# Submission No 157

## Inquiry into potential reforms of National Security Legislation

**Organisation:** Mr Daniel Judge

**Daniel Judge**

**20 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**: **Submission**

## Introduction

Firstly, thank you for the opportunity to make a submission in regards to this important issue, which has wide ramifications for Australian society, culture and democracy.

Due to the very limited time in which to prepare a submission I would like to point out that this submission is not as detailed as I feel the issues warrant and that not every point in the Terms of Reference (ToR) is addressed. While a number of elements in the ToR are related to minor administrative efficiency changes, to which I have no objection and in some cases support, my act of not addressing a particular point of the ToR in this submission should not necessarily be viewed as an endorsement of that point.

Of particular concern in the ToR are the provisions labeled:

- 15.A Establish an offence for failure to assist in the decryption of communications
- 15.C Mandatory data retention for 2 years.

These are, I feel, the most egregiously dangerous items in the ToR and, as detailed below, I am opposed to these items for a range of reasons.

My views in this submission are my own personal opinions and should not be taken as representative of any organisation or entity that I am employed by or a member of. I am a father of three children and have been employed for 12 years in the field of IT at an Australian University where I have also completed a Bachelor of Internet Science and Technology. Prior to that I worked as a public servant with the Commonwealth Employment Service.

It is my fervent hope that the committee considers my submission as well as those of other members of the Australian public favourably, and that this process assists in letting the committee come to a decision that protects the civil liberties and privacy of the Australian people from some of the more outlandish examples of the security services overreaching in their desire to protect Australia from threats, both real and perceived.

*Items in the Terms of Reference which I do not address have been excluded from the below for the sake of clarity and brevity. This is not necessarily to be construed by default as support or agreement with those excluded items, however many of those items are seemingly innocuous and of a minor administrative nature which I do have no opposition to, at least if they are taken at face value.*

**A - Government wishes to progress the following proposals:**

*Telecommunications (Interception and Access) Act 1979*

**2. Reforming the lawful access to communications regime.**

**b. The standardisation of warrant tests and thresholds**

While technological changes have made it more difficult to clearly define the difference between stored and real-time communications, simply equating them and arbitrarily assigning them both to the same low-threshold standard for interception appears to be an overly simplistic response to this issue.

Fundamentally the wider ranging implications for lowering the standards of intruding upon people's private communications and activities need to be taken into account. If anything, the changing nature of digital communications technology means that communication that ends up being stored is, in practice, utilised by people in the same manner that real time communications were in the past.

The increased use of SMS, instant messaging and social media means that many people now use a communications medium where the content of those messages can be stored, yet people use them to communicate in a manner more akin to the way people used a non-stored medium in the past. On an anecdotal level I find that a lot of people are unaware of the extent that logging occurs behind the scenes in chat services, instant messaging and social media and thus are not a consciously aware that services which they treat as a 'real-time' medium is actually being stored somewhere.

In light of the above, coupled with the original justification for the original separation between the two type of communication, it could be argued then that, if anything, the bar should be raised higher and that it should be the stored communications that should be raised to a 7year penalty threshold. However, this too would be an oversimplification and, perhaps a more detailed and thought out solution is instead needed to solve this problem. The discussion paper does point out investigations related to child protection as an example where the current framework falls short of expectations. So as to properly address such concerns in a manner that finds the best balance perhaps this element should remain at the status quo in the short term, with planned changes addressed in a separate inquiry or community consultation process to better come up with a solution that both gives law enforcement the tools needed to investigate crimes in the manner the community expects of them, while not simply oversimplifying the framework in a way that could open up privacy concerns for a slew of crimes that may not warrant unleashing such intrusive investigative tools upon so many people.

