Submission regarding a comprehensive review of the Telecommunications (Interception and Access) Act

Terms of Reference

As the terms of reference are relatively concise, I repeat them here.

1. the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and
2. recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013.

The relevant section regarding the first item may be found at Appendix A.

Glossary

The *Telecommunications (Interception and Access) Act 1979* will hereinafter be referred to the TIAA.

The *Telecommunications Act 1997* will hereinafter be referred to as the TA.

LENSAs - Law Enforcement and National Security Agencies

ALRC - Australian Law Reform Commission

PJCIS - Parliamentary Joint Committee on Intelligence and Security, hereinafter often referred to as the Committee.

The term "metadata" is used throughout this submission in preference to the term "data" because metadata is more in line with normal ITC industry usage and because, in the context of data communication networks (e.g. the internet), data is essentially the same as content.

ALRC report

ALRC Recommendation 71-1

Part 13 deals with "Protection of communications". As the primary threat to this at the current time appears to emanate from government, I think that this Part should be moved into the TIAA. With that structure a single Act would regulate when private telecommunications, content or metadata, may *not* be accessed and when it *may* be accessed.

ALRC Recommendation 71-2

There does seem to be a difficulty with having the Attorney-General's Department (AGD) responsible for the TIAA and the Department of Communications responsible for the TA.

This is confusing for the public and creates the potential for matters to fall between the cracks, on

the one hand, or be the subject of a turf war, on the other hand.

More importantly though, it seems that the AGD is far too beholden to the LENSAs i.e. cares little for communications, knows little about communications and is far too ready to accommodate the LENSAs, no matter who the incumbent AG is. Frankly, some of the material coming out of the AGD in relation to the review pertaining to item 2 in the Terms of Reference was frightening for its lack of understanding.

The Department of Communications would be more on top of the technological aspects and better able to balance telecommunications v. privacy v. the needs of the LENSAs.

Whether any administrative or legislative structure is “effective” depends entirely on whose perspective you seek and what the goal is.

If the goal is to make privacy paramount and to define strictly limited circumstances in which privacy can be breached and *my* perspective is sought then the current structure is not effective. For example, we saw in the Telstra / Netsweeper scandal that no legal action of any kind was taken and presumably Telstra could have resumed, this time more discretely, its interception activities.

I will reserve any further comments to the remainder of this submission where I address the recommendations of the PJCIS.

PJCIS Report

General comments

Much of the PJCIS's report should be treated with extreme caution, for two reasons.

1. The public consultation was invalid because the proposals were so poorly defined. Indeed it may be that the PJCIS itself had difficulty extracting an understanding of exactly what was being proposed. The PJCIS report suggests that this was the case. It is also noted that the AGD provided additional information *after* the closing date for submissions – and hence this information was not available for members of the public to digest or to comment on. Noone should give the LENSAs a blank cheque, not the government and not the people.
2. Significant new information has emerged since the committee's report. I refer to the Snowden revelations. I am not here to express an opinion on the morality or legality of those disclosures. However the fact is that the information is now in the public domain and it would be negligent of government in general not to take into account all available information. These revelations paint a picture of surveillance out of control, and at best being conducted at the edges of the law.

It is a sad indictment on government that I learned more about what the former government's proposals actually meant from Snowden than I did from said government.

If the government wishes to continue to pursue the original proposals then I would urge the committee to begin the consultation process again.

In reality however many of the original proposals were wholly unacceptable and should be abandoned. Instead, government should turn its attention to how the privacy of Australians can best be protected against predatory LENSAs and corporations, through a combination of gentle persuasion and legislation.

The picture that emerged from the US, via Snowden, is of surveillance out of control. Even some US legislators have admitted that. Considering how that might apply in an Australian context, it is salutory to note that the LENSAs are *not* accountable to the parliament. Because of the sensitivity of some matters, it is really only a small group of parliamentarians who are privy to what is going on. That is not a good basis for accountability.

LENSAs and cake

It seems that the LENSAs want to have their cake and eat it too. On the one hand, they decry the changing telecommunications industry that means that metadata is not retained for as long as it used to be. On the other hand, they are happy to benefit from the changing telecommunications industry that means that a much greater breadth and depth of information is now available. Who would have thought in 1979 that every non-criminal and every criminal could be persuaded to carry a tracking device disguised as a telephone, with the resulting location information available without a warrant?

Summary of earlier comments

This is a summary of comments from my submission to the PJCIS inquiry.

