Submission No 62

Inquiry into potential reforms of National Security Legislation

Name: J Trevaskis

Organisation: Private capacity

Submission to the Inquiry into Potential Reforms of National Security Legislation

Executive summary

Many of the potential “reforms” should be abandoned. The changes would be a significant infringement on the rights of the individual, and yet are largely without justification. The changes would take Australia in a dangerous direction.

The Discussion Paper's introduction talks about terrorism and “mass casualties” but in reality these changes will target much less serious crimes.

The introduction trumpets successes in thwarting planned terrorist attacks. However those successes were achieved with the current laws in place! Any suggestion that LEAs need more powers is entirely speculative.

The changes are only vaguely specified, making it difficult to know exactly what the implications are. Noone should agree to such vague proposals.

Neither safeguards nor privacy protection should be weakened in any way.

Comments on the Terms of Reference

Having regard to

Let me stop you right there. Why is there no regard to privacy? It is understood that Australians have no constitutional right to privacy and that any right to privacy established in legislation is likely to be overridden in other legislation. However Australians still have a legitimate aspiration to privacy and an inquiry should have regard to that.

Privacy *must* remain “front and centre” in any consideration of security legislation. There must be a presumption of privacy, with exceptions allowed only in limited, well-defined and justified circumstances – and where exceptions *are* allowed there must be robust safeguards in place to ensure that the letter and spirit of the legislation are being met.

'in camera' and classified hearings

This is in regard to Item 4 in the Terms of Reference. The extent to which this occurs should be at the absolute minimum. It is bad enough that the government would raise this set of proposals. Discussing the proposals in secret makes it even worse. Any secret consultations are unable to be challenged for correctness or self-interest.

Counterproductive

One of the difficulties with having an inquiry such as this one, and in particular in having proposed a number of highly invasive and highly controversial measures, is that it could be counterproductive.

- It highlights the powers that the authorities already have. People may be less tolerant of that existing level of invasiveness, the more they know about it.
- It encourages everyone, whether having committed a serious offence or not, to consider what they

might do to better protect their privacy. For example, it is obvious that both email and SMS (stored communications generally) are seriously flawed, in practice, from a privacy perspective.

- It encourages the development of even better technologies for the protection of privacy.

Discussion Paper structure

The Terms of Reference are nicely organised with 18 numbered proposals, further grouped according to the extent to which the government wishes to pursue these proposals. Why isn't the Discussion Paper structured to mirror the Terms of Reference? I apologise in advance if I have responded to text that is in the Discussion Paper under the wrong heading from the Terms of Reference.

Abbreviations

The *Telecommunications (Interception and Access) Act* is hereinafter referred to as the TIAA.

Comments on the proposals

A1 Strengthening privacy protection

Finetuning

I recommend the following amendments to the TIAA.

1. Remove the role of the AAT. That is, a warrant would have to be approved by a judge or magistrate – in a court.
2. Repeal 7(4), which allows interception without a warrant. It appears to be infrequently used and yet it is exactly the kind of “thin end of the wedge” that concerns me. (For example, there is no requirement in this subsection that the relevant party or any other party be *aware* that one of the parties to the communication is an officer of an agency.) A telephone application for a warrant should be used instead. In addition, if it's really so urgent that application cannot be made even by telephone, I would wonder how interception could be set up quickly enough. It is also dubious that an exception is made here merely on the grounds of possible self-harm, which is *not* an offence, let alone a serious offence.
3. In Section 5 the definition of “relevant statistics” should be amended to separate the accounting of “withdrawn” from that of “refused”.
4. Section 99 should be amended to tighten “as soon as practicable after each 30 June” to, for example, “by 30 September after each 30 June”.
5. Repeal 46(1)(d)(ii). It appears to be infrequently used. If a person is not involved then noone has any business intercepting that person's service. In most cases you would think that interception could occur on the service of the person who *is* involved.

Content or Substance

I recommend that Section 172 of the TIAA, or elsewhere, be clarified so that it is clear what “content or substance” of a communication means in the context of data network communication. (There may be implications and overlap with the *Telecommunications Act* regarding this proposed clarification of what “content or substance” means.)

I propose that in the context of data network communication, the IP address is *not* “content or substance” (and hence *is* telecommunications data) and that *all other* information that is transmitted or received by

the end user is “content or substance”.

