ABN 85 120 213 381
Level 4, 190 Queen Street, Melbourne 3000 Telephone: 03 8628.5561 Fax: 03 9642.5185
Offices in: Melbourne, Brisbane, Darwin, Canberra, Perth, Sydney, Adelaide

TRANSCRIPT OF PROCEEDINGS
TRANSCRIPT-UNCLASSIFIED

OFFICE OF THE INDEPENDENT NATIONAL SECURITY LEGISLATION MONITOR

CANBERRA, AUSTRALIAN CAPITAL TERRITORY

DR J RENWICK CSC SC, Presiding
MR M MOONEY, Principal Adviser
MS L JOHNSTON, Counsel Assisting
MR J ANDERSON, Solicitor Assisting

PUBLIC HEARING

REVIEW INTO TELECONMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018 (CTH) [TOLA ACT]

08.48 AM FRIDAY, 21 FEBRUARY 2020
DAY 2

EXHIBIT LIST

Date: 21/02/2020

Number Description Page No.

RESUMED **[0848]**

#SESSION 5: Law Council of Australia

DR RENWICK: Ladies and gentlemen, welcome back to the public hearings I am conducting in my capacity as INSLM in relation to the *Telecommunications and Other Legislation Amendment (Assistance and Access)* or *TOLA Act*. I am delighted to have here this morning as our first witnesses representatives of the Law Council of Australia, including the president and other distinguished representatives.

Can I first say, President, as I used to say to your predecessor, I greatly appreciate the enormous amount of effort you've put into these submissions. I always regard them as among the most significant submissions I get, so thank you very much.

MS WRIGHT: Thank you very much, it's a pleasure to be here. As you would be aware, the Law Council is the peak body representing the legal profession in Australia, and the Law Council thanks the Monitor for the opportunity to provide evidence to the review today of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (Cth), which I will refer to as *TOLA*.

DR RENWICK: Thank you.

MS WRIGHT: And for your continued consideration of these really significant issues. The Law Council acknowledges that there is significant benefit to public safety in allowing law enforcement authorities faster access to encrypted information where there are imminent threats to national security, and in order to prevent the commission of serious criminal offences.

Law Council also acknowledges there is merit in facilitating prompt international cooperation and assistance to deal with serious crimes which occur across multiple jurisdictions. But the primary concern of the Law Council is ensuring the policy objectives of the *TOLA Act* is achieved through legislation, which remains reasonable, necessary and proportionate to those legitimate objectives, and is accompanied by transparent and verified with reliable safeguards and controls.

A principal objective of the *TOLA Act* is to increase public safety by providing faster access to encrypted data. The Law Council's comments endeavour to balance achievement of that objective with the need to

ensure legislative clarity and certainty, particularly given the diverse range of agencies that might utilise these powers, and the significant expansion in the range and nature of entities that are now subject to the complex law enforcement legislation. The measures introduced by the *TOLA Act* were developed to address serious criminal activity, including threats by terrorists, crimes relating to the sexual exploitation of children, and crimes engaged in by criminal organisations who use encryption and other forms of electronic protection to mask their illicit conduct.

The *TOLA Act* was designed to address these threats by introducing a framework that improves the ability of agencies to access human readable communications, content and data. However, the measures introduced by the *TOLA Act* go far beyond what is required to guard against these threats, and have broad application applying to the enforcement of any criminal law force in any foreign country, or domestic laws which attract maximum penalties of three years' imprisonment.

Offences of those type are usually dealt with summarily and would not be classified as serious criminal offences in the eyes of the public and in the eyes of the profession. In comparison with other offences which attract significantly higher penalties.

Furthermore, the current decision-making criteria within the *TOLA Act* do not task the relevant decision-maker when making a reasonable and proportionate determination on a matter to examine whether perceived imperatives of law enforcement agencies outweigh reasonable expectations of confidentiality in electronic communications.

The Law Council is concerned that with the exception of technical capability notices, the measures introduced by the *TOLA Act* are not subject to any form of consideration by an independent judicial officer. The Law Council considers there should be ex-ante review by an independent judicial officer, in the case of part 15, industry assistance notices.

In the absence of independent judicial review and little transparency as to the frequency and nature of the use of these measures, there is a risk that the scheme created by the *TOLA Act*, which allows for exposure of such a broad range of private, domestic, commercial-in-confidence and sensitive communications for the investigation of lesser offences would both erode social licence for the continued existence and use of the powers, and undermine the reasonable expectations of confidentiality and privacy.

This can result in other significant consequences for the Australian economy, as data and potentially jobs may be moved offshore to other

jurisdictions where there's greater protection for the privacy and security of telecommunications data. For these reasons, the Law Council considers the measure introduced by the *TOLA Act* would be improved if the definition of serious offences is made consistent with the *Telecommunications (Interception and Access) Act* 1979, and that is offences punishable by a maximum term of imprisonment of seven years or more, instead of the currently-prescribed three years.

Secondly, if the reasonable and proportionate test within the *Telecommunications Act* specifically requires the decision-maker to determine whether perceive law enforcement imperatives demonstrably outweigh the reasonable expectation of confidentiality in the electronic communications between individuals and businesses, and decisions made under part 15 of the *Telecommunications Act* are to be made by a judicial officer. In the alternative, it's recommended that judicial review of part 15 decisions should be available.

A number of further recommendations in relation to the operation of the *TOLA Act* can be found in our written submissions to the review, but the key ones as we see them - and we thank you again for the opportunity to appear today, and we're very happy of course to respond to any questions that you may have.

DR RENWICK: Well thank you President very much, that's very helpful. Can I ask, have you had an opportunity to look at my opening remarks yesterday?

MS WRIGHT: We have.

DR RENWICK: All right, so to start perhaps at the top, some people say that firstly *TOLA* is not so significant, because actually obtaining the content or the metadata is something which is going to - that's going to be obtained by a pre-*TOLA* warrant or authorisation method. As you can see in my opening, I'm fairly sceptical about that, because after all, the Parliament was told the reason for *TOLA* was that the internet had gone dark, particularly on content, and that but for this, you might have something which was simply unintelligible.

So in broad terms, you agree with my scepticism about that?

MS WRIGHT: Yes we do.

DR RENWICK: All right. So the next step I think is some people also say, "Well, the existing methods of say, having a judicial officer acting in a personal capacity is perfectly all right." But in relation to that - and this

informs my thinking about the AAT, it seems to me firstly - well, the example I gave yesterday to ASIO, at the risk of rehearsing it, was if a warrant seizes my personal diary with writing on it, I know what's been seized, I know it's got my fingerprints and possibly DNA on it. In other words, I know reasonably what the authorities might be able to do with that.

But if they seize my mobile phone, and if for example I'm required to provide a password to it, I simply do not have a full appreciation of how that might be used. And part of that - the reality in which we all operate, is that DCPs monetize our personal information all the time, technically we may consent to it, and the ACCC as you know are doing their own inquiry into that, about whether that's real consent or not, but it's part of the world in which we live.

In other words, we have no idea really how much we're giving away, and it occurs to me it's therefore not good enough just to say, "Well we have these systems which worked in the past," for example, giving access to a telephone call, you know, which is technically content or data in motion. It just seems to me that a more informed form of approval is now required, because so much of what is in the mobile phone - to take an example, is unknowable, but certainly unknown. Would you care to comment on that, any of you?

PROF LEONARD: Peter Leonard. There are, I think, a couple of things that distinguish the position today from the prior history. One is that often the information is residing not necessarily on a mobile phone, which I as the user of that mobile phone know is the subject of review, examination by law enforcement agencies. It may be law enforcement agents dealing with the cloud or the data on the cloud. So often the affected individual is not even aware that there is the relevant investigation occurring.

That means that the controls and safeguards over how the processes occur become even more important. Secondly, the range and probative value - evidentiary value of data associated with individuals continues to expand, and often the mosaic of information available through the metadata is actually more telling - more of interest to a law enforcement agency than actually what was said, so the metadata may be in fact more sensitive than the content of the communication, suggesting that at least the same standard should apply as applies to the content of communication.