- Amend the TIAA so that under no circumstances is interception by LENSAs permitted without a warrant from a court – not without a warrant and not with a warrant from some other type of entity. The AG should have no power to issue warrants.
- Warrants should not be renewed or varied without additional court approval.
- Amend the TIAA to make the distinction between content and metadata unambiguous. The current definition is not adequate. If you can't adequately distinguish them then you can't have separate regulatory regimes for them.
- The threshold for interception and access is currently a dog's breakfast. The TIAA should be dramatically simplified regarding the threshold that must be met.
- The current content and metadata regime should not be extended to other entities (ancillary service providers).
- Data retention? Not now. Not ever.

Response to PJCIS recommendations

Recommendation 1

The dual objectives should not be given equal weight. Instead, the objectives should make privacy paramount and define strictly limited circumstances in which privacy can be breached. This recognises that the vast majority of Australians are law-abiding citizens, not suspects.

Recommendation 2

Primary responsibility for the TIAA should rest with the Department of Communications, with the AGD to argue the case for when and why privacy should be breached. The AGD has not shown itself either to have sufficient grasp of the technology or sufficient balance to have primary responsibility for this Act. The AGD can advocate on behalf of the LENSAs, which seems to be the way it perceives itself anyway.

Recommendation 3

See comments on Recommendation 2.

Recommendation 4

See comments on Recommendation 2.

Recommendation 5

The Committee should be making a recommendation rather than leaving it to the AGD. Standardisation of the threshold may help to reduce the number of agencies that continue to have access to metadata.

Recommendation 6

The Committee should be making a recommendation rather than leaving it to the AGD.

Recommendation 7

I disagree. This sounds dangerous. Like so many proposals, this is specified somewhat vaguely.

Would it ever be acceptable, under any circumstances, to intercept *all* communications occurring at a certain time?

To permit the interception of *all* communications occurring with a certain destination or from a certain location would potentially involve interception on an immense scale, hoovering up the communications of vast numbers of innocent parties.

I have not seen adequate argument that such capabilities are proportionate.

Some might argue “well, the LENSAs would never ask for such broad warrants” or “a court would never approve such a broad warrant” but in that case the legislation does not need to enable such broad warrants – and should not do so.

Permitting the interception of communications of a particular type has not been clearly specified. That is, what does this specifically mean? In the absence of this specification, I would have significant concerns if ISPs were even to build this capability into their networks.

It would also be doubtful how effective this (type-based interception) would be against someone intent on avoiding interception, as there are already means of obscuring some aspects of the type of communication e.g. IPSec.

It is noted however, as IGIS noted, that in respect of particular identified services, the LENSAs can always do this filtering for themselves. Provided that a warrant to intercept that service or those services has been issued by a court I don't have a problem with that.

However I have significant concerns about the idea that interception of *all* communications of a particular type would ever be proportionate.

Exactly how offensive this proposal is depends on what the final set of attributes is and whether new attributes can be added without legislative amendment.

Also, where is the reporting to the *public* in this?

Any proposal that allows a general warrant to be approved by a court, for example, and for the warrant then to be varied as needed by successively lower-ranked parties is of concern, as it serves to debase the approval.

As the set of attributes becomes larger and more complex, I have some concerns as to whether a court would be sufficiently well-informed to know what exactly it is authorising or even be able to anticipate how the warrant will be used. So if this proposal goes ahead, there could at the very least be a need for an education program.

Recommendation 8

Of course LENSAs will complain about restrictions on how they can operate. Interception is a significant privacy invasion and it is designed to be restrictive!

A key aspect of this that must be in place is that if a LENSA has properly obtained a warrant for interception in connection with an offence or a suspected offence that meets the threshold and thereby becomes aware, through interception, of a different offence or suspected offence that does not meet the threshold, then it or any other agency must not rely on the information about the second offence in any prosecution. To do otherwise would make the interception regime look dodgy since effectively the threshold is simply bypassed, especially if the original offence is not subsequently successfully prosecuted.

Is 2.81 really claiming that the NSW Police uncover child abuse accidentally via telephone intercept "every day"? Even so, it is not clear why the child protection authority needs to know that a telephone intercept is running. That would seem to be irrelevant to the more important point in that scenario. It is also not clear why the police could not themselves simply act. I hope this example and the example from Victoria Police are not a continuation of the established pattern of using child abuse to justify ever more draconian laws (in the manner of Senator Conroy).

Ultimately though this recommendation isn't a recommendation for any specific legislative change, merely a recommendation for further review.

Recommendation 9

Who can argue with this as a goal but what specific duplication is to be removed? This is a very vague recommendation.

