline my concerns even for proposals which I support, as the exact nature of the implementation will be critical in many cases.

By way of brief summary…

I broadly support the following proposals in the discussion paper:

- Reduction in the number of agencies eligible for communication interception warrants.
- Update definition of serious crime.
- Single warrants with multiple intercept powers.
- Add obligations to protect networks.
- Update the definition of computer.[1]
- Variations to warrants.
- Updates to ASIO employment conditions.
- Protection from criminal liability.
- Named person warrants.
- Surveillance devices.
- Warrant authorisation lists.
- Identification of ASIO officers.
- Ministerial authorisations.
- Cooperation between agencies.
- Weapons training.

I am opposed to the following proposals:

- Extend legislation to include new types of service providers.[2]
- Review cost-sharing requirements.
- Data retention requirements.
- Make failing to assist in the decryption of communications an offence.
- Interruption to service.

I do not believe there is sufficient detail to either support or oppose the following proposals:

- Re-examine privacy protection objectives in reporting.
- Allow sharing of data between agencies.
- Cooperation with private sector.
- Third party computers and communications in transit.

Reduction in the number of agencies eligible for communication intercept warrants

The paper notes that since the TIA act was created in 1979 the number of agencies able to apply for warrants have grown significantly. The paper proposes that this list of 'authorised' agencies be significantly culled. However, it doesn't actually state which agencies it is proposing lose their access.

This proposal seems appropriate to me, but it would have been nice to have a clear list of agencies that a) currently have this power, and b) will lose it under the reform.

[1] Although I support updating this definition, I have reservations about the proposed new definition.
[2] I do support part of this proposal, see the detailed section of this document for full information.

Re-examine privacy protection objectives of reporting

This proposal is focussed on the mandatory reporting that must be produced by agencies and the AG's office to help monitor the use of communication warrants. The discussion paper states that they feel the current reporting requirements are too focussed on administrative requirements (the number of warrants issued etc). The paper states they want reporting requirements to consider 'proportionality' when assessing what needs to be reported to the ombudsman.

The current reporting seems very good at monitoring 'workload' and assessing effectiveness in terms of the number of convictions etc the warrants are achieving. However, it doesn't seem to provide any information that would help assess if warrant powers are being abused for instance. From this regard, a review of the reporting requirements seems like a good thing. However, the term 'proportionality' in the discussion paper and the lack of details about what reporting the AG would like to introduce make me a little nervous. This is one where the devil is in the details and I can neither support nor object to this recommendation without knowing more about the proposed new reporting.

Allow sharing of data between agencies

This is a potentially tricky one. The discussion paper points out that the current legislation has very strict controls preventing the sharing of communication data captured under a warrant by one agency with any other agencies. Unfortunately, there is little detail in the paper as to what the AG envisions by this, so I think it is important for us to pain the picture.

As a privacy concern, I would not want my personal information being freely circulated amongst agencies. At the same time, if ASIO obtains a warrant to aid in an investigation and instead discovers evidence incriminating the target in murder I would want ASIO to be able to provide that evidence to the relevant police to prosecute. This type of scenario comes down to jurisdictional challenges.

Personally, I would support the following scenario:

- If an agency obtains evidence of a crime that is outside their jurisdiction to pursue, they may share that evidence with the relevant agency. However, they may only share the evidence relevant to the crime in question. They may not share the entirety of communications intercepted under the original warrant. They may *only* share that evidence with the agency holding jurisdiction over the crime / suspected crime in question.

It is important that all information gathered from warrants remain siloed for privacy protection. We cannot allow such data to be fed into a central database accessible by all agencies.

Update definition of serious crime

The current legislation makes warrants available only when investigating 'serious crimes.' However, there are multiple definitions of what a serious crime is. When applying for the interception of real-time communications (tapping phones) the definition is for crimes where the penalty is seven years or more. When applying for the interception of stored communications (email) the definition is for crimes where the penalty is three years or more. Based on the criticisms of the three year threshold on page 24, I am assuming the intention is to standardise the definitions on a seven year threshold.