And I think the third point, which is often missed, is that this legislation has substantially expanded the range of entities which are DCPs, with the result that many entities now will be receiving notices or other process that may not have the same interest in balancing interests and limiting

disclosures as, for example, the Silicon Valley giants have had as a result of public expectations of transparency and reporting as to transparency. So many of the providers that are now receiving these notices may not balance the interest of the affected individual in the same way.

And that I think means that the controls and safeguards in the system must rely to a greater extent upon the involvement of independent individuals capable of assessing societal interests and balancing those against the interests of law enforcement. Not saying that the interests of law enforcement and security are subordinate, but the balance is best judged through an independent judge who can synthesise the view of the affected individual, who doesn't even know often that this is going on.

DR RENWICK: And a technically-informed judicial officer.

PROF LEONARD: Yes.

DR RENWICK: Because Professor, you may be expert on this, but I know, having look at this, there are many things I still don't understand about the technical side. So I think I see you all nodding. In broad terms, this goes to the idea of a judge or former judge making such decisions with a technical member as well, who is independent but highly-qualified.

PROF LEONARD: Yes, I think it's too much to expect those skills to reside in one head in the current day.

DR RENWICK: All right.

DR MOLT: That is out position, yes.

DR RENWICK: All right, well can I ask you to look at section 317(j)(c) of the *TOLA Act*, just to talk about some of these issues. And there are similar provisions for the TANs and the TCNs, that's for a TAR. And it raises some very large issues.

So President, you talked about the reasonable expectations of privacy, and I suppose that might be a close synonym to subsection (h), the legitimate expectations of the Australian community relating to privacy and cybersecurity.

I asked a number of witnesses about this yesterday, and I think it's fair to say there's no universally-held view about what those expectations are, and I daresay they change over time. And so I suppose that's relevant to two things, the need for an independent person to make the decision, the

desirability of publishing at least some decisions or part of decisions, which provide an analysis of what that means.

MS WRIGHT: Yes, I think that's exactly right. There need to be, I think, clear legislative criteria that guide that decision-making process so that a proper balancing is made between those legitimate expectations that the community has for the security and privacy of their data against, obviously, the legitimate expectation that we're kept secure from bad actors, and so I think there would need to be a range of relevant factors to determine what is reasonable and proportionate under the circumstances.

DR RENWICK: So then also, if you look at (e) and (f), the availability of other means to achieve the objectives and whether the request, when compared to other forms of industry assistance, is the least intrusive form, effectively, in relation to the person who is not the target of interest, or the subject of interest.

One of the concerns I've got about the eligible judge model at the minute is typically what happens is the judge would receive the papers in private chambers, there would be a sworn affidavit, and it would set out these matters. But there's no hearing. If the judge says, "Well I haven't got enough information," they can ask for more, and of course they've got the option of saying no.

But the advantage of the AAT is at least in some cases, perhaps where there's novel technology, the AAT can choose to have a proper hearing, an inter-partes hearing. There's also the advantage that the AAT would allow - you see, I think the industry people yesterday agreed that they wouldn't want to share, necessarily, their closest intellectual property secrets with law enforcement and intelligence, and the latter wouldn't want to share their current operational objectives with the DCPs.

So the AAT provides you with a way - they're more inquisitorial, they inform themselves, they can weigh those matters up. There might be a difficulty doing that in a court case, it think.

MS WRIGHT: Yes, look, I mean, our preference has always been the judicial model, but we absolutely do appreciate that the AAT model that you're suggesting is vastly superior to what's there now, and will provide real opportunity for these things to be tested and weighed up.

DR RENWICK: And can I ask you this - and I'm not saying this in a political way of course, but from time to time there have been comments about the depth of experience perhaps, and the qualifications for AAT members. What would the Law Council's - say this was to be vested in

the security division of the AAT, how would you see that working in terms of appointments and the like?

MS WRIGHT: Well you would want to see appointed to the security division perhaps judges, judicial officers, who do have expertise in that area. That would be the best way to ensure a proper understanding of the issues that are coming before the AAT to be weighed up and considered. If a person hasn't got the experience in those areas, they're not going to be able to make an informed decision.

DR RENWICK: All right.

PROF LEONARD: I think it is actually quite a complex judicial balancing that is required here, and Mr Renwick, you identified the issues around trying to work out what are legitimate expectations of the public and balancing - and also taking into account other subjective factors, as well as the technical factors. And I think that suggests that the appropriate appointee would be a senior practitioner, perhaps a retired judge, who's well-used to apply complex balancing factors such as this, and informed by an appropriate technical expert.

DR MOLT: The retired judge approach would also add to the perceived independence of the process, which might assist with other arrangements such as the Australian/US agreement that's proposed under the *Cloud Act*.

DR RENWICK: Yes, and certainly the fact that the British have been able to get a *Cloud Act* agreement where IPCO is only retired judges suggests that the *Cloud Act* doesn't require serving judges, and so either Tribunal members who are in that capacity judges, but also retired judges there, yes. No, I agree with that Dr Molt.

And of course, this model also would mean that we wouldn't need to consider the arguments about the appropriateness of the Attorney-General granting the TCN, because it would be the AAT granting the TCNs, the most intrusive ones.

DR MOLT: That's right sir, yes.

DR RENWICK: Right, can I just ask this - there's been a lot of - I'm sorry, is there a question?

MS GANOPOLSKY: Can I just add to the discussion about obviously the composition and the qualifications that would be required?

DR RENWICK: Yes.

MS GANOPOLSKY: Which are perfectly in context. I think we would be greatly assisted if in the actual legal framework, once it's settled, where that decision-making authority sits, there would be criteria that that decision-maker of the collective decision-making body would have regard to, and we would be greatly assisted, with existing concepts of proportionality, that are well-developed, particularly in European law, and the factors that would need to be taken into account in order to address the question of proportionality, and if this is entrenched in our legal environment, we can then deal with both the dynamic nature of the expectations and the community, but equally we could have some certainty of law and perhaps with a sunset or some sort of a review mechanism.

DR RENWICK: Well certainly my approach with this is that the statute is the place to put those things rather than - or possibly some delegated legislation. I am not a fan of the idea that just because it might have been mentioned in the supplementary revised explanatory memorandum, that's enough. Because we've all seen cases where judges say, "Well that's jolly interesting, but the statute is the thing." So thank you very much, I think that segues nicely into the argument about systemic weakness and systemic vulnerability. So certainly you would've heard me say yesterday that I think there should be examples given of what is and isn't a weakness or vulnerability which crosses the line, because one of the things that bedevils this debate is that fact that a lot of the arguments are at a theoretical level, and I think there do need to be some real - it can't be exhaustive of course, but some real examples of what is acceptable and what isn't acceptable, and that's then something which - when it comes back before the PJCIS, there can be further debate and comment about. And I see you all nodding there, so I assume that's conceptually something you're happy with.

PROF LEONARD: I think there are two levels of issue here, one is the use of systemic in conjunction with weakness or vulnerability, and I'm not sure what that word adds to a weakness or vulnerability that is outside the specific subject matter of the notice.

In other words, I think systemic is a redundancy which creates uncertainty. The other is class of technology, and I'm not sure that even giving examples in the statute will assist to give any real guidance on words "whole class of technology". I've practiced technology law for 35 years, and I have no idea what a "whole class" of technology is. And when I read the Home Affairs' industry assistance guidance, what it tells us is that the term is deliberately broad and captures general items of technology across and within a category of product.

It encompasses all products which share similar functional attributes, for example, mobile communications technology, a particular model of mobile phone, a particular type of operating system within that phone, or a particular type of software installed on an operating system.

This definition is intentionally wide to capture product ranges and layers of technologies within products. Well, I read the words but I don't actually understand how they help me to make a decision.

DR RENWICK: So pleased you said that, because you're not alone in that. So can I just unpick some of that and discuss it with you. So the first thing is - I don't know whether you were assuming there that the TAR or the TAN or even the TCN would necessarily even be specific to a particular warrant, because I think I can say this, having looked at the paperwork, you know, that shouldn't be assumed. I mean, it could be, and Schedule 2 powers, for example, are more likely to be. That's a computer access warrant, for example. But here I think the concept is, "Well, I'm the AFP and I want to be able to make this sort of thing intelligible or accessible, or do a listed act or thing," and that will extend beyond perhaps a particular subject of interest.