I think there is general agreement that stored communication warrants could be dispensed with *provided that* those communications are subject to the same current level of protection that they would have had if they were being intercepted (which is not currently the case). Additionally however, access to stored communications does allow LENSAs to look back in time i.e. to a time before the issuing of the warrant. So there should be a legislated tight limit on (a) how long ISPs can keep stored communications, *and* (b) how far back LENSAs can request stored communications for. Note that these are both maxima.

However as noted my earlier submission, no sane criminal would use his or her ISP for email and no sane criminal would use SMS.

I see no problem with LENSAs having to report on all three of: interception warrants, stored communication warrants and access to metadata. It doesn't have to be a separate report but different types of privacy invasions should be itemised.

Even if there is a unified warrant regime where one warrant gets access to everything, LENSAs should still be obliged to account for what they actually did with the warrant. I get that LENSAs don't like to spend time on reporting but it is the price that they pay for the powers that they have been given.

"Account for" means reporting to the public, presumably by a report to parliament that is made available to the public.

Recommendation 10

It is not possible to agree or disagree with this because the Committee has squibbed the central question i.e. is the threshold being lowered?

It was always contentious that access to stored communications had such a low threshold but if the effect of the single threshold is that the threshold for access to other communications is lowered

then this is fail. The Committee should be recommending that the existing 7 year threshold be the single threshold. It is very clear that the LENSAs and the AGD (2.100) are simply angling to get the threshold reduced to, for example, 5 years.

In view of the trend, particularly at the state government level, towards law-and-order auctions and towards moral panic regarding the issue du jour, even if the threshold is unified at 7 years, the LENSAs can look forward to greater and greater access through a kind of jail sentence "bracket creep". Since the threshold is compared against the maximum possible sentence for an offence, not the actual sentences being imposed by courts, this works in favour of the LENSAs. (Fairest would be that the threshold is compared against the actual sentence handed down in the particular case being investigated but this is clearly impossible.)

If there is a unified warrant regime where one warrant gets access to everything, LENSAs should still be obliged to account for what they actually did i.e. what use was made of the warrant. To have it otherwise is simply to reduce accountability.

As mentioned in my comments to the previous recommendation, I don't have a problem with a unified warrant regime provided that the current 7 year threshold is maintained and provided that the unified warrant regime only unifies existing types of warrants i.e. without any expansion of the interception regime. I recognise the value in time, both for the LENSAs and for the courts, in only having to deal with a single warrant but that should not be a trojan horse for surreptitious expansion of the regime.

At 2.101 Victoria Police appear to be asking for much more than just a unified warrant regime but in fact for additional warrant powers, since things like "username" and "webmail address" and "internet account" are probably only meaningful to entities who are outside the current warrant regime.

Recommendation 12

The option of litigation must always be retained. While ACMA may issue an infringement notice, an ISP or telco must always have the option of challenging the infringement notice in a court of law.

Again though no detail is provided as to what enforcement mechanisms are contemplated.

Recommendation 13

It is not possible to agree or disagree with this recommendation because the scope itself is not spelled out. The scope that results from this recommendation may be wholly unacceptable or it may simply be a clearer expression of current law. Noone can disagree however that whatever is specified should be "clear". Making those obligations explicit in legislation would also be more transparent.

Recommendation 14

I disagree strongly with this recommendation. The Committee notes that Data Retention was one of the most controversial proposals. In my view the Ancillary Service Providers proposal deserves to be equally controversial.

Is this existing law?

There seems to be some inconsistency in the review as to whether these providers are or are not currently subject to the regulatory regime. The original Terms of Reference suggest that they are not.

> *extend the regulatory regime to ancillary service providers not currently covered by the legislation*

The Committee however disputes this implication (at 2.130) and yet at Recommendation 14 recommends an amendment to specify that these providers are covered. If the Committee were confident of its position then no amendment would be required.

At 2.135 the Committee notes that no providers supplied evidence to dispute that the TIAA applied to them. Absence of evidence is not evidence of absence. It could equally be that the relevant providers did not understand that they were being targeted, or were not even aware of the review, particularly as most providers are overseas. Neither the original Terms of Reference nor the Discussion Paper provided anything specific about the scope of this proposal. As far as I can see, none of the providers listed in the Committee's report (Facebook, Google, Twitter) actually made a submission. Silence is not agreement.

Analysis of the current law

(This section should be read with the disclaimer that I am not a lawyer.)

The Committee's belief that ancillary service providers are already covered (2.134) is debatable.

The crux of the issue would seem to be whether an ancillary service provider is covered by the definition of "telecommunications service" or "telecommunications system". The definition in s5 raises some serious questions.