I'm not particularly concerned by this proposal as it seems silly to have two different definitions.

Extend the life of warrants

Currently, communication intercept warrants are valid for 90 days after being issued. However, many other types of warrants are valid for six months. The discussion cites instances where warrants have lapsed without being served due to complications relating to catching the target at a location where the warrant is valid (this 'location' issue is also tackled elsewhere so I won't detail it here).

I don't have any real views one way or the other here. It would seem to me that it ought to be possible to act within 90 days (else why apply for the warrant) but I am not familiar with the intricacies of doing so. It is probably worth noting there are other proposals in the discussion paper that should make it easier to server warrants within the 90 day period. However, I don't see any real issue serving a warrant after six months rather than three.

Single warrants with multiple intercept powers

Currently all warrants are issued for single specific intercept. As such, if an agency wants to intercept phone calls, text messages and email of a specified target, they must separately apply for three different warrants. The discussion paper proposes that agencies should be able to apply once and specify the types of communication they wish to be covered by the warrant.

This proposal does not change the types of communications that can be intercepted by agencies. It also shouldn't affect the number of communications being intercepted or the oversight of the warrant process. What it will affect is the cost to the taxpayer of agencies applying for warrants. Based on this assessment, I support this proposal.

Extend legislation to include new types of service providers

When the original legislation was introduced in 1979, essentially all communications were provided by the traditional carriers / carrier service providers (C/CSP) and there were not very many of them. However, now there are thousands of possible service provides, and more importantly, most are not the traditional C/CSP covered by our intercept legislation. For instance, currently legislation permits agencies to get a warrant to intercept your email provided by Telstra or Internode, but not your Gmail or Facebook messages. The discussion paper proposes that the act be updated to include new

forms of service providers. The effect of this would be agencies could get warrants to intercept your Facebook messages, skype calls and other similar communications.

Part of the above proposal would require the affected service providers to 'maintain the capability to intercept' and submit plans to authorities detailing how that capability will be achieved / maintained.

Although I see the contradiction in the status quo where some email is subject to warrants whilst others aren't, I have reservations about the impact of this proposal. It has the potential to dramatically limit the range of services available in Australia due to the administrative and technical impost it would place on companies – especially companies not based in Australia. History has shown Australia to be a small and (relatively) insignificant market to many tech companies, so it would seem logical that many would simply 'not bother' if Australia required the development of such compliance plans. It would also likely completely block a range of services which are designed so that the service provider itself cannot 'spy' on its users. These services are often popular not because any desire to commit crimes, but because it protects users in the event the service provider is compromised.

I would support enabling such services to be served warrants for communications interception, but do not support the requirement for such providers to 'maintain the capability to intercept' along with the requirements to submit plans for enabling such capability. Such a requirement would be virtually impossible to enforce, given the global nature of the services involved and ultimately prove rather pointless whilst inhibiting the ability of local business to compete with innovation.

Review cost-sharing requirements

This proposal seems to be in recognition that a number of other proposals in the discussion paper are going to add a significant cost to service providers. In particular, I believe this is targeted at the proposal to introduce data retention requirements (coming up next). The proposal is that the actual requirements placed upon service providers to retain data and assist with interception of communications would be tiered based upon the 'size' of the service. The fewer users you have, the less you have to do.

This proposal does (somewhat) ameliorate my concerns about cost becoming a barrier to innovation with these services, in that the small players essentially wouldn't have to comply. However, it begs the question; if such a tiered model is introduced why bother at all? Surely under such a scheme the serious criminals would simply flock to small services with little requirement to retain data and enable interception of communication.

Data retention requirements

This is probably the proposal that has attracted the most attention in the media; placing a requirement on service providers to retain user data for up to two years in case authorities decide to get a warrant for it. The discussion paper is actually a little vague on this and doesn't specify what

data would need to be retained – would it be everything? Or just 'communications'? The proposed definition of 'data' on page 25 of the discussion paper suggests that the proposal may be to simply retain the data about communications, and not the actual content of such communications, but it simply is not clear enough to be certain. My understanding of the proposal is that it would cover all relevant service providers, from your Telco, to your ISP to FaceBook.