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

**a. Simplifying the information sharing provisions that allow agencies to cooperate**

The discussion paper states:

> "The requirements are aimed at ensuring that agencies keep appropriate records necessary to demonstrate that agencies are using their powers lawfully. However, many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate." (p 26)

I am wary of any attempt to justify a change that relies upon an argument that implies that concern about "corruption" and "misuse of powers" is an historical artifact. Corruption is always an ongoing concern, especially since the effects of corruption, when and where it does exist, can be such a negative force upon peoples lives. When these effects can often result from an associated "abuse of power" a healthy fear of and vigilance against corruption should be ever-present. While associated comments in regard to this section about recording the proportionality of intrusive powers would be a welcome addition to existing procedures, I would remain very opposed to any amendment that reduces record keeping and potential audit trails of such power usage overall as this could negatively impact the ability of investigations into corruption and power abuses to acquire an accurate picture of actual actions and events.

*Australian Security Intelligence Organisation Act 1979*

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

**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.**

It is my belief that there should be judicial oversight to any warrants or warrant changes as the separation of powers in a democratic government is essential to the health of that democracy.

As the Attorney-General is a partisan position the potential for future abuses by this provision are a danger that must be avoided. A system of judicial checks and balances is essential. There is a reason warrants are not a "streamlined" process, and while we have been fortunate in Australia in having a reasonably democratic government and society, allowing the implementation of a system that opens up avenues for abuse just because 'we've been mostly lucky so far' is not something I can agree with.

**B - Government is considering the following proposals:**

*Telecommunications (Interception and Access) Act 1979*

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

### a. Creating a single warrant with multiple TI powers

This section seems to be quite closely linked with the section under A.2B The standardisation of warrant tests and thresholds, above.

Again, I am concerned that the desire to simplify things will result in a situation where intrusive investigative techniques are applied to a much broader section of the Australia populace with all the associated ramifications.

I feel that this would be best addressed through a more holistic solution that takes a closer look at the types of crimes and thresholds that such measure can apply to. I also worry about the potential scope for abuse as well as the implications for people who may be loosely associated with a target for investigation on a personal level but not in association to any offence.

Any movement in this direction needs to be taken in accordance with broad ranging checks and balances, judicial oversight, and without simply reducing everything to the lowest common denominator. If that means retaining the status quo on this as well, and coming back to it separately in a manner that allows the Australian people to properly debate this changes, then so be it.

## 9. Modernising the Industry assistance framework –

### a. Implement detailed requirements for industry interception obligations

In the current digital age, the IT industry is a major area of growth and advancement. Any proposals, such as mandatory data retention, need to take account the prohibitive implications it may place upon new tech start-ups, ISP's and individuals.

As Mark Newton (Network Engineer for a large Australian ISP) wrote:

> "Data retention effectively increases the cost of evidence-gathering by requiring evidence to be gathered regardless of whether it's useful in a criminal prosecution; and outsources that magnified cost to the telecommunications providers.
>
> Telcos aren't charities, so they'll pass it on to their customers, permanently increasing the cost of communications, and, by inclusion, the cost of living for all Australians. If the Opposition is unswayed by civil liberties concerns, maybe the resulting banal economic inefficiency should give them pause for thought."
>
> [Mark Newton, The Surveillance State Tunes In, New Matilda, 16 July 2012, http://newmatilda.com/2012/07/16/surveillance-state-grow]

Even if data retention is only a matter of general logs rather than substantial content the infrastructure burden of maintaining this data would be an impractical burden upon tech companies. It also could open up the industry to an increased threat of damages and litigation should they be hacked and any of that data they store gets

released or abused to the detriment of the users or clients. It should be noted that the very act of storing such data would increase the desirability of any such business as a hacking target. Many service providers, for example, explicitly do not store logs of data as a security measure to protect their clients.

The burdens of data retention would not only act as a barrier to new business entering the market, it could negatively impact upon the smaller players already existing and thus decrease competition, to the detriment of the Australian consumer. Additionally it could act as an additional constraint upon new business models, technologies and services based in Australia when compared to competing services overseas. This could lead to potential new "Googles", "YouTubes" or "Facebooks" that may otherwise be an Australian success story either moving offshore or failing to get off the ground at all.

Again, in light of a lack of concrete evidence that we are faced with a massively increased threat or danger should we not implement all the measures outlines in the ToR and Discussion paper, it would seem that it would not be reasonable for the telecommunications industry to accept this burden to their operation costs, risks and international competitiveness.

