Submission No 97

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Daniel Black

Dear Parliamentary Joint Committee on Intelligence and Security,

Thank you for the reasonable length of time this inquiry was kept open for public submission.

The main point of my submission is on the large scale privacy breaches risked by the proposal mandatory data retention by ISPs and refining the models under which industry assistance can be meaningfully provided to assist law enforcement.

The following is my input on the items under review:

1. Strengthening the safeguards and privacy protections in the TIA Act:

a. the legislation's privacy protection objective

Record keeping, retention and destruction are the key procedures that ensure the privacy of those who have had their communications intercepted by justifications under the law and this should not be compromised. Their rigorous nature reflects their sensitivity especially in comparison to other information possessed by agencies. Agencies that do not have the means to effectively manage the privacy of interception should rely on specialist agencies like AFP and ASIO to extract related material to the offence with the assistance of the enforcement/intelligence agency. The extracted material will relate in a way that high sensitivity and limited distributed material is handled within an agency under the PSPF and indeed shared between agencies.

b. the proportionality tests for issuing of warrants

The general 7 year rule I believe is too high as the the number of exemptions to the 7 year rule. A simplified 5 year rule with a subclause that interception may also be permitted to where there are 3 or more offences carrying a minimum imprisonment of at least 3 years. If there are social expectations for severe classes of penalty then the penalty should be meet the minimum requirements.

For offences that can only be prosecuted with warrants (computer and network offences) need to be closer examined as network capture at the victim end is possible.

c. mandatory record-keeping standards and d. oversight arrangements by the Commonwealth and State Ombudsmen

I recognise the need for reform as described in the discussion paper and think that the Commonwealth and State Ombudsmen are best equipped to define the framework of reporting on privacy verses public outcomes and tailor these for the agencies involved in telecommunications interception.

2.Reforming the lawful access to communications regime. This would include:

a. reducing the number of agencies eligible to access communications information

Consistent with my views in 1a above I agree that reducing access to raw intercept should be limited and those agencies like AFP and ASIO should have a role distributing extracted communications to agencies.

b. the standardisation of warrant tests and thresholds

Consistent with my views in 1b above I have proposed some ideas related to standardisation.

3.Streamlining and reducing complexity in the lawful access to communications regime. This would include:

a. simplifying the information sharing provisions that allow agencies to cooperate

My views in 1a above support of sharing under the condition that information is shared and not unfiltered raw intercept.

b. removing legislative duplication

I agree with the sentiment of simplifying the nature and criteria associated with TIA warrants however the discussion paper did not lend itself to any substantial recommendation that could result in a meaningful discussion.

4.Modernising the TIA Act's cost sharing framework to:

a. align industry interception assistance with industry regulatory policy

The push of development of intercept capability costs on to C/CSPs creates a disincentive for agencies to economise of the intercept capability actually required. Without a significant cost contribution by the agencies there could be the incentive for the agency to impose a high capability and capacity requirements in well in excess of the requirements of the agencies and well out of the bounds of the C/CSP to afford.

To alleviate these pressures agencies should treat the acquisition of intercept like a service acquisition off an C/CSP and pay appropriately for the capacity and service received.

b. clarify ACMA's regulatory and enforcement role

I concur the the need for reform to allow non-court enforcement of C/CSPs failing to deliver on warrant demands.

5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions

a. to update the definition of 'computer' in section 25A

I support these changes.

b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.

I support these changes.

6. Modernising ASIO Act employment provisions by....

I have no opinion of these changes.

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

I have no opinion of these changes.

8. Streamlining and reducing complexity in the lawful access to communications regime

- this would include:

a. Creating a single warrant with multiple TI powers

I think this is a good idea however without details there can be no meaningful discussion.

9. Modernising the Industry assistance framework –

a. Implement detailed requirements for industry interception obligations

It seems a stronger relationship with C/CSPs is needed to negotiate the capability and capacity required.

b. extend the regulatory regime to ancillary service providers not currently covered by the legislation

I concur with this reform.

c. implement a three-tiered industry participation model

I concur with the sentiment of this reform.

10. Amending the ASIO Act to create an authorised intelligence operations scheme. ...

I concur with this reform. It has worked well for many AFP operations.

11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.