So it's in that context that I think we come to these opaque words - and I guess you've got to read the definitions in 317(b), with the extended definitions in 317(z)(g), where they're given extended meaning.

The first thing which occurs to me, I think, is that I'm not sure that you actually need to have a definition both of vulnerability and weakness, I'm not sure. I mean, they're dictionary synonyms really, and maybe you just need a single concept.

I take your point about a whole class of technology, what is it? I think it runs the risk of being whatever the applicant wants it to be. Is it all iPhone 10s, is it all iPhones, or as someone said yesterday, is it all iPhone 10s operating in Sydney at a particular time? I don't think anyone really knows.

The next thing - so I take your point about that. And then yes, so that's the class of technology point. And then you've got the extended definition in 317(z)(g). If you look at my opening remarks of yesterday if you happen to have them there, I put in a footnote or an endnote - endnote little five is the definitions contained in the current Bill, the *Repairing, Assistance and Access Bill*, which has been put forward, and there was a bit of debate about

this yesterday, so you'll see that on page 23, I think, of the - or it's the second last page anyway, of my opening.

And so what this seeks to do is talk about prohibited effects, and I must say I'm interested in your views. It seems to me there's something to be said for talking about prohibited effects.

PROF LEONARD: Yes, we in preparation for today were giving some thought to how the definition of 'prohibited effects' might be crafted, and specifically drawing the distinction between the particular instance which is the subject of the notice, and again, picking up your point that the instance might not be a single decryption, a single case, it may apply to a series of cases described by a class.

But the relevant issue is, is there a weakness or vulnerability - same word, I agree with you that they're synonyms - that is introduced outside that instance as described? And I think that's where the words need to go, and I think there also needs to be some assistance given to the decision-making through disclosure by the relevant law enforcement agency as to what its view is of whether there is any weakness or vulnerability that would flow from what it is that they are requesting.

So it shouldn't be as it were, left to the provider to prove the negative, that the result of this is to create a vulnerability. Because often the question will be best understood by the law enforcement agency that's seeking the appropriate order.

DR RENWICK: Yes, so just to pick up on that, so firstly the head of ASIO yesterday said it wasn't his intention to create backdoors or to weaken encryption more generally, and that's a sentiment, I think, which is generally shared by people giving evidence.

So the question then I guess is if that is indeed not the desire to weaken encryption generally or to create backdoors, appreciating that backdoor is a bit of a loaded term, I wonder whether - can I ask you to look at proposed section 317(z)(g)(iv).

PROF LEONARD: This is the proposal in your footnotes?

DR RENWICK: Yes, so this is the proposal in the current Bill before the Parliament - before the Senate, to be precise. And I'm just interested in the words - if we look, say, at subsection (iv), if you just delete the words 'or may' in the second line and if it was to read:

Effectively, a prohibited effect is something that would create a material risk that otherwise secure information would, in the future, be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.

I wonder whether that's getting closer to the concept you're talking about?

PROF LEONARD: Absolutely. Olga, I think you'd given some thought to risk factors guidance.

MS GANOPOLSKY: I think that's right. We would have to move the language to capture not just the technical weaknesses that are created, but the impact of those.

DR RENWICK: The effects.

MS GANOPOLSKY: The effects of those, and that would take you back to the discussion about proportionality and some things highly relevant. So the sort of matters that we would recommend addressed would take us to the type of information that would typically be in those services. The service that's actually being provided - so I think there would be a huge difference between a service that's provided as part of a health care industry versus a service that's provided more generically, and we would also call out some industries that are more sensitive to overseas legislation, such as some of our service providers who work with the EU and may have been affected by the extraterritorial effect of legislation such as GDPR.

So you would have to start looking at the context of the information cycle and how that information behaves in a particular industry or a particular point in time, at least by reference to factors.

DR RENWICK: Sorry to interrupt, just so I understand that - I understand the point that there are some pieces of information which are inherently more sensitive, and health records might be a good example to give. And no doubt that this something which should be considered, and could perhaps now be considered under the rubric of what's reasonable and proportionate in 317(j)(c) with additional factors.

But I just wonder whether - I mean, isn't there a universal desire to not weaken encryption so that it's able to be illicitly accessed by an unauthorised third party. So I just wonder - could we just focus on the words of subsection (iv) using the word 'would' rather than 'would' or 'may'. Can I just ask you to critique what's there in that proposed - and I'm happy for you to take it on notice, but wouldn't that achieve - wouldn't that state

the prohibited effect that you're seeking in subsection (iv) or not? Tell me if I'm wrong, please.

MS GANOPOLSKY: And I'm happy to do some further drafting and demonstrate how it could be made tighter, but I think it's definitely an improvement.

DR RENWICK: Sure.

MS GANOPOLSKY: The additional scope for improvement would come from making it obvious that you're not looking at simply the encryption element at a technical level, you're looking at the effect of the security and what the Europeans would call state of the art protection as it may be required in certain context, and gives you that balancing exercise that you're trying to achieve. So we'll happily draft some - - -

DR RENWICK: See that's what I - I must say, I just don't quite understand. I've got your point that there are categories of information which deserve higher protection, I understand that. And what I'm suggesting, I think, is that that's what you build into the reasonable and proportionate test.

MS GANOPOLSKY: Okay.

DR RENWICK: Are you saying in addition in relation to the prohibited effects in something like subsection (iv) that there be an additional technical concept?

MS GANOPOLSKY: Yes.

DR RENWICK: And I just don’t quite understand it, what's the concept?

MS GANOPOLSKY: The concept takes us back to the concept of privacy as a separate human right that sits at that community level. So we accept the fact that a certain form of intervention could create a compromise, the compromise for many. And what we're looking to make clear in the legislation is that if you are in that decision-making environment where you are considering the effect on many, you take into account the following considerations. So yes, it could be done by properly amending other sections of the legislation, but they do need to be consistent with each other.

DR MOLT: I might just add to what Olga has said. This subsection (iv) which you've pointed us to, it's certainly an improvement on what currently is the case, and the Law Council, in our submission, we did support this notion of material risk as really taking it up to the next level to demonstrate what's at stake in the decision-making process.

I think the terminology around systemic weakness or a systemic vulnerability that's still used in this subsection, Peter has already mentioned some of our concerns around the use of the word 'systemic'.

PROF LEONARD: Just one last quibble on this particular drafting, the words 'unauthorised third party' to me are a little bit problematic. I think they are fine insofar as they cover unauthorised third parties, but that then leaves the question as to the first and second parties, and their access in the future, which may be unauthorised. And you wouldn't want this to be - - -

DR RENWICK: You mean the agency?

PROF LEONARD: Yes.

DR RENWICK: I see.

PROF LEONARD: So a vulnerability that enables the agency in the future itself to access without authorisation.

DR RENWICK: Yes, I mean I think the agencies' answer would be - and they're coming along and they'll speak to it, but I think they would say if the Act says if you needed a warrant, State of Federal, you still need a warrant or authorisation. Yes, all right.

PROF LEONARD: And the second point is that the service provider is itself a party, so the issue may be vis a vis the customer and the service provider, and creating a vulnerability in what the customer thinks is a secure system that enables access by the service provider.

DR RENWICK: Yes, I mean certainly just in relation to that, the way I read - and I think the way the team reads the current *TOLA*, is a TAR, a TAN or a TCN doesn't prevent the DCP from imposing a patch, so for example, it might be a single-use and then the company can impose a patch and fix it up.

A related point I think which the DCPs have made in written submissions particularly is, they say, "Well we don't want to lie to our customers about what we may or may not do," and I think the response from the agencies to that would be, "Well firstly, many DCPs do say in their very widely expressed terms and conditions, 'We may assist law enforcement when required by law.'" Some even are a bit more specific and say in effect, "We've got a law enforcement switch or function, which if there's a proper lawful authorisation, we might do it." And the other point I think which would be made is that there's nothing wrong with a company saying, "We've

never received a request under Schedule 1." That's permitted under the current law. At least for the preceding six months they are able to say, "We've received the following numbers of TARs, TANs or TCNs," they can't otherwise identify for operational reasons who it's from and what they're about, but - so those are some of the issues.