More specifically, however, the legislation should use some term like “unique identifier of a device on the network”, rather than “IP address”, so as to avoid any explicit dependence on current technology. Alternatively, the legislation might use the existing term, “telecommunications number”, as defined in Section 5 of the TIAA.

Advantages of this definition are:

- It is simple and reasonably clear.
- It is objective.
- It can be automated.
- It is a sensible generalisation from the phone number as it applies to a phone service.
- It brings the internet into line with phone services.
- It is the one part of data network communication that cannot be encrypted and hence is always available.
- It should extend to future, as yet unknown, communication technology without legislative amendment since most likely any data communication technology will uniquely identify the sending and receiving device.

The important point here is that *all other* information that is transmitted on the data network *is* content or substance. In particular, URLs are content or substance. Hence IP addresses would be available by accessing (so-called) telecommunications data, in accordance with one part of the law, but in order to get more detail i.e. content and substance, a warrant for interception would be required, in accordance with another part of the law.

It is my understanding that the above proposal regarding “content or substance” is somewhat at odds with the current interpretation. For example, the Annual Report for FY11 regarding the TIAA says at 2.55 that telecommunications data can include:

> *… Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication*

There appear to be a number of flaws in this interpretation.

- It doesn't really define when a URL is telecommunications data and when a URL is content or substance.
- It is not possible to apply it automatically. Only a human being could guess whether a URL identifies content of a communication. That means that, under this definition, in order to protect privacy, privacy must be sacrificed. This is doublethink.
- Even a human being would struggle to make that determination in some cases. For example, in the URL http://gzjun3cc13.facebook.com/ does the first part of the host name (“gzjun3cc13”) identify content? It must be meaningful to the recipient. It may be meaningful to the sender. However it is unlikely that a third party could determine the answer.
- It is clearly not consistent with the general idea of protecting privacy, which is the stated intention of the TIAA. The set of URLs that a person requests is a private matter.

Another consideration is the “surprise factor”. A person may explicitly type a URL into the address bar of his or her web browser. It would come as something of a surprise for that person to learn that something explicitly typed by the user is not protected as “content”. (There is no reliable way for an interceptor to determine whether a URL was explicitly typed. However this point is just for illustration. I believe that URLs should be protected as “content” regardless of the mechanism that the user uses to access the URL.)

As a further illustration of the idea, imagine that I send an email to someone requesting her to send me some particular document. The person then emails me back a document. In that scenario, it is reasonably clear that the request for the document and the document coming back are *both* protected as “content or substance”. The current interpretation however could come to a different conclusion when the exact same scenario is carried out via the web rather than via email.

It would be even more difficult to assess whether an IP address identifies the content of a communication. (This is not quoted above but is included within the same text at 2.55 in the FY11 report on the TIAA.) It is difficult to propose a *realistic* example where an IP address would identify the content of a communication but equally I doubt very much that anyone could comply with this requirement. Most likely, if it is discovered that the IP address identifies the content of a communication then the law would already have been broken i.e. IP addresses revealed as telecommunications data when in fact the IP addresses were content or substance.

These difficulties and inconsistencies would be completely addressed by my proposal.

I would also like to see the term “content or substance” replaced by the term “content”. I don't see that “content” and “substance” are intended to be in any way different here.

Telecommunications data

Related to the previous, the term “telecommunications data” should be defined in the TIAA or elsewhere.

A2 Standardisation of warrant tests and thresholds

Section 5D of the TIAA is something of a dog's breakfast. I recommend replacing the entire section with just the content of 5D(2)(a) i.e. 7 or more years imprisonment or life. This provides an objective and relatively simple specification for what constitutes justification for an invasion of privacy via interception of telecommunications.

The same threshold should apply to access of stored communications i.e. 7 or more years imprisonment or life.

If this wholesale simplification of Section 5D is *not* adopted then I make the following recommendations.

1. Repeal 5D(1)(f). This is very broad and somewhat undermines the intent of this section which is to limit use of interception to specified serious offences.
2. Clarify 5D(2)(b) as to what is meant by “serious arson”, “serious fraud” and “serious loss to the revenue”. In the absence of specification here or somewhere else, these terms risk being circular i.e. “serious” is “serious”.
3. Clarify 5D(1)(a) as to the meaning of “an offence of a kind equivalent to murder”.
4. Amend 5D(2)(b)(iii) to clarify that the person must have had the intent to endanger safety and not just that the intent was to damage property and the consequence was endangerment.