While industry needs clearly guidance on what their obligations are in regard to legislative requirements, I worry that the proposed changes in this regard cast too wide a net and impose an unfair obligation upon the telecommunications industry which is likely to be passed on to consumers with no net benefit.

**b. extend the regulatory regime to ancillary service providers not currently covered by the legislation**
and;
**c. implement a three-tiered industry participation model**

I see that "Ancillary service providers" are defined as: "Telecommunications industry participants who are not carriers or carriage service providers. " and in intended to include "social networking providers and cloud computing providers".

This proposal strikes me as a near absurdity if the implication is that the regulatory regime is supposed to be extended to pretty much any entity providing an online service where communication can occur, regardless of "a three-tiered industry participation model".

This again links very much to my comments in regard to 9A above. In addition to the issues detailed there the implication of this proposal is that a kid setting up a personal Minecraft server (A game: http://www.minecraft.net/) which some of his friends could connect to, would then be obliged to fulfill a range of legislative requirements in regard to data retention and so on. This is patently absurd, and would stand as an insurmountable barrier to any kind of new social network development or cloud computing based internet start up. The detriment to Australian innovation would be crippling.

Despite the possibility of implementing "a three-tiered model", many online services are run with very narrow profit margin or even at a loss. A "three-tiered model' that is based solely on the number of users is a preposterous means of attempting to mitigate the burden of the requirements when it comes elements such as data

retention because a valuable online service can have millions of users yet not have the means to comply with a data retention framework. The costs of compliance could destroy the existence of the service and would adversely affect any person running their own internet services for personal use or as a non-profit or public good. This could simply push any such participants out of the space completely, or direct users to offshore services, which would disadvantage any Australian attempting to get started in the industry with a new service. Additionally this could also cause a contraction of services available to Australian users should overseas based services see such requirements as too onerous to bother complying with and thus decide not to bother with the Australian market.

Another implication of pushing people to offshore services to escape a driftnet surveillance approach, would be to potentially push people further away from a sphere in which genuine and targeted investigative activities could otherwise be employed on a case by case basis.

*Australian Security Intelligence Organisation Act 1979*

**10. Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.**

Admittedly this does not look as bad as it first appeared to be.

So long any such granting of powers are explicitly akin to the provisions detailed in the Crimes Act 1914 and that the safeguards detailed within the discussion paper are strictly adhered to, and that any such powers do not extend further then this is does appear to be a reasonable amendment.

**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.**

This seems like it could be a reasonable amendment but again with some of the same concerns detailed elsewhere in the submission related to warrants.

I do have concerns that this could be abused when used in conjunction with some of the other changes to warrants as detailed and ideally this could be addressed within a more holistic warrant reform process. However on it's own with appropriate checks and balances, coupled with judicial oversight, this amendment seems like it could be reasonable pending further information.

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

The discussion paper is too vague on this issue, relying on a caveat of "proportionality". As such, unless very specific cases are outlined with specific safeguards, I cannot support this proposal.

Without a very specific regimen of specific actions in specific circumstances, this provision could otherwise be widely abused by security agents, or used in a manner that would have disproportionate implications upon either targeted people or even innocent parties.

Unless there is more information or clarity in this proposal it could be interpreted to mean any number of actions including but not limited to:

*Deploying viruses or Trojans, Keyloggers, Spyware or Hijacking software.*

Such things could then be abused to attain passwords to online services, or to hijack a webcam and view within a person's (or a 3rd party's) home, or result in infections of other 3rd party computers. Or even to access online banking and transfer a suspects funds.

*Planting incriminating information.*

Whether this is by specifically putting incriminating files, or by using means to spoof browsing by a fake history, or to redirect network traffic to incriminating or suspicious locations, or even by planting encrypted information which the suspect would be unable to decrypt later (as per C.15a)

*Removal of evidence*

If suspect has information or evidence that they could either use in their defence, or information that could point to misconduct by agents, this could be removed.