So anyway, on systemic weakness and vulnerability, I know you've put in submissions about this. If there's anything further you want to say on that, by all means.

MS JOHNSTON: Sorry, Laura Johnston.

DR RENWICK: You need to push your button.

MS JOHNSTON: Yes, Laura Johnston, I'm the counsel assisting. I just wanted to take you to one point, a recommendation at paragraph 51 of your submission, and I can read you out the relevant part just to save you finding the page. In essence it says:

> *Subsection 317(z)(g)(i) the limitations on industry assistance notices, should be amended to prohibit an industry assistance notice from requesting or requiring anything that might require a DCP to either implement or build any weakness or vulnerability into a current or proposed product of service.*

And I've heard here what Professor Leonard and other panellists have said about your view of the lack of content of the term systemic. My question is just am I understanding the submission correctly, that it is taking issue with any form of weakness or vulnerability that might be introduced, whether it rise to the level of a systemic weakness or vulnerability or otherwise.

DR MOLT: Yes, so that's correct in terms of the recommendation. And I think the context in which we were making that recommendation is really around the concerns that we have with the term "systemic" and what material difference that adds.

PROFESSOR LEONARD: I think it comes back to the discussion that we were just having, which is that the notice should make a fair disclosure of what is sought and any ongoing nature of the access or decryption capability that is being sought. And anything that is outside what is there specified should be regarded as a potential weakness or vulnerability, because it's not within the ambit of what is being authorised.

And to then introduce the word "systemic" raises a question as to what that means, and what system we're talking about. And I think that amendment that we've just been discussing is useful because it focuses back on the question of whether that which has been encrypted, there's a material risk that that might be accessed by an unauthorised third party in the future.

So I think it creates a clearer distinction between that which is the subject of the notice, and that which is outside the notice. And that's a better focus than trying to define what is systemic and what isn't.

MS WRIGHT: I think that's right. I mean, clearly, in order to intercept a target person's data, you have to introduce a weakness into that target person's data. We're not saying that that ought not be allowed, but it must be within the context of the notice itself.

MS JOHNSTON: One of the reasons I raise it is because I've been trying to grapple a little bit with what are some offline real-world analogues to these powers that do exist, and where we draw that line in the offline context.

And one that comes to mind - and I appreciate again you don't have this legislation in front of you - but Part 1AC of the Crimes Act deals with assumed identities, and in particular Division 3 contains powers whereby agency heads can direct government agencies to issue, in effect, false identification documents to bolster the credibility of an undercover operative or other person using an assumed identity.

Even in the private sphere, while they can't compel private providers to do the same, they can make requests. And I expect that is things like false credit cards or bank accounts and the like, although I'm speculating from the legislation. On one view, whether we call that a systemic weakness or just a weakness or vulnerability, to my mind, that does, on some level, create some weakness or vulnerability in our system of identity verification that we all use on a day-to-day basis.

I suppose my question is, if we accept that - and that's on the books already, in the offline context - we accept that that serves a legitimate purpose, we accept that it could hypothetically affect everyone, but in reality its consequences come most directly to bear on someone who's presented that false identity document and is probably the suspect of a criminal investigation.

If we accept that in the offline context, is there some relevant distinction that means we can't tolerate that degree of weakness in the online context?

PROFESSOR LEONARD: I think there is a legitimate distinction, and that is that the purpose of the false identity in that credit card example is a particular - I assume - to ensnare, entrap, a particular individual believed to be doing something illegal. And it doesn't undermine potentially broader trust in the system; whereas, in the digital world, digital trust of citizens is affected by activities that may not relate to their specific digital activities.

So we always need to consider, as we look at the digital world, the effect on broader digital trust of citizens, and potentially undermining that trust. Now, often a degree of undermining that trust will be justified in national security or law enforcement, but I do think that you can't take the digital world as an exact analogue of the physical world, because of that different nature of the digital system.

MS JOHNSTON: Just finally on that though, if the agencies were using it - and this is again hypothetical - if they were using it in a similarly targeted fashion, would that address your concerns, or are you still concerned in the sense that the public perception is different in the digital space as to what can and can't be trusted?

PROFESSOR LEONARD: An interesting and difficult question; I think I'd need to take it on notice.

MS JOHNSTON: Fair enough.

DR RENWICK: Well, one final question then, relates to the defences available to DCPs under 317ZB(5). And a number of DCPs have dealt with this and said where a civil penalty order is sought against them, it is a defence if they prove the compliance with the requirement in the foreign country would contravene a law of the foreign country. And they talk about a requirement under a technical notice to do an act or thing in a foreign country.

I think the point a lot of them have made, the DCPs have made, is that that's not actually how things work in the real world, in other words, things are not done solely in a foreign country anymore; they're done over the Internet. They may be done in two or three places at once. The participants - to use the language of the criminal law, the conspirators - are in different places.

And so I take it you would encourage an amendment which would respond to the real-world situation where the actions take place in more than one country, including the foreign country?

DR MOLT: I think that's right. So we would be likely to support an amendment which makes it clear for example, that where there's operations or providers, where there's a partial impact both in Australia or in a foreign country, that it's made very clear on the face of the legislation that they may also fall within the ambit of the defence.

MS GANOPOLSKY: I think that's right. The critical question - just coming back to the issue that was explored earlier - is actually the diffuse nature of the impact because of the instantaneous collaboration that naturally happens online.

And so if you go back to the question of consequences and who bears them, the group is naturally much larger in a digital environment than it is in the physical sphere, and not obviously apparent at the first cut. So you're dealing with unintended consequences that are multiple waves of the consequences, if I can frame it that way/

DR RENWICK: Anything further from you?

MS WRIGHT: Look, I think just a general comment.

DR RENWICK: Yes, please.

MS WRIGHT: Just in terms of, because Australia doesn't have an overarching bill of rights or charter of rights, it's even more important for legislation of this kind to give guidance to decision-makers in relation to that balancing act that they've got to undertake in this legislation. So in the absence of that human rights legislation in Australia, it's even more important.

DR RENWICK: Well, look, can I thank you all very much? As you know, this is my last public inquiry as Monitor, because my term finishes at the end of June and there'll be a new Monitor. So can I publicly thank the Law Council? Your assistance to me has been absolutely invaluable over the last three years, so thank you.

MS WRIGHT: Thank you.

DR RENWICK: And shortly, we will have Ms Genna Churches from the Allens Hub for Technology, Law & Innovation.

#SESSION 5: The Allens Hub For Technology, Law & Innovation

DR RENWICK: We welcome Ms Genna Churches, speaking on behalf of the Allens Hub for Technology, Law & Innovation. Welcome, Ms Churches. Did you have an opening statement?

MS CHURCHES: Yes please, Dr Renwick. Thank you for the opportunity to give evidence to this review. Given the issues raised in the Allens Hub submission, we're very pleased to hear the reflections in your opening address given yesterday, and the thoughtfulness of the evidence provided so far.

However, the importance of this review cannot be underestimated. The TOLA Act was controversial from its introduction, but was passed due to a perceived necessity. Unfortunately, the legislation suffers from similar issues that we see across other legislative responses to perceived technological crises: a lack of clarity. This is particularly apparent in the context of the government's concern to keep up with data technologies.

Take, for instance, the metadata retention scheme and the recent data-matching bills. We are all aware that technology will continue to have a great influence over our individual lives, and shape our society, however this means that we equally must become better at drafting legislation which deals with technological issues, and addresses the actual objective to be achieved; in this case, dealing with faster access to encrypted communications for national security, terrorism, and other serious offences.

Our submission covers the primary issues of transparency and accountability. First, we highlight the importance of boundaries for national security and law enforcement powers, to collect, assess, analyse and act on data, whilst maintaining public trust. This requires the creation of laws which are clear, coherent, simple, and comprehensible.

While we accept there are certain aspects of such laws which require operational secrecy, that secrecy must be kept to a minimum. At the very least, the public are entitled to translucency; that is, as much information as they can be provided with, up to the point where it may compromise operations. This includes clarity on what precisely the Act requires, and clarity on the position taken on controversial technical questions and how that position was reached.