I don't support this proposal at all. A fundamental principle of the modern age is that users own their own data; whether that be their medical records or their email. This proposal attacks that basic right by declaring that individuals do not have the right to control how and where their data is used. A second argument against this proposal is the significant privacy risk it creates for individuals. With data and identity theft now such a serious risk for the community, people have the right to protect their information. By mandating that all service providers retain user data, you remove the ability of citizens to effectively protect themselves from data and identity theft. After all, it has become common news for a company to be 'hacked' and user data stolen. This proposal would create virtual treasure troves for such thieves to raid and citizens would be able to do nothing to protect themselves. Finally, there is the question of cost. The world has entered the age of Big Data (look it up) and the quantity of data being stored and transmitted between services is skyrocketing. The cost impost this proposal could have on service providers is staggering and cannot help but to stifle innovation and restrict the services available to Australians. It seems the previous proposal, making the cost-sharing model tiered, was intended to alleviate this last point. However, as I stated under that heading, if you are going to remove the requirement from small services (and hence create a massive loophole for criminals to exploit), why bother at all?

Note: If this proposal was actually to be read with the new definition for 'data'; information about a communication that is not the content or substance of a communication I still have reservations. Translated to (for instance) instant messaging, this would mean information on who you were communicating with and when, but not necessarily the actual content of the conversation. If this is what the data retention proposal is actually about it does improve the proposal somewhat, as it brings the data retained essentially in line with what telco's currently track and retain. However, it is still far from ideal as this would still infer a massing amount of information about our lives – information not easily extracted from phone records. It is also important to point out that the wording of the data retention proposal is very vague about what specific 'data sets' they want to retain and that is concerning.

Make failing to assist in the decryption of communications an offence

There isn't a lot of detail on this, but my reading of the discussion paper is that they want service providers to be able to decrypt any communications on their services when intercepted under a warrant and make it an offence not to do so to force compliance.

This poses a serious issue to a number of service providers and should be opposed. Take as an example the online backup service iDrive. To protect users in the event iDrive itself is compromised, all user data is encrypted so that only the user can decrypt it. By design, not even iDrive can decrypt the data. This isn't to enable criminal activity, but to protect users from data theft and is considered

normal industry behaviour now. Forcing service providers to have a 'back door' into such data is a serious security threat and flies in the face of modern best-practice.

The very vague wording of this section could mean organisations and individuals are merely required to 'assist', not necessarily build back-doors into their services. This is certainly possible, but on contemplation I don't see why they would bother if this is the case. Without a back door there should be no need for assistance, as our agencies should have access to all the same tools the service providers have for breaking encryption.

Add obligations to protect networks

This proposal is focussed on the security of Australia's critical infrastructure. The discussion paper points out that our communications infrastructure is entirely managed by private enterprise now (NBN aside) and looks at the possible impact a failure of those services would be. Similar to regulations placed on our electricity industry to ensure the security of electrical supply, the paper proposes introducing a regulatory framework for ensuring continuity of communications services to Australia. The paper posits this is necessary as a) commercial interests will not always result in businesses providing sufficient emphasis on security over profits, and b) individual enterprises may not have a sufficient understanding of the overarching security threats / context faced by Australia.

The paper talks about a couple of ways this regulatory framework could be enacted. The core of the proposal seems to be:

- Define a compliance framework of security outcomes the industry must meet – specifically states that this should avoid specific technology definitions to allow industry to determine the best implementation.
- Auditing of compliance. This point seems a little confusing as to how it will be enacted. Some sections seem to suggest companies submitting plans to government, others using independent audits.
- Penalties for non-compliance.

I support the concept of a compliance framework to ensure our critical infrastructure is protected – it is a strategy that has worked in other infrastructure scenarios fairly successfully. However, I think it is important that compliance with the framework be assessed by independent audits. Similar to previous points I have made, if all participants submitted their security plans to government for assessment it would represent a security risk in and of itself.