*Adversely affect third parties*

As mention above 3rd parties could be affected by using the webcams or microphones in a suspects computer as a bugging device. Or if a self-replicating virus was used, others could become infected. Or if the pertinent computer is part of a wider cloud computing system, action that may damage that computer's integrity could adversely affect services used by other people.

As it stands any reference to this potential power is too broad and undefined as to what it actually means. Anything that comes close to allowing any kind of powers above need to be very specifically laid out and with a case by case approval process that ideally involves some sort of judicial oversight. Otherwise this has the potential to be far too easy to abuse to be able to support it.

**C. Government is expressly seeking the views of the Committee on the following matters:**

*Telecommunications (Interception and Access) Act 1979*

**14. Reforming the Lawful Access Regime**

**a. expanding the basis of interception activities**

I am unclear as to what specifically is being referenced here and as such this might be a good opportunity to point out that the discussion paper overall was decidedly vague and confusing and in some circumstances bore little relation to the actual ToR.

However, overall from a general perspective, as mentioned previously, I have not yet seen the case made that this is actually necessary. Again, any increase in interception activities are an extreme measure and, in the context of this Inquiry, requiring a level of proportionality when compared to privacy and the rights of the citizenry.

Since the September 11 attacks in 2001 there have been a number of changes to the powers enjoyed by the Australia security services at the expense of civil liberties, freedoms and privacy. With 54 pieces of anti-terrorism legislation passed in the decade after September 2001;

> ''Australia has exceeded the United Kingdom, the United States, and Canada in the sheer number of new anti-terrorism laws that it has enacted since September 11, 2001. Australia's hyper-legislation strained the ability of the parliamentary opposition and civil society to keep up, let alone provide effective opposition to, the relentless legislative output.''
>
> [from a study by Canadian Professor Kent Roach as quoted in: The laws that erode who we are, George Williams, Sydney Morning Herald, 10 September 2011, http://www.smh.com.au/opinion/politics/the-laws-that-erode-who-we-are-20110909-1k1kl.html]

Yet, here 2012, the case has not been made that there is an increased threat of such attacks. Nor does there seem to be a large uptick in general crime rates. In fact property crime is steadily trending downwards while most violent crimes see steady or downward numbers.

[see Australian Crime: Facts & figures (2011), Australian Institute of Criminology, http://www.aic.gov.au/documents/0/B/6/%7B0B619F44-B18B-47B4-9B59-F87BA643CBAA%7Dfacts11.pdf]

Additionally there are high figures touted as the costs of "cybercrime" but it seems that these may be overinflated:

> "McAfee's trillion-dollar estimate is questioned even by the three independent researchers from Purdue University whom McAfee credits with analyzing the raw data from which the estimate was derived."
>
> [Peter Maass and Megha Rajagopalan, ProPublica, 2 Aug 2012, Does Cybercrime Really Cost $1 Trillion?: http://www.motherjones.com/politics/2012/08/cybercrime-one-trillion-symantec-macafee ]

While it would be naïve to ignore that there are real and present threats to Australian national security, the burden of proof needs to be on the security services requesting increased powers to demonstrate that such a threat is proportionally larger than the existing and/or past threats. This is especially important when the powers requested could have such wide-ranging impacts upon the freedoms, privacy, safety and civil liberties of the Australian people and civil society that they are supposed to protect. The shift to a broad and all encompassing surveillance of the Australian people to combat a threat that seems no greater than the threat of past decade is a bridge too far. If there were indeed 4 major attacks thwarted in the past decade, and there have been no successful terrorist attack on Australian soil during that time either, then it seem that the current legislative framework is capable of doing the job already. As such any further changes should be viewed with a critical eye against the implications for the democratic freedoms enjoyed in Australia, as well as the privacy rights that each citizen should be afforded.

When viewed in the context of a proportional response to the current threat landscape I do not feel that the expansion of interception activities as outlined in the ToR and discussion paper are proportional to the massive invasion of privacy entailed. The cost to our privacy is too high in relation to a threat that if anything is subsiding and to which it appears the security agencies of our nation have enough tools to combat effectively anyway.