I concur with this change.

b. Align surveillance device provisions with the Surveillance Devices Act 2007

I concur with this change.

c. Enable the disruption of a target computer for the purposes of a computer access warrant

I concur with this change.

d. Enable person searches to be undertaken independently of a premises search

I concur with this change.

e. Establish classes of persons able to execute warrants

I concur with this change.

12. Clarifying ASIO's ability to cooperate with the private sector.

I concur with this change.

13. Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.

I concur with this change.

14. Reforming the Lawful Access Regime

a. expanding the basis of interception activities

Consistent my views in 1b) earlier

15. Modernising the Industry assistance framework

a. establish an offence for failure to assist in the decryption of communications

Decryption is not a skill of the telecommunications industry. If a cryptographic occurs it is based on the clients action and the decryption capability is solely with the parties concended. If decryption is required DSD is already authorized and capable as per ISA section 5(e) "to provide assistance to Commonwealth and State authorities in relation to: (i) cryptography, and communication and computer technologies".

b. institute industry response timelines

This needs to be carefully considered that agencies are funding the capability and capacity for interception and not exceeding it. If they are it would be unjust to levy industry penalty.

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

Privacy impacts:

Even the most basic level of metadata retention, who's talking to who and when, exposes end users up to socially engineering attacks like a message to the client saying "with regard to your NAB transaction at 09:33:22 we require additional verification. Please phone 130022224444 to conform that this was you making the transaction" with knowledge that the bank and the time of transaction are 100% correct.

C/CSP do not have sufficient skill level to protect stored data as indicated by the recent compromise of AAPT (http://www.databreaches.net/?p=24899), and the loss by Telstra (http://www.databreaches.net/?p=24620). With some of the larger companies like Yahoo (http://news.cnet.com/8301-1009_3-57471299-83/top-domains-and-passwords-compromised-by-yahoo-breach/?tag=txt;title) and Sony's Playstation Network (http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity) having trouble protecting information critical to their business it is unlikely that ISP will be able to protect any volume of intercept that is so valuable in the criminal Internet.

Two years and an extraordinary length of time to have potential evidence collected about you without action. This length of time would create risk for the potential defendant to forget legitimate legal reasons to explain any evidence presented in network traffic like: had visitors, wireless was unsecured for a while etc.

Metadata of the last 6 weeks is a more realistic length of time however I still believe there is far too much risk and not enough benefit.

Cost Impacts:

The raw hard disks storage costs for the most basic of traffic data recording, consumer talked to X network address at this time (second accuracy), would be costing at the very minimium $4 million per 2 years at 2011 volumes (calculations included later). For any full capture of data a cost of at least $500 million per 2 years. This does not even include the cost of the storage arrays that write to the disks, or the automation to rotate several disks every few hours or the associated network infrastructure, or the physical storage and security costs.

The volume of a full intercept of all users will exceed the capacity of modern hardware to capture.

The rate of increase of anticipated network usage exceeds the growth in the storage industry capability to produce larger storage devices. Therefore frequent and significant architecture changes will need to occur to implement such a collection system.

Telecommunications Act 1997

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:

a. by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference

The Australian telecommunication industry manages hundreds of thousands of kilometres of infrastructure that cannot be physically protected to a level that prevents unauthorised interference in any form ranging from a malicious person performing an illegal interception, to a tench digger cutting a Perth to Adelaide trunk. (more below)

b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs

Private industry values the privacy of its business and procurement decisions as much as the government values its "information about the national security environment". Instituting obligations in legislation is a crude mechanisms and shows the government to industry relationship is broken that these meaningful private dialogues are not taking place to the level required. I'd suggest there is an extreme disconnect with the industry resonating in even in this discussion paper, and the Internet filtering proposals of this and previous governments. I'd recommend against any form of obligation here and that significant steps occur to remeditate this relationship.

c. Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers

This again is largely a relationship issue for the government. Also the majority of security risks are outside the responsibility of telecommunication providers. Social service providers have some risk however this should be controlled by the Privacy Act.

d. Creating appropriate enforcement powers and pecuniary penalties

Regulation around privacy protection should stem from the Privacy Act.

National Security risks should be managed by not relying on C/CSPs to protect network confidentiality and integrity.