Operational secrecy itself needs to be justified and explained publicly; the reports of David Anderson QC in the UK are an excellent example of this. And we note your interest more broadly in some UK examples. However,

we see difficulty in explaining the current regime to the public. Even the Department of Home Affairs concedes that the legislation is complex, and as seen by the submissions and evidence yesterday, has a wide range of interpretations and understandings of effect.

Given the potential ramifications on broader network security, potential use by autocratic regimes and bad actors, and the impact on the Australian tech industry, clarity in legislative drafting and considerations of the impacts more broadly must be seriously undertaken; this includes appropriate reporting mechanisms, currently absent from the legislation, which provide qualitative insight into the report of requests and notices. This should include a breakdown of the types of offences, convictions of offenders, and the discovery of plots, and reflect on the overall effectiveness of the scheme.

An understanding of the effectiveness must be maintained to ensure intrusive legislation such as this is operating as it should. Overall clarity within the regime is even more important, given the revelations that the data retention and access regime may not be working as legislators intended. The TOLA Act bridges across the *Telecommunications Interception and Access Act*, and the *Telecommunications Act*, the same pieces of legislation which are known to cause duplication, confusion, conflict, issues with interpretation, and have been the subject of calls for complete review or revision, since 2005.

This means there is a very real risk that the TOLA Act will, at some point in the future, reveal instances of mission-creep, unlawful access, or unforeseen or unwanted interactions between other provisions, or external legislation, which may permit a far greater incursion into the privacy of the individual than was originally anticipated.

We note the discussions raised yesterday regarding the proportionality of the regime, and concerns that the interests of the individual are not being considered as fully as they should be, and EU jurisprudence, which provides guidance on that proportionality.

We close by highlighting that this legislation does not make transparent to the public the compromises at stake between broader network security and agency access to unencrypted communications. We reiterate that complex legal drafting and patchwork solutions to agency demands, or perceived shifts in technology, rather than deliberate policy, are barriers to transparency and are not the proper basis for proportionate responses to societal objectives.

Thank you.

DR RENWICK: Thanks very much. All right, well let's start with the question of transparency. You've heard my example, today and yesterday, about the transparency involved if my paper-based diary is seized, and the lack of transparency if my mobile phone is seized, even if you don't include what's held, linked to the cloud.

So that's not a criticism of the DCPs in this context; it's just that's the world in which we live: that we don't know, and we probably aren't able to fully know, how personal information is used, sold on, analysed, and all that sort of thing. So when you're talking about transparency, you start from a different base, don't you, than you do with a paper-based traditional approach?

MS CHURCHES: Of course. When we're talking about the data, the difference between the data in your diary and the data in your phone, there is a disparity. And I take on board your comments that we really don't know what is on our phones, what can be inferred.

But there are a number of differences between the diary and the phone. So firstly, the diary may be the subject of a search at a premises, of which you would know your diary has been intercepted, for want of a better word; it's been read, it's been detained, it's been scrutinised. Whereas, there is the possibility that your mobile phone, you may not be aware that your mobile phone has been accessed and that data has been removed or copied, or altered in some way, on your phone.

So we've got that disparity between the two straightaway. But your point about the cloud and what's there, and Google and other bodies perhaps taking data and doing things with that data; you gave the example of knowing your gait and those kinds of things. There is a difference there between what the government should be able to collect - and I appreciate perhaps others should not be able to collect your gait information as well - but there is an opt-in for those other organisations; they're private organisations, and there is a process of opting-in.

Whereas, with the government, unfortunately we've all opted-in because we are subject to governmental laws. So in that perspective, there is a difference between that private and governmental aspect. We've opted-in to the government, that is there, it can be done surreptitiously. And I know that there was some discussion, I think about the ACCC, inquiring into just how those private organisations use our data.

DR RENWICK: So you'd agree with me then that whoever is making the decision needs to be fully technically informed about what it is they're getting access to, and the consequences of getting access?

MS CHURCHES: Absolutely. And even if we do have a legal professional, or a retired judge, or you were suggesting the AAT model, who perhaps is technologically savvy, I struggle to believe that one singular mind can have sufficient knowledge of the movement in IT spheres and technology to actually be able to fully conceptualise those potential ramifications down the track.

DR RENWICK: So then, the British model which I have referred to, in IPCO, has 16 retired judges, very senior retired judges, who become specialists in the operations of particular agencies. And they are assisted by presently about half a dozen really very, very distinguished technical and scientific people whose expertise covers the full likely range. So that's something you would support, isn't it, a range of experts, depending upon the technical issue which arises?

MS CHURCHES: Exactly. And that was an excellent example that you gave yesterday. Our only issue was that something that was raised yesterday about the impartiality of those experts, that they must be impartial, you know, they can't be favouring one side or the other, or perhaps work for a law enforcement agency part-time, et cetera.

DR RENWICK: Sure. But those concerns, providing they were sufficiently independent, that wouldn't extend, for example, to them being consultants to the people who audit the operation of this scheme, for example, the IGIS or the Ombudsman?

MS CHURCHES: I'm not sure; I'd have to consider that a little bit more in depth. But I'm not sure on that front.

DR RENWICK: Okay. Can I ask you about your comments on revealing the purpose? In order that there be public trust, I think you said, there should be some revelation of the types of operational reasons, there should be a justification for operational secrecy. So I suppose that could happen in two ways, without jeopardising an ongoing operation; one is that that would have to be justified to the independent decision-maker. So that's one aspect which you would support, I take it?

MS CHURCHES: That's right.

DR RENWICK: And the other aspect might be, and obviously secondly, the IGIS and the Ombudsman have access to everything after the event, so they're able to ask questions about, "Well, why did you say this? Why did you say that?" So that's something you support, I guess?

MS CHURCHES: That's right. And if they could then provide some tangible, qualitative statements about, "These are the statistics we've viewed. These are the understandings about those notices that were issued, and we believe the regime is working because there's been these convictions, we uncovered these kinds of plots, therefore it's being effective."

DR RENWICK: And so that could be done in a number of ways: it could be in their annual reports for example, but there could also be I suppose, additional obligations on the agencies themselves to reveal a greater breakdown in the use of the powers, and what has followed from them. Yes, you'd agree?

MS CHURCHES: That's fine.

DR RENWICK: Yes.

MS JOHNSTON: Just on that note, perhaps one way of doing that would be, holding aside from the statistical analysis, to pick up on the qualitative point you mentioned; we'd discuss the possibility perhaps of there being prescribed forms. Would it address your concerns, or would it be sufficient if it were to address, in general terms for instance, the type of listed act or thing, or even failing that, the type of eligible activity that the DCP was able to, or was required to, exercise the powers in relation to?

What I'm thinking of here is that the *Court Suppression Act* in New South Wales deals with, obviously, highly sensitive material; it grapples with that issue of making an order that's sufficiently clear, on its face, as to the basis on which it's made, without giving up the very secret it's trying to protect. And the way that that legislation deals with that is to require that each order made under that Act identify, in broad terms, one of the five or six statutory bases available on which it's made, and thereby gives essentially enough information in the parliament's view, about it.

I'm thinking is there something similar that you might be able to propose for this context?

MS CHURCHES: Well, I would probably have to take that on notice, but my initial response would be the concern that we've only sort of got three basic provisions which we can issue a TCN, a TAR or a TAN. I'm just wondering what sort of specific provisions you would point to within the TOLA Act to be able to give that clarity? I just don't know that those provisions are sufficiently clear in the TOLA Act to represent that clarity.

MS JOHNSON: Look, I'd be very happy for you to take it on notice. I think what I'm envisaging, just thinking out loud, is less about necessarily the justification or rationale, but perhaps more just to give the public some confidence that it has been issued to a DCP in relation to an eligible activity of that DCP; and then in some or other general term, what kind of listed act or thing it is in relation to.

So I suppose the public would have some ability to trust that it falls within the broad statutory criteria. Obviously, the specifics would need to be kept operationally secure.

MS CHURCHES: Yes, well in that case, that is the line of thought that we're progressing down, and we're happy to put something together more thoroughly for you.

DR RENWICK: Thank you. Just last question from me, Ms Churches. If you look at your submission of 25 October, at the bottom of the first page?