Expanding interception activities to a broader array of mediums such as social media are an overreach. They should be viewed in the context of the current day usage of social media. For many social media is a key means for communication with each other and the implication that anything said and done on social media is fair game for arbitrary retention for investigation is an egregious imposition upon the civil liberties of the Australian populace.

While much content can be posted on social media publically it is wrong to assume that people across the board equate social media as definitively public. Much material is intended for private consumption among friends and family without an intended wider audience and it should not be a default assumption that anything said between two people is susceptible for later perusal and analysis by a third party. As such any need for security agencies to access such information should be as a targeted investigation and not some grand driftnet scheme to capture all data and then poor over it for connections.

**15. Modernising the Industry assistance framework**

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

This proposal is one of my key concerns with the Terms of Reference and am opposed to this provision. Firstly the discussion paper, again, is vague and only includes a small easily missed reference on page 28.

From the context on that page, it could be construed that the target of this decryption offence is service providers and telecommunications industry players. Even if this proposal is limited to these targets it is still a problematic proposal. If it is intended for a wider audience, such as any suspect, then very idea is even worse!

Needless to say, I am opposed to this item for a number of reasons.

If it is intended to be an offence that targets, for example, a telecommunications company or service provider, then at what "tier" (in a hypothetical "three-tiered system") does it apply? Does it apply to the CEO of the company who makes a decision on behalf of the business, or to the low level employee who refuses to do so until he can see clarification from his boss, or who may not even have the level of access required to do so?

If targeted at service providers such as, for example, a cloud storage service, then how to account for data that may be stored in encrypted form by users on that service, whom the service provider has no means to decrypt? Or what of situations where a cloud storage service is employing a system of encryption of data that it cannot decrypt so as to protect users. This is often considered best practice from a security standpoint, ie the company providing the service does not have the means to decrypt the data. In such cases, if an Australian based provider is unable, legally, to provide such an encrypted service to users, then users would just use an offshore service, which would be beyond the reach of our law enforcement or security agencies anyway.

If a cloud service provider is required to provide a "back door" means of decryption, then this creates a security liability for any back door system could conceivably be found and taken advantage of by hackers.

If the offence is something that can be targeted at individuals then we need to ask the question of which individuals. Does it include suspects charged with a crime, or could it just be anyone that ASIO decides to question in regard to a matter? If charged with a crime, do they have to fall within one of the aforementioned thresholds, or is it just any crime?

Despite the right to remain silent being under attack in NSW it remains a fundamental tenet of a free and democratic society. The compulsion to decrypt data is a violation of this right.

Another aspect to consider is that a person may be in possession of data that merely appears encrypted but is not. Or they have encrypted data but are unable to decrypt it as they do not have the required decryption key. Encrypted data can be generated by software and the user could have no idea that it is using or storing encrypted data, or even if they are aware of it's existence and use by the software they may be unable to comply with an ASIO request to decrypt it because they either lack the technical know how, or just lack the relevant keys.

What happens if somebody emails a person an encrypted file? Is the recipient required by law to decrypt it? Again, they may not have the key.

In addition to the numerous 'false positive' issues a person could fall afoul of, this also opens up opportunities for abuse of power by investigating agents who may 'plant' encrypted data to secure a conviction under this law. Or a person could be framed by a 3rd party who deposits encrypted data into someone's possession, and then 'tips off' investigators.

Quite frankly the horror scenarios seem almost endless with this particular provision and even if the intent is not to use it against individuals, the ramifications within the IT industry of requiring adherence to this would have a chilling effect on software development and adversely affect Australian competitors in this space.

**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.**

This is another proposal on the ToR that simply must be roundly condemned and opposed. Yet again the discussion paper is vague on the details of this point, yet this is probably the singular most egregious violation of the civil liberties and principles of democracy that we should all do our utmost to protect.

This is wide scale driftnet 'collect everything' surveillance of every Australian, it destroys the presumption of innocence by turning us all into suspects by default.