A4 Cost-sharing framework

This is fairly vague. As a general principle, all costs reasonably incurred by industry in complying with lawful interception requests and in enabling that capability in the first place should be borne by society as a whole i.e. by taxpayers. Law enforcement is not a cost that should be borne by industry.

It is stated in the Introduction to Chapter 2 in the Discussion Paper that interception is a cost-effective tool for law enforcement authorities. It is also stated that it is becoming more difficult and by implication more costly. Pushing some of the cost onto industry does *not* make it more cost-effective nor maintain the current level of cost-effectiveness. This is complete bogo-nomics. It would be more transparent to ensure that the entire cost is borne by the LEAs (and hence ultimately borne by taxpayers). This will ensure that

any view of cost-effectiveness is an accurate one.

In addition, pushing cost onto industry, and thereby hiding the true cost, may encourage cost-inefficient law enforcement.

A5 Definition of 'computer'

The Discussion Paper makes reference to the possibility that “data is stored on a computer network”. There is no such thing as data that is stored on a computer network. Any device that stores data and makes it available is in some sense a computer. The network merely allows computers to communicate.

I don't see a problem with extending a warrant so that it can be issued in respect of all computers at particular premises.

I think there may be difficulties in having a warrant for all “computers connected to a particular network”. What a network includes and what its boundaries are is fairly difficult to specify. A court granting such a warrant would have no real way of knowing the extent of what it is authorising and whether the warrant is therefore appropriate or not.

In most cases “premises” would include the entire relevant network i.e. “computers on a particular premises” would cover it. If there are several known sites, a warrant for each site could be sought. In such a multi-site arrangement, part of the network of an ISP would almost certainly be involved. Is it anticipated that the warrant covers the ISP's network? If so, this would be a substantial expansion of power.

In the worst case of potential abuse by law enforcement, the internet is a network. Is it acceptable that a warrant could be issued for all computers connected to the internet?

What does “computers connected to a particular person” mean? I assume that “connected” is intended in a different sense. (This is an example of syllepsis.) Otherwise the text could be interpreted as a reference to some kind of cybernetic organism!

Assuming that “connected to a person” is intended to mean something like “associated with a person”, this notion of “connected” suffers from vagueness. Again, a court may be granting much more than it intends if the actual interpretation of “connected” is left to officers on site.

I recommend that expansion to allow a warrant for computers connected to a network or computers connected to a person be rejected.

A5 Variation of a warrant

This section in the Discussion Paper does not make clear who authorises the variation or how this occurs. If it is authorised by a court and it saves having to go over those parts of the warrant that have *not* changed then I don't have a problem with this.

Variation should *not* be permitted simply on the 'say so' of the Attorney General, after having been initially authorised in one form by the court. The Attorney General is a political appointment and does not have the required impartiality.

A5 Renewal of warrants

I think this proposal subverts the intention of the safeguards. A threat to security may indeed exist for several years but equally it may no longer exist. It is precisely for this reason that someone should have to justify the continuation of the warrant. While I am not opposed to some extension, there must be some strict limits, otherwise it is all too easy to keep renewing without ever having to justify the continuation.

Taking into account the suggestion that all warrants endure for 6 months, I suggest that a single renewal of 6 months be allowed i.e. a maximum of 1 year in total, after which a full rejustification and a new

warrant would be required.

B9 Ancillary service providers

This is a very concerning proposal. Do we really want a situation where everyone is spying on everyone? Any attempt to extend the reach of these laws to other entities (i.e. beyond carriers and CSPs) would be worrying. It appears to be a transparent grab for more power by law enforcement.

The Discussion Paper is relatively silent regarding the range of entities that would be covered.

Since any interception capability comes at a fixed cost, whether it is ever used or not, this will hurt smaller providers most.

What about not-for-profits?

What if the service is provided free?

Can an individual be an ancillary service provider?

What is a service?

What is a “telecommunications industry participant”? In its broadest sense it could be just about anyone who does anything on the internet.

While carriers and CSPs are more or less by definition domestically based, this would not apply to ancillary service providers. How does the government intend that this be enforceable on foreign ancillary service providers? How will a foreign ancillary service provider know that a demand for assistance is legitimate?