MS CHURCHES: Yes.

DR RENWICK: You talk about the need for powers to collect, access, analyse an Act to be democratically based, and you refer to the Open Government Partnership. Could you briefly expand on what you mean by that?

MS CHURCHES: Okay. what we're sort of saying is that right now, we don't believe that there are sufficiently tight, clear and unambiguous terms around what powers there are to collect. I know the hearing has discussed that there has to be a warrant, or whatever. If a warrant was required before TOLA, it's now still required after TOLA; so what we're suggesting is that that is not really sufficiently clear within the TOLA Act.

We note that that's a number of issues which fall within clarity: we've got definitional issues and those kinds of things. So that's the reference we're making there.

DR RENWICK: Thank you. I think we don't have any other questions, but can I say Ms Churches, we very much appreciate your attendance here today and yesterday, and also the submission on behalf of the Allens Hub. So thank you so much.

MS CHURCHES: Thank you very much.

#SESSION 5: Independent Commissioner Against Corruption (ICAC SA)

DR RENWICK: And I invite I think the South Australian ICAC representatives to come forward. I welcome you gentlemen from the ICAC of South Australia. Could you identify yourselves for the transcript, and if you have an opening statement, can I please have it?

MR JENSEN: Thank you, yes. Mr Rod Jensen, Director Legal Services at the ICAC.

MR BAKER: Andrew Baker, Director of Investigations.

MR HEWLETT-PARKER: Andrew Hewlett-Parker, Team Leader of Specialist Services.

MR JENSEN: And we do have an opening statement, thank you. Thank you for your invitation to appear today, and to provide an opening statement.

The Honour Bruce Lander QC is the Independent Commissioner Against Corruption in South Australia. The Commissioner is the inaugural Independent Commissioner Against Corruption in South Australia, having been appointed to the role in 2013, pursuant to the *Independent Commissioner Against Corruption Act* of 2012, which I will refer to as the *ICAC Act*.

The *ICAC Act* sets out the Commissioner's functions and powers. The primary objects of the *ICAC Act* include the identification and investigation of corruption in public administration, and the prevention or minimisation of corruption, misconduct, and maladministration in public administration.

Whilst any potential issue of corruption, misconduct, or maladministration in public administration may be the subject of a complaint or report under the *ICAC Act*, the Act specifies that it is intended that the Commissioner's primary object is the investigation of corruption in public administration.

Corruption is defined widely in the *ICAC Act*. In essence, the expression "corruption in public administration" covers any criminal offence committed by a public officer while acting in his or her capacity as a public officer. The definition extends to the actions of former public officers and includes ancillary offences such as aiding and abetting.

Under the *ICAC Act*, complaints and reports about potential issues of corruption, misconduct or maladministration in public administration are received by the Office for Public Integrity, or OPI, which is created by the *ICAC Act*. The OPI is responsible to the Commissioner for the performance of its functions.

The OPI assesses the complaints and reports received. If a matter is assessed as raising a potential issue of corruption in public administration, it is referred to the Commissioner for further consideration. If the matter is assessed as raising a potential issue of corruption in public administration that could be the subject of a prosecution, the Commissioner can investigate the matter or refer it to South Australia Police or another law enforcement agency for investigation. If the Commissioner decides to investigate the matter, the Commissioner must oversee the investigation.

In such cases the Commissioner has available to him a range of investigative powers, some of these are contained in the ICAC Act, for example, the power to enter and search under warrant and certain coercive powers to compel attendants at examination or to produce documents. Others are contained in other legislation, for example, the Commissioner is an exception agency within the meaning of the Telecommunications (Interception and Access) Act of 1979, the TIA Act.

The Commissioner in his written response to your invitation to make a submission to your review attached a copy of the joint submission made by investigative commissions, which included the Commissioner, to the Parliamentary Joint Committee on Intelligence and Security, or PJCIS, review of the TOLA Act.

The joint submission identified the importance of access to the kind of powers contained in the TIA Act when investigating serious corruption offences and highlighted the need for investigative commissions to have access to encrypted communications. The Commissioner reiterates that need and seeks to emphasise that further by way of a practical example, which was not referred to in the Commissioner's written response.

In an investigation by the Commissioner into corruption in public administration involving the alleged movement of contraband into the South Australian prison system, the Commissioner became aware, through evidence obtained in the investigation that various persons of interest were using encrypted communications to plan and carry out their activities.

In the absence of the powers contemplated in the TOLA Act, the Commissioner's investigation was unable to access those encrypted communications. The consequence was the Commissioner's investigation

was likely prolonged by the inability to access the encrypted communications, and it is possible that additional contraband was introduced into the prison system over that prolonged period.

In the event, the investigation proceeded to a successful resolution from a law enforcement perspective and arrests were made. But it can be said that the investigation would have benefited from early access to the encrypted communications and that such access to encrypted communications may have assisted the investigation to reach an earlier conclusion.

The Commissioner's written response to your review noted that notwithstanding the exclusion of State and Territories' independent commissions against corruption from access to powers contained in Schedule 1 of the TOLA Act, the PJCIS has subsequently reported that the committee had made statements in the House of Representatives to signal its bipartisan agreement that the commissions against corruption should be reinstated in Schedule 1 of the TOLA Act.

The Commissioner was grateful to hear that in the course of your opening statement yesterday you indicated that you considered that ICACs have the same need as the police to have urgent access to TARs and TANs on the same terms and with the same safeguards as the police for as long as the police have access, and that you commend to the PJCIS the idea of immediately recommending such powers with a view to prompt legislation to that effect. The Commissioner acknowledges your remarks and thanks you for them.

It is well understood that corruption is oftentimes difficult to detect and then even more difficult to investigate. This is recognised in the ICAC Act by the nature and extent of the powers given to the Commissioner to investigate allegations of corruption in public administration, including coercive powers that assist the Commissioner to advance his investigations when they might otherwise stall.

With the recognised growth of the use of encrypted communications to aid the furtherance of serious criminal offending, including serious offending within the corruption space, it is important that law enforcement agencies, including the Commissioner, have access to sufficient powers to keep pace with that growth. Thank you.

DR RENWICK: Thank you very much, gentlemen, that's most helpful, and I should say that in addition to what I said yesterday, I intend to write to the PJCIS next week formally saying, this is what I said, and over to you. So it's then a matter I think for them to progress it, I've really done all I can at this stage.

Can I just start by – as you know my statement yesterday was just limited at this stage to TARs a TANs, TCNs are in a different category conceptually because you're talking about creating a new capability. There's also of course an obligation to ensure that the DCP isn't out of pocket. And it's possible I think to imagine that a TCN could actually cost quite a lot of money, which the agency would have to pay.

What did you want to say in addition to the importance of you having access to TCNs as well as TARs and TANs, as Schedule 1 powers? Did you want to say anything in addition?

MR JENSEN: To be frank, the Commissioner's primary concern was that we were included in the legislation and that we had access to the same things that like agencies would have. So the answer to your question is we would like to have access to the same things as other agencies, and to have that as an investigative tool available to us if required.

DR RENWICK: But you're not in a position, sitting there, to say that there's a particularly urgent need for a particular TCN for example?

MR JENSEN: No.

DR RENWICK: No, thank you. And I don't mean that critically of course at all. I asked some questions of the New South Wales ICAC and the LECC yesterday, and forgive me if I'm repeating some of them. So I mean, obviously enough, it's unsatisfactory when your obligations include investigating potentially corrupt police to not have the same powers the police force has, and so you can assume I don't need any more convincing on that front.

I discussed yesterday with the New South Wales representatives that – and I welcome your additional comments – that presumably you, like the New South Wales ICAC, say what you're after is what's on someone's mobile phone, I daresay that comes up from time to time. Now, you could go, as it were, through the front door I presume, summon that person to a hearing and say, "What's your password". I assume you have those powers now if you want them, that's an investigative option open to you?

MR JENSEN: Yes, the Commissioner has the ability to summons a person to a coercive hearing and to ask questions of them. I think that a very interesting question arises in that context about if you receive the password, what can you do with it, and that you would need to work through the legal implications of then accessing the phone with that password, what permission are you using in order to do that, but that's a different issue.