I don't think Facebook would regard themselves as offering a system or service for carrying communications via electromagnetic energy. Indeed, from the perspective of Facebook, the manner in which the communications are provided to it is irrelevant. Facebook's ISP could replace electromagnetic energy by avian carriers and Facebook would not be aware of it, other than the anticipated reduction in network performance.

Facebook does not *provide* a telecommunications service, Facebook *uses* a telecommunications service, just as its customers do. Or, if you prefer, Facebook offers *its* service *over* a telecommunications service – but that does not make Facebook's service a telecommunications service.

If you don't accept that argument then consider a psychiatrist who sometimes allows her patients to get service via the telephone or via the internet. If you believe that every service that is offered over a telecommunications service becomes itself a telecommunications service then you would believe that LENSAs and ACMA now have power to compel the psychiatrist to participate in this offensive regime of spying.

It seems to me, in the context of interception and access, that LENSAs are more likely to be interested in access to stored communication that an ancillary service provider has possession of (as compared with interception). Indeed, depending on the exact network arrangements that an ancillary service provider has, it may be legally impossible or technically impossible or both for the ancillary service provider to arrange interception – since that is really interception of a telecommunications service that it does not own or operate, does not have privileged access to and does not have knowledge of i.e. the service that is provided to it by its ISP.

However the definition of "stored communication" in s5 says that it must be in the possession of a carrier, which, by the current proposed definition of an ancillary service provider, an ancillary service provider cannot be.

It seems to me also that LENSAs are likely to be interested in metadata that an ancillary service provider has. However at a somewhat cursory glance it seems unlikely that any of the provisions in the TA relating to compulsory surrender of such metadata would apply to an entity who is not a carrier or CSP (except possibly where the entity is a telecommunications contractor or employee thereof but the definition in TA s274 cannot in my opinion be stretched to include entities like Facebook).

In addition, TIAA s15 defines the process for imposing an interception warrant on a carrier. It is therefore silent on the process for an ancillary service provider (which, again, cannot be a carrier). Even if such a provider is compelled under current law, there is no process to make it happen.

Finally, the definition of "telecommunications system" in s5 is clear that it does not extend outside of Australia. However the definition in s5F for when a communication is passing over a telecommunications system specifies that it continues until accessible to the intended recipient. When one party to a communication is overseas and one is in Australia we would seem to get the result that the communication is passing over a telecommunications system even at points in time when there is no telecommunications system involved!

Admittedly, the definition in s5H of when a communication is accessible to the intended recipient is not exclusive. So a communication could be deemed to be accessible and no longer passing over a telecommunications system once it leaves Australia. That however is not entirely satisfactory, since it enables warrantless interception. From a practical standpoint though that is the case. There is little that Australian law can do about "interception" that occurs overseas and we know indeed that this is occurring on a massive scale. This would mean though that interception, in the sense defined by the TIAA, cannot be performed by an overseas ancillary service provider because it is literally impossible.

These comments may be relevant because all three of the specific entities mentioned in the Committee's report are based overseas. This particular difficulty would not exist for domestic ancillary service providers.

What is an Ancillary Service Provider anyway?

The discussion at 2.131 and 2.132 seems predicated on a continuing and widespread misunderstanding as to what "ancillary service providers" means. For example, the point made in 2.132 seems incorrect. Regardless of Facebook, Google, Twitter and VoIP, LENSAs can intercept *all* internet traffic simply by going to the ISP with a suitable warrant. It is true, as stated in 2.132, that a person can have a conventional telephone service with one provider and an internet service with another provider but the service providers here (the telco and the ISP) are unambiguously covered by the existing legislation.

This misunderstanding is not surprising given that neither the original Terms of Reference nor the Committee's report attempted to define what "ancillary service providers" means. The best that is offered is "Telecommunications industry participants who are not carriers or carriage service providers" but this doesn't really clarify much. Am I a "telecommunications industry participant"? Who is?

The crux of the matter

However, regardless of whether ancillary service providers are or are not covered by existing legislation, and exactly who these providers are, is not the point. To apply the existing interception regime to those providers would be a *major* extension to current practice and should only be considered after informed debate. In other words, even if this is not a legal extension, it is a practical extension and hence should be treated as such.

Because the Committee believes that this is not a change to the law, there may have been inadequate consideration of all of the implications of this, in its opinion, non-change.

Erosion of trust

It seems to me that the revelation that companies such as Google, Apple, Facebook, Microsoft, skype, YouTube, Yahoo and AOL can no longer be trusted (because they have been compromised by the US government) represents a greater threat to society than any criminal activity – and that's

without even considering the risk that the existence of a metadata honeypot presents, if this proposal is combined with the Data Retention proposal.

The US government has created a Stasi-like surveillance regime where everyone spies for the government. Are we seriously suggesting that Australia should follow that lead?