I have already in this submission addressed potential concerns in regard to the burden upon service providers and the adverse effect this could have on the IT industry in Australia as well as consumers through possible price increases and less competition and services. But this issue goes well beyond economics; it is dare I say it, an Orwellian overreach on behalf of the security services and law enforcement.

While the security agencies who propose an adoption of mandatory detention draw a parallel between being able to access internet communications data, and being able to access phone call records, consideration needs to be given to the fact that internet traffic data contains more information in regard to the content of the communication, as opposed to phone logs which would really only give investigators a time of call, number called and duration of call. As such, simply granting the same or greater powers to agencies to access this information via data retention is a more onerous imposition upon privacy than to equate it with the equivalent of just giving us the phone records generated by a new, more technologically advanced, 'phone system'. Retaining information about access to URLs, Facebook "Likes", Twitter Direct Messages, Instant Messaging and so on also retains a great wealth of information about the content of the communication. In addition to the linkages between people in can provide, as well as the potential 'false positive' alarm bells that out of context data could trigger.

The Internet today is used for a broad range of things and in many cases is the first port of call for people before seeing a doctor, or psychologist, or lawyer or marriage counselor or any range of professional services all of which are activities that would be captured and detailed by a mandatory date retention scheme. Any such information could be highly embarrassing to individuals should it fall into the wrong hands or become public knowledge. As such, the decision to retain this data a highly dangerous endeavour when viewed within the context of the damage that could be done to people should the wrong information be leaked or stolen.

As an adjunct to the above such information as retained by a data retention regimen would become a highly sought after asset. Criminal elements will seek the data for use in fraud or identity theft or possibly blackmail. People could use such information to embarrass or blackmail political opponents of business competitors. Even foreign intelligence would view this data as highly valuable for espionage reasons, even if just as a means to information garnered to obtain people willing to pass on secrets so as to prevent embarrassing communications from being revealed.

The best security for this data is for it to not exist in the first place, as its existence would be a treasure trove that others would seek, and since no security can really

always be 100% effective it would likely only be a matter of time before such data theft or publication occurs. Should any number of high profile leaks or revelations occur in relation to data from this data retention scheme, then the confidence of the Australian internet user would be compromised.

Such loss in public confidence could result in a "chilling effect" as users turn away from using the Internet for personal affairs. Alternately some people could turn to more secure means of masking their identity such as proxys or VPNs which could actually result in a net negative effect on law enforcement efforts as people train themselves to become more conscious of potential surveillance and learn how to more effectively bypass such surveillance, mask their identity or cover their tracks.

With the Government spending so much on the NBN and highlighting benefits to the system such as remote access to medical services, it is worrying to think that the potential benefits of such long distance Internet based medical services in regional areas could be compromised by peoples reluctance to use them out of fear of surveillance, loss of privacy or data theft.

In addition to the numerous threats and dangers to abuse of this data, the additional costs and resources needed to maintain it, the threats to privacy, the dangers to civil liberties, and the potential to open average citizens up to fraud, identity theft and blackmail, it seems that for al that cost it is likely that such a broad ranging data retention scheme is not even an effective law enforcement tool anyway, such as in the German experience:

> "Blanket data retention can actually have a negative effect on the investigation of criminal acts. In order to avoid the recording of sensitive personal information under a blanket data retention scheme, citizens increasingly resort to Internet cafés, wireless Internet access points, anonymization services, public telephones, unregistered mobile telephone cards, non-electronic communications channels and such like. This avoidance behaviour can not only render retained data meaningless but even frustrate targeted investigation techniques (e.g. wiretaps) that would possibly have been of use to law enforcement in the absence of data retention. Because of this counterproductive effect, the usefulness of retained communications data in some investigation procedures does not imply that data retention makes the prosecution of serious crime more effective overall. All in all, blanket data retention can actually be detrimental to the investigation of serious crime, facilitating some investigations, but frustrating many more."
>
> [http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf ]

It almost seems like data retention is treated like the holy grail amongst law enforcement agencies but not only is its effectiveness for the task questionable it also comes at too high a price and is disproportionately extreme for the security threats facing us in real terms today.