Definition of computer

Current definition of what constitutes a computer is from 1979 and poses limitations on warrants. For instance, if an individual has data stored on a home network or multiple computers, agencies must apply for multiple warrants. Similarly, I imagine smartphones etc. must be challenging. The discussion paper proposes the definition be extend to include 'a computer, computers on a particular premises, computers connected to a particular person or a computer network.'

Although I support the need to update the definition used for forming warrants, I am not convinced the updated definition is adequate as it seems overly focussed on physical devices. Virtualisation and cloud services are now mainstream, and we need an intelligent warrant system to accommodate this. If a user has a virtual machine hosted on a major cloud service provider, how do our agencies get a warrant for that? I would like to see a definition that enables a warrant for just that virtual machine (which the cloud service provider can then supply) without affecting the potentially thousands of other unrelated systems on that infrastructure.

Variations to warrants

Currently, when a warrant expires (such as for phone interception), the agency must file for an entirely new warrant if they wish to continue. This proposal is to allow the agency to apply for a the warrant to be renewed instead. This would still require the same level of approvals as a new warrant, but would streamline the process by removing the need to re-establish all the relevant evidence. Similarly, the document proposes agencies be able to request variations to warrants.

I cannot see any major issues with this proposal.

ASIO employment conditions

The discussion paper outlines a number of changes concerning employment with ASIO to bring it in line with other agencies, simplify secondment between agencies and agency collaboration and remove some confusion about the functions of the Defence Imaging and Geospatial Organisation (DIGO).

This sectional seemed pretty straight-forward and I support it.

Protection from criminal liability

This proposal is specific to intelligence officers (ASIO, ASIS). Under current legislation, there are no protections for officers when required to breach the law in the course of their duty. The proposal here is that some limited protections would be introduced and this time the paper does give some specific examples. For instance, if an intelligence officer is tasked with infiltrating a terrorist organisation, which includes attending one of their training camps. Under Australian law, receiving such training is a crime and the agent could be prosecuted.

There is already a protection scheme in place for non-intelligence agents under the Crimes Act 1914 which covers police etc. The proposal is to enact a scheme based off this with some minor modifications to recognise the covert nature of ASIO and ASIS activities. The discussion paper includes a number of specific safeguards that would be required:

- Would not be blanket protection. Approval would be required in advance similar to a warrant and would only last for a specific period of time. These approvals would state the specific activities being allowed – no other activities would be protected against.
- Full oversight of approvals would be maintained.
- The proposed legislation would also state a list of conduct that cannot be authorised by the scheme (intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person).
- Full independent audit / review of the scheme after five years.

Based on the above I support the proposal. The example provided is one where it would not make sense for the agent to be liable for prosecution.

Named person warrants

Currently, ASIO warrants cannot be just for a person, but need to be for a premise. This not only causes a problem with cloud and mobile services but also means if you want to 'search' the person, you need to wait until you can catch them at the relevant location. The proposal is for the introduction of 'named person' warrants, where permission is granted to intercept communications (email, text, phone etc) associated with a person, not location.

This seems to make a lot of sense and I support it. It is worth noting that specifics of the proposed warrant matches changes proposed earlier where one warrant can be for multiple forms of communication intercept.

Surveillance devices

This proposal is to update the rules concerning warrants for ASIO's use of surveillance devices to match other agencies. For instance, currently ASIO cannot get a video surveillance warrant separately from an audio warrant. Essentially, the proposal is to make the ASIO rules match those found in the Surveillance Devices Act that governs police.

As this is bringing ASIO in line with police I support this change.

Interruption to service

The current warrant legislation prohibits any action that would interrupt another's lawful access or use of the computer including adding, deleting or altering data. The discussion paper states it would like this prohibition changed to include a proportionality test based on what is necessary to execute the warrant.