How big is this?

In my original submission I asked a number of questions regarding exactly how wide this extension of the surveillance regime is intended to be, none of which were answered by the Committee's report. I ask these questions again.

> *What about not-for-profit entities?*
>
> *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.*

Since the Committee's report makes clear that the Committee intends Facebook to be an ancillary service provider and yet Facebook customers get the basic service for free, presumably providing a service for free does not exempt the provider from the burdens proposed here. However it is more complicated than this because anyone who believes that Facebook is "free" is kidding themselves. *You* pay Facebook by providing a service to *them* (i.e. in supplying an endless stream of personal information to them, which they then convert into revenue for themselves, and hand over to the NSA). Hence while no money changes hands, each party provides a service to the other, and the service is in each case provided over the internet. Does this then make all Facebook customers "telecommunications industry participants"?

In other contexts there has been the suggestion that a provider would be exempt until it reaches a certain threshold number of customers (e.g. 50,000) although it is not clear whether that number of customers is tallied on a world-wide basis or limited to Australian customers only. The latter makes more sense to me. (Indeed if large company that is successful overseas is immediately brought into the interception regime as soon as it has its first Australian customer then this would constitute both a trade barrier and a disincentive to bother with the Australian market.)

A threshold of, say, 50,000 customers would at least ensure that the web site of the Bagdad Pigeon Fanciers Association can stay outside the snooping regime.

There is some suggestion (2.120) that ACMA and the authorities may move to a regime where enforcement of the obligation to assist the LENSAs can take place without any legal niceties, but is the Committee seriously suggesting that ACMA will be able to come down on every Joe Public who runs a small web site or hosts a game server? That such a person could be issued with a notice to assist the LENSAs, and prevented on pain of serious penalty from revealing that such a notice had been issued, and prevented from challenging it in court … is a direction that no *democracy* would go in.

As abhorrent as an ancillary service provider interception regime might be, it sits even less well with the corresponding enforcement regime.

I would wonder how the "cost sharing" arrangements work in such a scenario. At this level of service provider it can't even be assumed that development or other technical capability exists.

What about foreign providers?

While carriers and CSPs are more or less by definition domestically based, this does not apply to

ancillary service providers. How does the government intend that this be enforceable on foreign ancillary service providers?

What if the Australian government's requirements are incompatible with the domestic law where the service is provided? (This could be the case if the other country's domestic law better protects human rights, such as is plausible in Europe but sadly perhaps not in the US.)

How will a foreign ancillary service provider know that a demand for assistance is legitimate? This is an important question because if a foreign ancillary service provider is receiving requests from thousands of agencies in hundreds of countries, it becomes increasingly difficult to verify each request and in the absence of adequate verification it is obvious that a new breed of scam could emerge. (Unfortunately the current primary internet-based authentication mechanism is somewhat deficient, particularly for something as grave as a privacy violation request. I think we knew this before Snowden.)

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?

Content is now fair game?

It is impossible to extend the metadata access regime to ancillary service providers without weakening the protection for “content” because what is metadata at the ancillary service provider level is content at the ISP level. I am sure the LENSAs wouldn't complain about that but if we are going to significantly weaken the protection for “content” and give almost unfettered surveillance powers to LENSAs then we should be honest about it.

Since content is only accessible with a warrant while metadata is a LENSA free-for-all, it is crucial to retain and clarify the distinction and separation between content and metadata.

Recommendation 16

This proposal remains unclear in its scope. The recommendation does not state unambiguously on whom this obligation will fall.

If it is intended to impose an obligation only on carriers and CSPs then the AGD may not have got the memo because their reference at 2.145 to s3LA of the *Crimes Act* suggests a much broader scope if the proposal is intended to be analogous to s3LA.

Taking for a moment the assumption that it is intended to impose an obligation only on carriers and CSPs, it is far from clear how a carrier can assist anyway, assuming that they did not themselves set up the encryption. That is, no useful encryption mechanism has a means of decryption unless the required “key” is available. No examples have been given as to how a carrier/CSP could assist.

In addition, it is not clear how any of this would deal with “Forward Secrecy”. The basic intent of Forward Secrecy is that even if the long-term key becomes compromised at some time after the communication was conducted (e.g. the long-term key is revealed under duress, including of course under legal compulsion) then the session cannot be decrypted – not by either party even assuming that a complete record of the encrypted session was made by the intercepting agency. Note that Forward Secrecy goes beyond the normal encrypted communication protocol practice of using a session key that is independent of the long-term key and used just for one communication.