A foreign ancillary service provider would no doubt argue that if it agrees to cooperate with Australian law enforcement then it would have to agree to cooperate with law enforcement in every country. This would create a bureaucratic nightmare. No doubt every country would have different rules, procedures and conditions.

If foreign ancillary service providers are exempt, does this have the effect of disadvantaging domestic providers?

B9 Three-tiered model

The documents do not define what this means. What are the tiers? What are the implications at each tier?

This appears to be referring both to interception and to data retention. As noted in the previous section, interception and/or retention *capability* comes at a fixed cost, whether it is used or not.

B10 Authorised intelligence operations scheme

Some constraints should apply here.

- Whatever limitations are placed on it must be defined in *legislation*, so that any attempt to weaken limitations will be more evident.
- One such limitation should be that the specified conduct is only authorised in the context of the operation, not more generally.

Possibly both of these are as intended in this proposal.

Notwithstanding this, I have reservations about this general idea. Too much criminality can be corrupting.

B11 Computer tampering

There are probably good reasons for this prohibition.

- Any such tampering may alert the target. (In fact, in the world outside ASIO, we would all want tampering to be impossible. If tampering *is* possible, we would all want tampering to cause an alert. Contrast the suggestion here with the proposed requirements on ISPs to maintain the security of their infrastructure.)
- The target may even deliberately trigger some action when tampering is detected i.e. a tripwire.
- It may pollute evidence that would subsequently be used in court.

On balance the case has not been made for allowing ASIO to tamper with target computers.

B12 ASIO cooperation with the private sector

While I am not opposed to the clarification sought here, it would be important that *substantial* safeguards are in place. Experience has shown how private sector involvement can work against the public interest. Example scenarios could be:

- Private sector employees are not as well vetted as ASIO employees.
- Even if well vetted, the practical effect is to expand the pool of people who have access to unusual powers or who have access to certain information.
- By conducting activities at arms length from law enforcement, public and governmental scrutiny over law enforcement is reduced.
- Law enforcement may gain “deniability” about whether certain things have occurred and “blame shifting” when finally forced to admit that those things have occurred. There is a reduction in accountability by law enforcement for events and activities that occur in their name.
- Law enforcement can hide behind “contractual obligations” and “commercial-in-confidence”.
- The private sector entities involved may be foreign-located or foreign-owned or foreign-controlled such that in practice much of their activities are beyond the control of Australian law.

On balance, I do have reservations about this proposal and any steps in this direction should be cautious indeed.

B13 References by ASIO to law enforcement

It is arguable that ASIO is only granted extreme powers for the purposes of national security, and not for general law enforcement i.e. not for general spying on Australians. As such, it is appropriate that ASIO has some restrictions on what it can communicate to law enforcement. It seems to me that the definition of 'serious crime' being used here is wildly out of synch with the definition used in the TIAA. I recommend therefore that:

- the definition here be changed to match the TIAA (7 or more years imprisonment or life). It is important that ASIO *not* be involved in general law enforcement and it is important that that be the public perception.
- the actual proposal – that an offence of publishing the identity of an ASIO officer can be referred to law enforcement – be rejected. In the internet era it is becoming less practical to control the flow of information. If the identity of an ASIO officer becomes known then failure has already occurred. It will not likely be possible to prevent that information being published, whether Section 92 exists or is strengthened or not. ASIO should concentrate on keeping the identity of its officers secret! (Someone might point out though that this same argument applies to the restrictions in Section 18 too. That is, those restrictions are yet another attempt to control the flow of information, which would be easily subverted via the internet, in this case subverted by ASIO.)

C14 Expanding the basis of interception

The Discussion Paper does not appear to define this at all. It can hardly be said that public consultation has occurred when the sum total of information about the proposal is “expanding the basis of interception activities”. It is too vague for anyone to agree with. On the face of it though, it sounds like a bad thing – reducing everyone's privacy.

C15 Failure to assist in decryption

This is not clearly defined. I can envisage three ways in which this might apply. (There may be others.) I urge rejection of this proposal.

1. A company provides an encryption product and law enforcement wants that company's assistance.

There are several points to be made about this.