I am extremely nervous about this proposal. The discussion paper does not provide any details of what this 'proportionality test' would entail. Further, as evidenced earlier in my points, this discussion paper does not seem to take into consideration of virtualisation and cloud services. Where in the past allowing disruption to a computer might affect a handful of individuals living at the same address, or a single businesses files (if a business was being searched), in the modern environment this could potentially affect many thousands of users worldwide – all dependant on the wording of what is allowed. Any reform that allows interruption to service needs to be worded to be cognisant of the potentially very broad implications of such interruption, and that warrants for physical computers are becoming less relevant in the face of rapid virtualisation.

Warrant authorisation lists

Under current legislation, ASIO must name individual officers on warrants who are approved to carry out that warrant. The proposal is that warrants be written with approved 'levels' of officer approved to carry out the warrant to make execution logistics simpler.

I don't have any concerns with the change.

Cooperation with the private sector

The ASIO Act currently allows ASIO to cooperate with other government departments (police etc) but is vague as to whether they can cooperate with private enterprise. The discussion paper wants to update the wording to make it clear ASIO can cooperate with private enterprise.

Again the discussion paper is unclear as to what 'cooperation with private enterprise' actually entails. In general, this does make sense. However, it needs to be clearly defined – we do not want a CISPA[3]-like scenario where private enterprise and ASIO are free to pass around information gathered on individuals. I believe this proposal needs much more detail before it can be supported one way or another.

Identification of ASIO officers

Under the ASIO act it is an offence to publish the identify of an ASIO officer, even if 'publishing' is referring that officer to the appropriate authorities (read, police) due to serious crimes. The discussion paper proposes changing this legislation to allow ASIO to refer known criminal activity by ASIO officers to the appropriate agency for prosecution.

This change seems like absolute commons sense and should have happened some time ago.

[3] Cyber Intelligence Sharing and Protection Act. A proposed United States act that was finally defeated after a lengthy public campaign of opposition by civil rights campaigners.

Third party computers and communications in transit

The discussion paper would like to enable warrants to authorise the use of third party computers and interception of communications in transit when accessing a target computer. The paper recognises that there are potential privacy concerns with this as it would almost always result in agencies gathering unrelated communications in the process.

In addition to the acknowledged privacy concerns, I am worried about the potential abuse of such powers in the form of 'fishing' trips. Potentially warrants could be crafted for a target in a manner to enable the interception of the communications of entire online communities from a single warrant. Unless more details are released, including strict controls over how such warrant powers would be used, I cannot support this proposal.

Ministerial authorisations

Current legislation places very strict controls over the ability of Australia's intelligence organisations (ASIO & ASIS) to gather intelligence on Australian citizens. One of the controls is a defined list of activities the target must be suspected of before approval can be granted. This list includes 'distributing WMDs, acting as an agent of a foreign power, etc. The discussion paper seeks to include one more item in that list; 'involved in intelligence / counter-intelligence activities.'

As far as I am concerned, adding this extra item to the list makes little difference. From my reading, it is essentially the same as 'active as an agent of a foreign power' but can cover working for non-nations (like terrorist organisations) as well.

Cooperation between agencies

When addressing specific threats and scenarios, cross-agency task forces are sometimes established. This can result in confusion where participating agencies operate under different rules. For instance, in a cross-agency task force featuring the AFP and ASIO, the AFP can gather intelligence on Australian citizens and ASIO cannot. The discussion paper proposes that for clarity, explicit rules be introduced such that the task force members operate under common rules. In the previous example, any ASIO officers working with the AFP on the task-force would be able to request search warrants as if they were AFP.

I don't have any concerns about this proposal.

Weapons training

Under the current acts, ASIS officers are trained in various weapons and exercises. However, they are expressly forbidden from cooperating with non-ASIS personnel in such training. The discussion paper proposes that this rule is relaxed to permit cross-agency training exercises. ASIS agents would

not receive training in any weapons or tactics they wouldn't have otherwise, they will just be allowed to take part in joint training exercises.

I don't have any concerns about this proposal.

Thank you for taking my submission into consideration during this important inquiry.

Respectfully,

Robert Batten.