Surveillance should be done on a case by case basis, not in an arbitrary manner which encompasses everyone while increasing real risks their privacy and rights. The potential for abuse with such a system is rife and goes beyond the benefits such a scheme could provide. There have been numerous high profile hacks and data theft cases in recent times such as hacks against Sony, LinkedIn, or AAPT, or mishandling of private information such as Telstra's sharing of usage data with an offshore entity.

*Australian Security Intelligence Organisation Act 1979*

**17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:**

**a. Using third party computers and communications in transit to access a target computer under a computer access warrant.**

This is another element that wish to register my opposition to. This power, when combined with some of the other powers listed in the ToR is another power that would be open to abuse. When considered as a proportional response to the current threat levels, again, this is a disproportionate level of intrusion and risk of threat to people who may be innocent third parties.

It is not unreasonable, when not suspected of any wrongdoing, to expect that one's privacy, data and possessions should be accorded the utmost sanctity and that any intrusion upon that as part of an investigation of a third party should only ever be done in the most dire of circumstances.

While the relevant portions of the discussion paper (p 50) seem to imply that the intent of this is to use third party computers controlled by a service provider to intercept communication in transit, but this is not specifically stated and i would worry that any legislative change that does not specifically state such a provision would eventually result in this power being used to target any third party computer.

Even so, restricting this to service providers would still be an overextension of power, especially in circumstances where it may be difficult to target specific communications originating with or addressed to a suspect. My fear here is that it would allow the capture of broad communications data by a range of innocent third parties in an attempt to obtain the data or communications of the specific target.

**b. Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant**

See above point.

Additionally one would want to ensure that any potential damage to property or disruption of services caused to third parties in the investigation of specific suspects would be adequately compensated and would account for third party users of a service that would otherwise be disrupted by such actions.

**Conclusion**

I do wish that we had been afforded more time so as to be able to address these matters in more detail and with stronger supporting arguments. Additionally I do wish that the Discussion Paper has covered some of the specifics to these proposals more adequately.

The elements of the ToR to which I am opposed I feel are a case of overreaching for powers that have the potential for too much negative impact upon the populace, while not being warranted by any increased threat which is so dangerous as to necessitate such changes.

When I refer to security agencies and/or law enforcement abusing powers, planting evidence or using powers in ways that are beyond their intent, I do not mean to imply that this is endemic or rife within the current agencies and their employees. I am certain that the majority of officers respect the democratic principles that we hold dear in this nation and are honest and forthright in their desires to serve with honour the tasks they are assigned. However, my fears in regard to bequeathing some of these powers to the respective agencies are for future iterations of these agencies. We do not have a crystal ball and cannot see whether or not future governments will potentially resort to abuses that these proposals would so readily facilitate. There is no guarantee that future governments won't try to misuse these powers, nor that 'bad apples' within their respective agencies won't be tempted by them.

Once these rights and privacy's we currently enjoy are further limited by acceding to the proposals in the ToR, they will be very difficult, if not impossible, to reclaim. I wish to see a future where my children can enjoy no lesser rights to privacy or civil liberties than I and my parents enjoyed. A future where they do not to have to grow up into a society where it is presumed that everything one does and says is being monitored. I think for those of us for whom life changed when we entered the so called "War on Terror", owe it to future generations to not give up on the principles that our soldiers have supposedly been fighting for. Quietly giving up our privacy and rights and enabling modern technology, which can be otherwise so empowering, to instead become our Panopticon style overseer, would, I fear, be a betrayal of those before us who sacrificed to ensure we had our rights and freedoms. Surely when the dust settles even further, and we look back in history at the post September 11/War on Terror era, we do not want to be remembered as the generation that gave up those aspects of our society that made it special.

Thank you and I do hope that governments come to see the Internet and Digital Age for the potential it provides for empowerment and freedom, rather than how it can be twisted into ways that control us more than our forefathers would ever have dreamed, or tolerated.