- It is extremely doubtful that law enforcement *should* have the power to compel that assistance.
- The company may be, and most likely is, a foreign company. So the same issues as noted in “B9 Ancillary service providers” arise.
- The company will rightly be reluctant to expose its intellectual property. (Government should encourage open source encryption products though because then this item largely goes away.)
- If the company were aware of any security weaknesses in its product then it should fix the weakness and then reveal its existence – or withdraw the product. It would be unethical for it to sell a flawed product, and potentially illegal to do so.

2. An individual or company has expertise in encryption technology and law enforcement wants assistance.

It is extremely doubtful that law enforcement should have the power to compel that assistance.

At the very least, questions would arise as to whether this is slavery or what compensation regime would apply. It is also somewhat doubtful that expert assistance from a third party who is compelled to provide it would be very useful.

3. In the context of the investigation of a serious offence, either the target of the investigation or some other party has “secret information” (typically a decryption key or password or passphrase) that would assist in decryption – and law enforcement wants to compel that party to reveal that secret information. Some issues raised by that possibility are:

- This may be tantamount to self-incrimination.
- It tramples on a person's right to remain silent.
- It would seem to be very difficult to prove that the person is actually in possession of that secret information. The difficulty of proving this should not be used as an excuse to reverse the onus of proof.
- There are already technologies available to counter this. See “rubber hose cryptanalysis” and hence “deniable encryption”.
- It raises issues of identity theft. It may be that revealing that secret information does much more than assist encryption but in fact allows a person's digital identity to be stolen. This would then bring into question the validity of any digitally signed documents. Similar considerations could apply to any digitally signed communications. (This may not yet be a major issue because I suspect that most people are not using this kind of technology today.)

It has also been reported that the NSA has broken the encryption systems typically in use. If that is accurate, there should be no need for assistance from individuals or companies, and this specific proposal

can be abandoned immediately on the grounds that it is unnecessary.

C15 Data retention

This is one of the most controversial of the proposals. Does any government, any parliament, want to be the one that legislates Big Brother into existence? The idea that telecommunications information will be recorded and retained for every single Australian just in case that person commits a serious offence some time in the next 2 years should be *abhorrent* to anyone committed to a free society.

This proposal is vague in that it does not explain what “tailored” means, or how “up to 2 years” will translate into actual time frames, or whether it applies to stored communications or telecommunications or both, or what details will be required to be recorded.

There is insufficient detail provided to know whether this is actually practical. However even if it were practical, government should step back from the abyss. Just don't do it! Appendix A in this submission contains some discussion of practicality.

I suggest that this measure would not be as effective as law enforcement thinks it would be. For example,

- A person who intended to communicate something about a serious offence on the internet could generate “millions” of dummy exchanges on the internet. While those exchanges would all be recorded and available to law enforcement, the person could die of old age before the last exchange had been checked out by law enforcement.
- Every person who objected to the data retention proposal on principle could generate “millions” of dummy exchanges on the internet thereby making the data retention mechanism itself less practical. (Both this item and the previous are likely to become more problematic with the advent of the NBN, offering much higher bandwidths, higher quotas or both.)
- Data retention for stored communications that are email can be avoided by anyone merely by not using the ISP for email. This is to be recommended anyway because anyone who uses their ISP's email address then finds it more difficult to change ISP. That is, national economic efficiency says that people should not use an email address provided by their ISP. (Hence, for example, if a person used the gmail.com web site for all their email needs, the ISP would never see a single email. It is true that the web traffic to gmail.com instead would be seen by the ISP but that raises a number of practical difficulties for “data retention” as compared with simply keeping copies of emails that are being handled by the ISP.)
- Use of an HTTP proxy may conceal the true destination of a web request.
- Use of encryption, in forms such as SSL or VPN, by ISP customers could limit how much useful information is present within the data retention archive anyway.
- There are other reasons that I forbear to mention here because it is not in anyone's interest to do so. (For example, the above techniques have already been published or are already sufficiently well known, but there are other less well-known techniques.)

There are good reasons to believe that anyone who *has* committed a serious offence is less likely to have their privacy breached than the vast majority of Australians, who are law-abiding citizens. What's wrong with this picture?

The suggestion has also been made that such a treasure trove of information would be an irresistible target for abuse (if its stated purpose is not abuse enough).

C16 Industry obligations regarding security

I reject the suggestion that the regulatory environment should be formalised to give government a role in managing ISPs regarding security. Is there any evidence that ISPs are deliberately ignoring security? Is

there any evidence that a cooperative approach wouldn't work? Has it been tried?