Attached is a more detailed discussion of the reforms of the industry and some measures of

costing for large scale ISP retention.

TELECOMMUNICATIONS SECURITY SECTOR REFORM

The discussion paper of telecommunications security sector reform complicates the relationship between the telecommunications industry, national security and privacy because:
a) continual lack of specification of to the meaning of 'security' which implicitly means different things at different times; and
b) the lack of specificity of "data on their networks" could mean in a TIA framework the customer's data that is currently in transit under direction of the customer or the information about the customer stored on the carrier service provider's network.

Assuming that the "information about the customer stored on the CSP's network" definition:

The expectation of confidentiality on customer information is justified as is the protection of temporary stored items just as email and data about a customer like billing. Currently the proposed amendments to the Privacy Act under consideration by the current government seem wanting to achieve a similar goal as the 16.a of the terms of reference ("by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference").

It seems like proposals in this area are going to duplicate Privacy Act changes and regulations and therefore should be deferred from being included in the Telecommunication Act.

Assuming that the "customer's data that is currently in transit" meaning is intended:

The critical understanding required is that **the telecommunications industry provides, for the most part, a temporary transit of information for its clients.** This industry is very capable of ensuring the availability of networks that are resilient to a variety of influences as that is what their business model drives them to achieve. A wide spread outage is the only national security threat to the services provided by the telecommunications industry and it is precisely the aspect that industry is best capable of mitigating.

Referring to the discussion paper:

> "Australian citizens, businesses and public entities rely on telecommunication carriers and
> carriage service providers (C/CSPs) to handle information and data on their networks, including customer information, securely."

The expectation of security about "data on their network" referring to anything more than reliable transit of information then the customers expectation is an unrealistic expectation not supported by any contract, law, or carrier provided marketing or disclose. The TIA act prohibits unwarranted interception however there is little a provider can do to prevent unwarranted interception. To protect the confidentiality telecommunications providers would either be required to physically secure the hundreds of thousands of kilometres of the network from being physically accessed, to logically protect the supply chain of carrier grade network equipment and provide encryption between millions of end points. For the current price of telecommunication services across a vast country like Australia this simply isn't possible.

The only way a telecommunications provider incurs a significantly confidentially risk is if a government requires them to retain large quantities of personal data.

For the last 5+ years consumers have been exposed to proposals about Internet filtering, child safety, and ISP iCode to the extent that there is an implicit expectation that ISPs can just make the Internet safe. This approach has significantly damaged the consumers' responsibility to look after their own security. Going further down the regulatory approach with ISPs is going to further erode the consumer's responsibility for their personal information.

If clients of telecommunications providers require confidential or integrity of transfer of data over a network they either implement encryption at the gateway between their infrastructure and the telecommunications providers or acquire specific service off the telecommunications provider.

The communication end points outside the carriers control being the the web sites, Internet services and the authenticated users of these services are susceptible to cyber espionage threats. The responsibly for defence and risk management is entirely within the realm of the telecommunication's customer. If the customer requires a level of availability from the telecommunications provider then they will need to acquire the level of service required to ensure this availability. The responsibility the integrity and confidentiality of services is the customer's and that of the professional services and software that the customer acquires to defend itself.

The discussion paper states:

> Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual
> Australians.

Unless there is a security risk assessment that suggests the availability of a C/CSP is the direct target of a national threat actor this assertion is flawed. An unavailable network will only seriously affect a provider and the clients that failed to adequately acquire redundant networks. The attribution of a cause to a capable attack is usually sufficient to mitigate any medium to long term negative image about the consequences of outage. As seen from the security compromises of Telstra and Sony this year it can been that there is only moderate period of news reporting before it dies down. Compromises of large companies are happening so regularly that they are

rarely attracting significant long term loss of good will.

To look at the objectives of the framework:

- government and industry have a productive partnership for managing national security risks to Australia's telecommunications infrastructure,

While this is important the much more important aspect, which is currently outside the scope of this enquiry and not as I'm aware being actively considered is the responsibility of the software manufacturers to produce unbroken software. Software that needs security patches was undoubtedly sold to the consumer in a broken form. This broken software then becomes infected with malware and then through the spread of virus, botnets etc becomes a threat nationally an internationally to the sustainability of internet services.