DR RENWICK: And I think also, I mean, obviously enough, there are many reasons why in an investigation you don't necessarily want to start with the ultimate target first and tip them off that you're actually investigating them. That's obvious enough I suppose as an investigative matter.

MR JENSEN: Yes, that's right. It depends very much on what the sequence of evidence is that you're following, and in most investigations at the end of the day what you're doing is following the evidence that's available to you, which might lead you to other evidence.

DR RENWICK: So with that in mind, I can well understand that you want to access things covertly, and that the TARs and the TANs and indeed the TCNs would allow you to do that without showing your hand prematurely or perhaps at all to the relevant subjects of interest.

MR JENSEN: Yes, that's right. And I think it's worth making the point that in the corruption space, when you're investigating a corruption offence, it's often what's happening in real time that's very important as well. Corruption investigations, unlike some police investigations, don't look at the historical fact, they're looking at real time activity and trying to understand an ongoing arrangement. And if you have access to encrypted communications in real time, that that can very much aid your investigation.

Contrast that to having access to those communications after the fact, that might help from an evidential point of view, but it would be much better sometimes to have it while the investigation is on foot to allow you to follow other leads.

DR RENWICK: Indeed. All right, then turning to oversight and accountability, and forgive me if you did mention this in your opening. I assume there is, apart from the oversight of the Courts, is there an Inspector-General or the like for the South Australian ICAC?

MR JENSEN: Yes, the ICAC Act itself specifies that there is a reviewer, and the reviewer has wide powers under Schedule 4 of the ICAC Act to oversee the activities of the Independent Commissioner Against Corruption. In addition to that there is set out in the legislation a strict oversight regime including parliamentary committee, who in South Australia is called the Crime and Public Integrity Police Committee, who have an active role in overseeing not the actual investigations for the Commissioner but the nature of the work undertaken by the Commission.

DR RENWICK: Of course the Commonwealth Ombudsman has oversight in relation to your access under the TI Act.

MR JENSEN: Yes, so I think it would be fair to say that there are multiple levels of oversight, not only in relation to the activities under the ICAC Act, but the activities of the Commissioner generally if he's acting in the space of for example a telecommunications intercept.

DR RENWICK: So then returning to TOLA, one of the points, which I thought was well made by New South Wales yesterday, is they feared that they might be doing a joint investigation across boundaries, say if there's a Federal ICAC they might be doing a State/Federal investigation into corruption, and if they didn't have Schedule 1 powers they might be shut out of collaboration and shut out of joint meetings, and that's a reason why they should have those powers. And I assume you would agree with that?

MR BAKER: Absolutely we agree with that, and we agree with the comments that the New South Wales ICAC made and the LECC yesterday, yes, it would be issue. I think one of the others things that they were trying to mention was that in order to identify what the capabilities are of the DCPs, we need to be included in those conversations so that we know whether to approach them to serve the TAR.

DR RENWICK: So equally I should indicate that I am inclined to recommend that the ombudsman for example should be able to freely communicate with your reviewer in relation to your use of the TOLA powers. And I assume you have no in principle objection to that, they each have their proper oversight functions.

MR JENSEN: Yes. And in fact the reviewer is interested obviously in that space and does do reviews of what the Commissioner has undertaken. Looking specifically at Schedule 4, it would appear that as currently structured there would be scope for the reviewer to have the ability to do that under the powers currently given.

DR RENWICK: All right. Well, just I'm happy to indicate publicly I am inclined to recommend that there be power for, say, the ombudsman or perhaps likely the IGIS to be able to speak to ICAC, Inspectors-General or reviewers, however they're described around the country.

Another safeguard I suppose is having a prescribed form for the notice. You may have heard that I've indicated yesterday that – and this is really based on my review of some of the documentation issued by agencies so far under TOLA, that there should be a prescribed form which says things like this is what this notice is based on, this is the lawful authority for this notice, if

you need an additional warrant or so on, as you may often do so, that would be indicated, and it would indicate things like the definition of systemic weakness, it would indicate that you have a right to complain to the ombudsman in the relevant State, you have a right – you may have rights in Courts.

In other words, the standard form, so that that recipient of a TAR or a TAN or a TCN actually knows what their rights are, and I assume again that would not be something you would object to?

MR JENSEN: No, I think there'd be great advantage in consistency in a space like this, based on the comments that you've received already.

DR RENWICK: You've given a real example, so thank you, in relation to the South Australian prisons, and that's – it's good to have real examples in this. I suppose just finally from my point of view, and I'm not asking you to reveal particular DCPs, but I assume you have good relations with particular DCPs and you'll use a TAR, you'll use the request as a first preference I imagine rather than moving to compulsion. That would be your sort of preference in broad terms I assume.

MR BAKER: Yes, absolutely. We practice that in all of our powers that we have available to us, we will always try and obtain the consent, obtain things voluntarily first, and if that doesn't succeed and we think there's a necessity to go down the further line, then we'll obviously go down that path.

DR RENWICK: I suppose the final thing is you will have read I've raised the issue about whether there should be AAT-type oversight, because I am concerned that it's not the full story to say that it's the underlying warrant or authorisation say the TI Act which is the solely intrusive thing. After all, the reason agencies want access under TOLA is because you might get data or content which is unintelligible and you want to make it usable.

So my information at the minute is to say, well, there should be some sort of independent oversight similar to the granting of the warrant for the content. I appreciate metadata is something which usually agency heads can authorise, really because these things (a) are very technical, actually people don't quite understand necessarily what is being compelled, and (b) just in terms of public expectation.

What I'm really trying to say is it is an incomplete picture to say, well, the warrant for the content is the thing, it's the warrant for the content plus when something is encrypted, whatever it is, which decrypts it or makes it intelligible. And what I'm inclined to recommend is that you have a

uniform level of authorisation for the Schedule 1 powers, as you do for example for the TI warrants. Is that something you wish to comment about at all?

MR BAKER: We would offer a slightly alternative version, a view.

DR RENWICK: Yes.

MR BAKER: Our opinion is that when we obtain a warrant under the TI Act, we go through that process of going before a judge or an AAT member, those issues of privacy are obviously a key consideration within that, also our expectation would be that the issuing judge or AAT member would take into consideration that they're issuing a warrant, that we can obtain all the information available, and that the TOLA Act is really a means of how we access some of that information that's already authorised under the warrant.

So I guess what we would err on the side of caution in saying as to having another process of going through that same rigorous process that agencies have already done through by going to obtain a warrant in the first place and how that might impact on availability of AAT members and the Courts.

DR RENWICK: So are you saying that if it all could be done once, for both TOLA and warrant, that's what you're looking for?

MR BAKER: Yes. I would suggest that when an AAT member or a judge is issuing the original warrant, that there could be some provisions in the application for that warrant that would include the fact that the warrant may enable the obtaining of encrypted data and communications. They can then consider that in their privacy.

DR RENWICK: Thank you. Could I just ask one follow up question then. I mean, I've obviously spoken to some of the people who issue the warrants, and they're no doubt very experienced lawyers and some are judges or retired judges, but I am candidly concerned that technology in this area is so rapidly changing that it doesn't matter how distinguished the judge or Tribunal member might be, unless they have access to some independent technical advice, they may not fully understand the position.

Now, of course they can say to you, look I don't understand paragraph 10 of your request, please go away and give me an expansion about what that means. But I'd be very interested – I mean, without revealing any particular matters, do you think that the complexity of technology is sometimes a challenge for the eligible judges or Tribunal members to really comprehend what's involved? Or can't you say?

MR BAKER: On experience, I probably couldn't really say. I would suggest that they probably wouldn't take in too much consideration the technology side of it, just understanding that the type of information that can be obtained through that warrant and authorisation.

MR JENSEN: An additional aspect of that, is this, that if an applicant is making an application, it's up to the applicant to put before the deciding authority or the decision maker sufficient information to allow them to make the decision that's sought. What Mr Baker referred to earlier on in the evidence was the advantage of being connected with other agencies who are operating in this space, such that the information about the technical side of things is commonly shared at that level, and it's not uncommon for agencies to talk about common experiences and common problems and common challenges.