It is nonsensical to think that an ISP would not itself act if its infrastructure has been compromised in a significant way – and if it does fail to act, it is doubtful whether legal sanctions will make any difference.

Availability is the major concern here. However it is far from clear that government can tell ISPs things that they don't already know about availability and security i.e. that government can do a better job. If government is aware of information that it thinks that ISPs are not aware of, there is nothing stopping government communicating that information to ISPs. Whether an ISP should be legally obliged to act on the information is then the crux of the question. In my view, the case has not been made that an ISP should be so compelled.

It is not necessary to place any legal burden on an ISP to protect the confidentiality and integrity of communications passing over its network. That responsibility lies with the choices that the end user makes. If the end user chooses not to use a secure protocol then the end user has chosen not to have any guarantee of confidentiality or integrity. The choice of and management of ISP network infrastructure makes no difference to that. A secure protocol chosen by the end user is not affected by even compromised network infrastructure as far as confidentiality and integrity go.

This is not to say that an ISP is permitted to compromise confidentiality or integrity *deliberately*, only that if it happens by accident or by malicious action of a third party, it is not something that should result in punishment of the ISP. For the most part, if an ISP were involved in *deliberate* compromise of confidentiality then this would already be illegal.

One way in which Australia's telecommunications infrastructure can be kept robust is by encouraging diversity, diversity both in the number of providers and in the nature of the infrastructure used by those providers. Hence, for example, if a serious security issue arises in some make and model of equipment, only those providers using that equipment are affected, and for example if an entire ISP is affected by a serious security issue, other ISPs may be isolated from it and unaffected.

As such, government should ensure that its policies encourage rather than discourage diversity. The introduction of the NBN is probably going to act to reduce the robustness of Australia's telecommunications infrastructure, by reducing diversity.

The proposal has been put up that ISPs should be obliged to provide information to government so that national security risks can be assessed by government. I don't see that the case has been made for this but make the following two observations, which observations are intended to be independent of each other.

- This could be limited to those parts of the telecommunications infrastructure that connect directly to other countries. This would limit the number of affected ISPs and limit the amount of information.
- This could be addressed within an industry forum, independent of government.

Another difficulty with the proposal is that the Discussion Paper observes that Australia is in the process of refashioning its telecommunications infrastructure via the NBN and yet this would imply to a large extent that no new laws are required that will oblige cooperation. The government owns NBN Co and can already direct it to act in certain ways. An example would be the “Huawei ban”.

If the NBN were sold off at some time in the future then most likely legislation would be required merely to enable that sale and that would be a time to revisit this question.

On the subject of Huawei, it is doubtful whether anyone can absolutely guarantee the security of *any* maker's network equipment. Cisco is a well-known and reputable brand but do you know for sure that Cisco equipment does not have a backdoor for the NSA? Do you know for sure that Cisco equipment does not have a backdoor for the *Chinese*?

If you want this level of guarantee then may I suggest that you encourage the development and adoption of open source network equipment.

However network equipment is the tip of the iceberg. The vast majority of Australian businesses and households, as well as all levels of government, use a certain operating system that every month demonstrates how insecure it is. A widespread outbreak of some nasty malware could do far worse than take out telecommunications infrastructure. If government is concerned about national security risks that arise out of technology, it is probably looking in the wrong place.

Again, diversity and open source could be two aspects of improving Australia's overall robustness regarding security risks that arise out of technology.

C17 Third party computers

This should be rejected. This would mean involving computers owned by people who are suspected of nothing.

It also raises the issue of what happens if the third party detects what is going on. The third party is unlikely to be aware of the ASIO operation. The third party may deliberately or unintentionally reveal details of it, or interfere with it. The third party, thinking his system is under attack, may actively take countermeasures. Will the third party be indemnified for any of this?

If the third party becomes aware of what is going on is the third party obliged to consent to the intrusion? (“obliged to consent” is an oxymoron. I hope you understand what I mean.)

C17 Reasonable force

It is asserted in the Discussion Paper that this is a “drafting anomaly”. It is for parliament to determine that. Perhaps it really was parliament's intention that reasonable force can be used for entry but not for subsequent purposes i.e. not an anomaly at all.

Is there any evidence that there is an actual problem? Are the courts interpreting these subsections to imply a limitation? If no, then no change is required. If yes, then this extension of power should be justified.