- security risks relating to Australia's telecommunications infrastructure are identified early, allowing normal business operations to proceed where there are no security concerns and facilitating expedient resolution of security concerns,

Assigning security responsibility beyond availability to telecommunication industry will drive costs to consumers greater and not achieve a significant outcomes as most security risks are the responsibility of the users of telecommunication services.

- security outcomes are achieved that give government, business and the public confidence in their use of telecommunications infrastructure for both routine and sensitive activities,

Confidence can only be achieved by realising that security can only be implemented at telecommunication end points and focusing a variety of regulatory, social awareness and legal responsibility mechanisms to ensure this happens. Some of this is happening with proposed Privacy Act amendments however software manufacturers and to a lesser extent IT professionals are still left to produce "no warranty" products and services.

- the protection of information, including customer information and information about customers, contained on or transmitted across telecommunications networks is better assured, and

The protection of customer information and information about customers is potentially handled best under the proposed Privacy Act amendments rather than introducing duplicate legislation. The confidentiality and integrity aspects of security on transmitted communications cannot be achieved without a massive cost to the industry that can only be passed onto consumers.

- compliance costs for industry are minimised.

Privacy Act amendments should drive the incentive for the industry to protect its holding of stored customer data.

The cost model proposed in the discussion paper seems to be imposing on ISPs to economise on the solution to telecommunications interception capability without the government agencies being required to economise on the capability that they require. To alleviate this imbalance government agencies need to significantly fund the capability and capacity they require to deliver the service expected of them.

The cost of interception capability imposed also has a moderate to significant effect on business viability especially for small ISPs. The proposed teiring model seems a reasonable way of achieving this however care must be taken to ensure that smaller ISPs are still viable. The merger of larger ISPs like iiNet, Internode, TransACT to name a few seems to indicated that this may not be the case. The reduction of ISPs to a duopoly will only detriment consumer prices.

There are also significant risks in imposing penalties for late delivery in 15b. The operating costs may be agency borne of a non-profit/non-loss basis however this leads to the provision of staff that have the capacity to deliver a volume of interception assistance. A ISP could quite easily become over capacity during a peak time and suffer that penalty costs while the intercepted assistance covering costs cannot deliver additional trained staff in a timely manner to assist.

15 Modernising the TIA Act's cost sharing framework – measuring data retention

To assess the privacy impact lets for a start consider what the minimal possible data retention. This would include a timestamp of the traffic and the network address of the remote service. This is the most basic traffic data excluding content available.

The traffic volumes in the discussion paper indicate the volume of 274,202 terabytes a quarter in June 2011. As the wired and wireless communications very commonly enforce a 1500 byte limit or slightly less on each packet of data and if we roughly assume that an average packet of data is about 600 bytes. An IPv4 address is 4 bytes long and the information to store a second accurate measurement when the data was transmitted is also 4 bytes long. So volume of storage of internet traffic for data retention on the Australian people is (4 + 4) / 600 * 273202 TB (June 2011 as per discussion paper) which is 3642 TB of data per quarter. At a disk cost of $143 (rough price for consumer grade disks) per 2 TB and an absolute minimum of 2 disks being required to maintain redundancy brings the cost to $520806 per quarter. This does not even include the cost of the hardware chassis, network equipment or storage security to obtain the interception.

With IPv6 the address is 16 bytes long so the cost is going to increase as its assured growth continues. IPv6 will become the preference once the end users device and the server support this so here we anticipate eventually (up to ~5 years) up to a 4 fold increase in these volumes and costs.

A more realistic traffic data excluding content would be the full IPv6 and TCP header which is 40 bytes (or 60 for IPv6) so here we're looking at $5 to 7.5 million dollars in disk storage per quarter and this still isn't sufficient to look at which URLs are being used. In the case of shared hosting, more that one website on an IP address we can't even resolve which one it is accessing.

A full data retention is about $40–80 million dollars per quarter on disk alone based on 2011 figures.

Given the growth of 76% over the June quarter from 2010 to 2011 and the advent on the NBN we can only assume this will increase again. These even the current increases are greater than the growth of disk capacity and probably other storage capacities the interception capability therefore need a redesign every year or two.