It is possible that it is intended to impose an obligation on all “telecommunications industry participants” – with the attendant vagueness about who is included in that, and with the issues of

jurisdiction over "participants" that are overseas.

In some cases it would be a very serious problem for a business to reveal its encryption key, as contemplated in 2.147. Essentially each time the business was hit with a demand to reveal its encryption key, and did so, the business would have to get a new encryption key. There is a cost in dollars of doing this, as well as a cost in time. (This applies whether or not the business is using Forward Secrecy.)

The text at 2.148 contains a grab bag of interesting information but almost none of it is relevant to assisting in the decryption of communications. That may reflect the lack of detail in the original proposal.

However 2.148 does make reference to one important point: plausible deniability means that a securely erased empty disk is indistinguishable from an encrypted disk. (It is of course recommended practice always to erase a disk securely when the information on it is no longer required.) How then could we countenance the possibility of someone sitting in jail for 2 years because they failed to decrypt a securely erased disk? Is this what we have come to?

I understand that LENSAs may be frustrated with such advances but, if anything, plausible deniability was designed to protect their ilk e.g. Australian agents overseas who may have been captured, or otherwise compromised.

Regarding the actual recommendation, where is the consultation with the *public*? All of the listed entities should indeed be consulted but so should those who will advocate for the rights of the public.

Recommendation 17

Regarding the suggestion at 2.159 that timeliness be improved by implementing B2B (G2B?), while I am not opposed to that idea, it would be crucial to ensure that authentication is not lost as part of that implementation. See my comments above under "What about foreign providers?" under Recommendation 14.

In the absence of a fully automated solution, exactly how costly this is depends on what the required response timeframe is. If the required timeframe is measured in hours then this mandates 24x7 staffing, which has implications for barriers to entry and adversely impacts smaller or cheaper providers.

In addition, when taken together with other proposals for "attribute-based interception" and other proposals that would potentially impact on a large number of services, the sudden influx of a mass of requests from LENSAs would test even the most well-resourced telcos and carriers. As such, introducing penalties for failure to meet timeframes may be unreasonable and inflexible.

Unless the number of agencies with the power to require assistance is tamed and with the assumption that such agencies do not coordinate their requests in any way, such an influx may occur.

It remains to be seen how such a system would interact with requests that come in from foreign agencies. After all, if LENSAs expect to be able to make demands of foreign providers, we would have to assume that the opposite situation is true.

The actual recommendation is reasonable but in light of 2.163 a more robust recommendation would have been to reject this proposal until such time as an agency is able to demonstrate a need for it.

Recommendation 18

Being technology-neutral superficially makes sense but that is often at the cost of trying to fit a

square peg in a round hole. The current confusion regarding content v. metadata is an example of this.

It may be better to accept that legislation, like most other things, needs periodic maintenance.

Wholesale rewriting of this legislation must not be a trojan horse for an expansion of the spying regime.

Recommendation 19

I disagree with the third bullet point of the recommendation. Why doesn't the government try a cooperative approach before giving itself greater power?

There seems scant evidence that there is actually a problem to solve here though.

Recommendation 20

I disagree with the recommendation. Without an adequate limit on what a network means this is far too broad. The internet effectively means that all computers operate in the one network.

The Committee should be clarifying what is meant by “directly associated” if it ultimately intends to expect a court to authorise a warrant on this basis. Is a computer “directly associated” with a person of interest because the computer has been accessed by that person? What is the test to be applied here?

Recommendation 21

I disagree with the recommendation. The Committee does not seem to have addressed at all any of the public's objections to this proposal.

Recommendation 22

I disagree with the recommendation. There are several issues that were raised in the consultation phase that have not been addressed at all in the report. In addition, this proposal is simply a bridge too far. If ASIO can't directly access the target computer then that's just too bad! ASIO should not be given greater and greater power, particularly as here we are talking about computers belonging to and used by people who are completely innocent.

It seems to me that it would be very difficult for legislation to specify or for ASIO to give effect to any limits regarding the extent of impact on the third party. To take a hypothetical example, what if the third party computer is in use in relation to a serious medical condition, as will probably become more common in the future? What if the computer is in use in relation to an industrial or other control application, as will probably become more common in the future?

Likewise it is doubtful that the AG could consider the potential effects (as suggested in 4.44), as those effects would be as unknown to the AG who is issuing the approval as they would be to ASIO - until after the fact.

Recommendation 23

I disagree because the AG, particularly as a political appointment, should not have the power to issue warrants at all.

Recommendation 25

See comment to Recommendation 23.

Recommendation 33

I suggest extreme caution is necessary here. Extreme powers should not be spread even more widely, nor should outsourcing be used to decrease transparency even further.