C18 Ministerial authorisations

Anything that allows a minister of the crown to act without the legal authority of a court, merely on the grounds of a judgement about what is “likely to be” should give rise to apprehension. In particular, one would have to consider the potential for political considerations to influence a decision of the minister.

The existing grounds of “acting for, or on behalf of, a foreign power” or “activities that are, or any likely to be, a threat to security” may already cover the proposed additional grounds. The case has not been made for why more power is needed.

Appendix A Data Retention storage estimate

The Discussion Paper states that in the June 2011 quarter, Australians downloaded 274202 TB from fixed internet services. Suppose that legislation required Australian ISPs to record for every packet, the source IP address, destination IP address, a timestamp and some identification of the internet service involved. For concreteness I have taken each of these to be 4 byte values.

Furthermore, the Discussion Paper states that for mobile handsets the download figure is 3695 TB. Suppose that legislation additionally required a latitude and longitude value to be recorded in the case of a mobile internet service. For concreteness I have taken each of these to be 4 byte values (even though the resulting implied precision is probably beyond current position estimation technologies).

I have assumed an average packet size of 600 bytes but concede that the exact figure is debatable.

Crunching the numbers gives 81 TB per day. Let's take a typical hard disk size as 1 TB. So that's 81 disks per day or, equivalently, a disk every 17 minutes. (That is for the whole of Australia based on the June 2011 figures.)

There are reasons to treat this an underestimate.

- If the quoted traffic figures are for download only, not upload also, then upload is missing. It seems unlikely that law enforcement would be happy to see only data for received packets and to miss out on data for sent packets. If legislation requires upload to be recorded too then the estimate goes up. (When downloading, the upload volume is much smaller but so are the packets.) I don't have adequate data to estimate the increase caused by including upload data.
- All hardware is subject to failure. With this many disks, disk failure would be frequent. So disk storage redundancy would be needed. Let's suppose a RAID set with 3 data disks plus one parity disk i.e. a 33% increase in number of disks required. This gives 109 disks per day or, equivalently, a disk every 13 minutes.

However it gets worse. Eventually Australia and the world will no longer be able to put off migrating from IPv4 to IPv6. IPv6 has 16 byte IP addresses i.e. an IPv6 IP address occupies 4 times the space of an IPv4 IP address. A complete migration to IPv6 would mean **270 disks per day or, equivalently, a disk every 5 minutes**. (Some Australian ISPs are already offering IPv6 services to customers.)

Even this understates the practical difficulty. Is anyone ever going to use this data? If so, finding relevant data would either be a complete nightmare or even more storage, and performance, could be required in order to index the data in some way.

For example, given a service id, finding information about all packets received by that internet service in the last 2 years would involve examining over 59,000 disks (TB) of telecommunications data (IPv4) or over 148,000 disks (TB) of telecommunications data (IPv6) – unless the data is indexed. (Things are not quite as bad as this because a service id is presumably already known to apply to a specific ISP and it is *assumed* that the data from ISPs will not be aggregated. In that regard, the larger the ISP, the closer it comes to the figures in this paragraph, in proportion to the ISP's share of traffic.)

Naturally, if the legislation requires some part of or all of the *content* to be recorded too then volumes will balloon further.

There are some technical reasons why the above analysis may overstate the storage requirements (there are tricks that will reduce the storage required but usually at the cost of making it run more slowly) but I expect these would be eaten into by the ever-increasing volume of data that Australians download. Any trend away from fixed service to mobile service would also work to increase the Data Retention storage requirement. Changes in user behaviour *caused by* Data Retention should also be taken into account.

It is difficult to avoid the conclusion that data retention applied to all data network communications is not practical.

This analysis has focused so far only on data network communications, not stored communications. If the legislation applied only to stored communications then the number of messages may well be much lower, but I can imagine that law enforcement would want much more information about each message. For example, for email, law enforcement might want the sender email address and recipient email addresses and subject. In any case, retention of stored communications, in the case of email, is too easy for anyone to bypass.

Government might also want to consider that a substantial fraction of all email is never delivered – usually because it is spam. (Estimates are that about 80%-90% of all email is spam.) There is no way in the world that government should contemplate the data retention proposal but if it did, I would suggest that only email that is actually delivered should be in scope. Email that the ISP knows that it is not delivering, either inbound or outbound, should be out of scope.