The actual recommendation is completely vague about the nature of the cooperation and the types of private sector entities.

Experience from the US suggests that this is a bad direction to go in.

Recommendation 37

I disagree with this recommendation. This sounds dodgy. I can accept that an officer's identity may be kept secret, and is probably irrelevant in most cases, but a person attempting to defend charges in court must keep the right to see all the evidence against him/her and to challenge its validity and to cross-examine. We should not abandon basic fairness in the justice system just because you are frightened.

As networks become more complex and the types of intercepted information becomes more varied, I believe that it is increasingly untenable to avoid a full examination of the facts in court, if it comes to that.

No person should be able to be found guilty on the basis of evidence that is only presented in an evidentiary certificate. In other words, the evidence that is fully and openly discussed in court must by itself establish guilt to the satisfaction of the court.

The identity of a *source* may be so relevant to a prosecution that I cannot support the idea of keeping the identity secret.

Recommendation 42

I strongly disagree with the idea of data retention regime but, since the Committee passed the buck on this recommendation, I can't actually say that I disagree with the recommendation.

It is not possible to exclude content until a satisfactory definition that distinguishes between content and metadata exists.

To exclude “internet browsing data” is somewhat vague. “browsing” suggests web but web is only a small subset of what might be accessed on the internet.

It is inadequate merely to exclude “web” because “web” could easily be superseded by some new flavour of the month. (It is interesting to note that Appendix H specifically admits that URLs – web browsing data – are disclosed to LENSAs.)

The provisions for “content that cannot be separated from data” are inadequate in the sense that it is by then probably too late! With the sheer volume of content flowing on the internet, it is clear that any collection of metadata must be automated. Hence the distinction between content and metadata must be able to be made by a computer.

I attempt to address some of these issues in the section below entitled “Content v. Metadata”.

Encryption of metadata

While I don't disagree with the idea that any entity that is obliged to retain metadata must encrypt it, this addresses only the tip of the iceberg. Since *someone* must have access to this metadata, issues still exist regarding access to the metadata. For example, LENSAs will presumably want access to this store of metadata and they may want that access remotely.

Questions arise regarding rotation of the encryption key and retention of the encryption keys.

In addition, since we now know that the US government may have acted to compromise the design of widely used encryption schemes, the choice of encryption algorithm is fraught. (Just because the US government may have caused the compromise to be present does not mean that other governments or other entities are not now or will not become aware of how to exploit it. In other words, it is not valid simply to argue that the US is an ally of Australia, and friendly to Australia. In any case the US has shown itself to be interested in conducting spying against countries that are ostensibly its allies.)

By the way, in reference to the Glossary definition of "encryption" in the Committee's report, encryption in the context of communications in transit also seeks to prevent *alteration*, not just access, and that additional aspect would seem to have applicability to a store of metadata. That is, the *integrity* of the metadata is fairly important if anyone intends to use it in a prosecution, for example.

Data Collection?

It has not been made clear whether what is being discussed here is only a Data *Retention* regime or if it is also a Data *Collection* regime. In other words, does the government envisage that it will compel providers to collect data that they would not otherwise collect, or only to retain data that they do collect?

How long?

I have seen no justification for the retention period of 2 years. LENSAs have already admitted that what they really want is an indefinite retention period. 2 years would be the first step towards that. The best protection is never to introduce such a scheme in the first place.

I would think that from a law enforcement perspective, the time to crack a case is as soon as the investigation begins and that the probability of getting anywhere decreases with time. I wonder really what proportion of cases would benefit from 2 years of retention. 2 months maybe. However, as I said, LENSAs cannot even be trusted with a 2 month retention regime because as sure as night follows day in a few years time we would be debating an extension of the retention period.

Overall response to recommendations

It is disappointing how few of the recommendations were against the LENSAs and in favour of the rights of Australians. Given the partial lack of transparency in this process and in the application of whatever laws arise from it, someone in the parliament needs to stand up for the rights of Australians. The government is after all supposed to represent the people but it sure doesn't feel like it.

By the way, failure on my part to respond to a specific recommendation should not be construed as agreement. It may indicate that I didn't understand the recommendation or didn't understand the implications of the proposal involved, or that I overlooked it, or that I ran out of time.

I recommend that all members of parliament read Orwell's *1984*, not as an instruction manual but as a warning. The government is building a "digital 1984". The only thing that Orwell got wrong was the date!

Content v. Metadata

Since the Committee hasn't grappled with this question, regarding interception, I will take a stab at it.

In the context of a data communication network (i.e. the internet)

- content is everything that is transmitted by the end user equipment but excluding anything that the ISP has already come to know through other means (e.g. information disclosed by the customer during signup and e.g. information that the ISP itself has assigned)
- metadata is anything that is not content (provided of course that the ISP has the information)

So

- the unique identification of the service that is assigned by the ISP (some kind of service number) – NB: this is *not* the IP address
- the unique identification of the customer that is the lessee of the service (some kind of customer number)
- the date and time at which content was transmitted or received
- customer (i.e. lessee) name and address details that the ISP has on file
- billing details that the ISP has on file
- the IP address that is presently assigned to the service
- the type of technology that the communication is using (e.g. ADSL, cable, fibre, wireless)
- if wireless, the location of the tower that the communication is using and, where the ISP chooses to infer it, a more precise location of the end user equipment
- if wireless, the SIM number (IMSI) and, if already known to the ISP, the IMEI
- if not mobile wireless, service address details that the ISP has on file

are examples of metadata.

This definition attempts to put a clear stake in the ground, rather than allowing some content to be called metadata and having the boundary between content that is protected and content that is fair game because it is called metadata from moving inexorably in the direction of the latter.

It is intentional in the above that URLs and email addresses are content, not metadata.

This definition is not intended to apply to a traditional phone network.

None of this is intended to apply to access to stored communications in the context of how the legislation *currently* treats stored communications.

Other Measures

I believe that there are measures within this policy area that the government *should* be pursuing i.e. measures that relate to community expectations of privacy.

1. The TIAA should be amended to weaken the exemption for ISPs and carriers to intercept for operational reasons. Where possible it should be a requirement that customers give explicit consent to specific violations of their privacy, rather than an ISP or carrier relying on the current blanket exemption in the TIAA or on weasel words in the Terms of Service that the customer had little choice but to agree to.
2. Carriers and ISPs should be encouraged to encrypt all communications that they cause to transit a third country i.e. traffic passing to or from Australia from or to a second country that transits a third country should not be directly accessible to the third country. This is not expected to impact on the ability of LENSAs, either in Australia or in the second country, to intercept since the encryption would be introduced as the traffic leaves the ISP in Australia and removed as the traffic arrives in the second country.
3. It should be illegal for a LENSA to procure or attempt to procure intercepted information

from another country if the communication was sent from or to Australia and it would not have been legal for the LENSA to have obtained the information itself.

4. Section 313 of the TA should be reviewed. It is now evident that this Section is far too broad and vague. To the extent that interception and access to metadata is required, this is already available as specified in some detail in the TIAA. Other areas in which freedoms are compromised by Section 313 should be tabled, debated, justified and legislated on a far finer level of granularity than is currently provided by the vague language in this Section.
5. The regulatory regime that applies to traditional phone network metadata should be separated from the regime that applies to data network metadata. Access by LENSAs to phone network metadata could remain as now, a free for all, with no judicial oversight. Access by LENSAs to data network metadata should involve judicial oversight i.e. a warrant. This becomes particularly important if a broader definition of metadata is adopted i.e. one that includes some content.
6. The legislation should be amended to eliminate the distinction between stored communications and communications that are passing over a telecommunications system (i.e. in transit) i.e. give stored communications the same protection that the communication would have had if it were still in transit. The current legislated access to stored communications is really just a way of bypassing some restrictions on interception.
7. ISPs that store communications, presumably as part of some store-and-forward message delivery mechanism, should be legally obliged to delete those communications as soon as practicable after the communication is no longer required to be stored, presumably aftter delivery is either successful or unsuccessful.
8. The Committee should have made a recommendation that ensures that IGIS is at all times sufficiently resourced to monitor an ever-growing intelligence service. This could take the form of linking the funding or personnel numbers of IGIS with those of the agencies that it has to monitor.
9. Mandatory assistance by telcos and ISPs should be limited to serious criminal matters (including of course terrorist and other similar national security threats).
10. LENSAs should stop targeting politicians and political groups and activists. The current broad interpretation of “national security” is corrosive to democracy.

Earlier Submission

My earlier submission is at

http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs/sub62.pdf

Many of my comments there are not repeated here. Hence this submission should be read in conjunction with the earlier submission.

Appendix A

71. Telecommunications Act

Recommendation 71–1 Part 13 of the *Telecommunications Act 1997* (Cth) should be redrafted to achieve greater logical consistency, simplicity and clarity.

Recommendation 71–2 The Australian Government should initiate a review to consider whether the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act*

1979 (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

(a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;

(b) how these two Acts interact with each other and with other legislation;

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation;

(d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and

(e) whether the *Telecommunications (Interception and Access) Act* should be amended to provide for the role of a public interest monitor.