Consequently it may well be that the sort of information you're contemplating could be included in the initial application, simply because the agency is aware that that is a technical space that requires additional information and that that technical information is put before the decision maker at the application stage, in the form of the affidavit or whatever.

Areas like Mr Hewlett-Parker's area, who have intimate knowledge of technical capabilities that, to be quite frank, some of us might not completely understand, but which can be explained to a member or a judge and who can then take account of that for the purpose of deciding whether or not to grant the application. We would certainly never want a situation where a decision maker was granting an application based on potential information, it should be information that's at hand and understood.

DR RENWICK: So I think you've been – do you want to add to that, Mr Hewlett-Parker? I mean, can I give you this example, at the minute under a TI application for content, a judge has to consider the impact on privacy. If you in your application say, look, we anticipate this will all be encrypted. Then the impact on privacy is small. If on the other hand you say, look, there's also a Schedule 1 TAR in place which means we anticipate we're going to be able to read all of it, then the impact on privacy is much larger.

Explaining why that is so, for example, looking at some of the provisions of Schedule 1 which require the decision maker to consider the availability of other means to achieve the objectives, or whether the request when compared to other forms of industry assistance are the least intrusive form, so far as the non-subjects are concerned. If you see what I mean.

I know that's a rather long question, but what I'm getting at is that it seems to me quite quickly, if the eligible judge is considering both the TI warrant and the impact because of Schedule 1, it could get very technical when the judge is being asked to consider is there a less intrusive way of doing it, when you're considering the people who aren't the subjects of interest.

Is that reasonably clear? I'm sorry, it's a very long question.

MR HEWLETT-PARKER: Yes, sorry, I probably got lost a bit in the question, but I think the information that we'd possibly put before the judge or AAT member would really I suppose highlight to them that we're after the content of communication, be it messaging, standard phone communications, and some of that content is likely to be encrypted, and we're simply seeking access to that encrypted part of that content.

The whole idea of the application is to seek content of communication. The fact now in this day and age a lot of that communication is encrypted, through peer-to-peer networks. I don't think it takes away the fact that the privacy is impacted any more, it's simply asking them to open the book. We've got a library shelf full of books, some we can open, some we can't, I think the warrant – the idea of the warrant is that the assumption given, you can read every book that's there, and we're simply asking for the ability to read those books.

DR RENWICK: Thank you. But if the question under Schedule 1 of TOLA is for example, as the statute says, the availability of other means to achieve what you want to achieve, that may require some deeper understanding about the technological alternatives, mightn't it?

MR HEWLETT-PACKER: Yes, I think it would.

DR RENWICK: I mean, the real point I'm trying to make is I can imagine fairly rapidly even a very experience judge might need a bit more assistance in understanding the technical ramifications of what they're being asked to approve.

MR HEWLETT-PACKER: Yes, certainly.

DR RENWICK: All right. Well, gentlemen, thank you so much, as I say, I will be writing to Mr Hastie next week and I would aim to be giving my report to the PJCIS in June. If there's anything further arising out of this morning you want to put in, could we have it soon? And thank you all.

MR JENSEN: Thank you.

DR RENWICK: And we have morning tea and we will be back at 11.

ADJOURNED [1025]

RESUMED [1050]

#SESSION 6: BSA The Software Alliance

DR RENWICK: So we now return, we have one and only person dialling in. We have Mr Jared Ragland, who is speaking on behalf of BSA, the software alliance. Mr Ragland, can you hear me?

MR RAGLAND: Yes I can.

DR RENWICK: Do you have an opening statement?

MR RAGLAND: I do, if you don't mind.

DR RENWICK: Yes, please go ahead.

MR RAGLAND: All right, well first of all, good morning and thank you so much Dr Renwick and to your staff for inviting me to speak on behalf of BSA, The Software Alliance, on this very important topic. I also want to thank you for allowing me to participate via telephone conference, as I'm based in Singapore it would've been very difficult to have made it there in person, and I'm sorry for that.

So I'm the senior director for policy for Asia-Pacific for BSA, and my responsibility is to cover technology policy-related issues throughout the region. BSA itself is an industry association headquartered in Washington DC with offices in Latin America, Europe and through Asia. And our member companies, which include companies like Adobe, Amazon Web Services, (indistinct), CISCO, IBM, Microsoft, Sales Force, Splunk and Twillio just to name a few, are at the forefront of data-driven innovations, including cutting-edge advancements in artificial intelligence, machine learning, (indistinct)-based analytics and the internet of things.

And these innovations are helping to make our devices smarter, our businesses more competitive, and the delivery of government services more efficient.

So BSA has been engaged in discussions with the policy makers and legislators there in Australia on the *Assistance and Access Act* since its introduction as a Bill in 2018. As you may know, we've filed several submissions to the government of Australia, which we included in our 13 September 2019 submission to you, the INSLM. And we testified before the Parliamentary Joint Committee on Intelligence and Security on 19 October 2018.

First, I want to emphasise that BSA and our members fully support the Australian government's desire to have more powerful tools to aid in the fight against criminal and terrorist activities. Some of our members are the recipients of regular lawful requests for information from law enforcement agencies around the world, and they are committed to complying and cooperating with lawful requests to the extent that they can do so from a technical and legal perspective, and in a manner that does not violate the obligations that they have to their customers.

The benefits of the innovations our members are driving depend on consumers trusting the technology, whether they are individual citizens or large enterprises running global businesses. Therefore, BSA is committed to working with governments across the globe to ensure that law enforcement capabilities can be enhanced in ways that do not necessarily undermine consumer trust, consumer privacy or the security of our technologies.

And because the *Assistance and Access Act* will set a precedent looked to by governments throughout the Asia-Pacific region and beyond, it is especially critical that the legislation meets that goal.

So in my remaining time, I would like to touch on a few of our specific recommendations for improving the *Assistance and Access Act*, highlighting key points that you can find in our several submissions to the PJCIS, INSLM and other entities.

First, the decision to issue or vary a technical assistance notice, or a TCN, should be made or approved by an independent judicial authority. Strengthening judicial oversight of this authority would help align the act with foundational values of the Australian justice system, and it would go a long way toward assuaging broader concerns about the scope of the authorities in the Act.

Second, we recommend that the Act should explicitly incorporate a procedure to allow an affected designated communications provider or DCP to challenge a decision to issue or vary a TAN or a TCN on its merit.

The other issue I wanted to flag was the importance of amending the definition of 'systemic weakness' and 'systemic vulnerability' in the Act. We know that the Act clarifies that TANs and TCNs and TARs have no effect if they require a DCP to implement or prevent the DCP from correcting any systemic weakness or vulnerability in a forum of electronic protection. This is a very, very helpful clarification, but the definitions of systemic weakness and vulnerability remain too limited and unclear in our opinion. And our submission to the PJCIS on 12 February 2019, which we also reproduced in our 19 September submission to the INSLM, we proposed a revision to section 317(v)(g), that we think would improve the situation.

As an alternative, we can support the proposed amendments, the definition and the repair Bill that was introduced at the end of this last year. So I think I've run out of time. There are a number of matters that we raised in our written submission that I sincerely hope will be carefully considered both by the INSLM as well as the PJCIS and ultimately the Australian Parliament. But in the interests of time, I'll skip over that list of items and conclude my opening statement for reiterating my appreciation and thanks for inviting to participate in this hearing, and I look forward to any questions you might have.

DR RENWICK: Yes, thank you very much. Can I ask you then first, if you look at your submission - I'll just get the date - well, can I ask you first about the independent judicial approval proposal?

MR RAGLAND: Yes.

DR RENWICK: Are you familiar with the role of the IPCO in the UK?

MR RAGLAND: I'm vaguely familiar, and I did read your opening statement regarding that body in the UK, but I can't pretend that I'm very familiar with the institution.

DR RENWICK: All right, but do I take it then if you've read my opening that you would broadly support the idea of independent lawyers assisted by technical experts making key decisions in relation to Schedule 1 powers?

MR RAGLAND: Yes, I think as a general matter. I mean, obviously it would depend - as everything does - on the details and how that kind of an entity would operate within the Australian legal system, but you know, without attributing any you know, ill intent or otherwise to enforcement agencies, we are concerned that there is either a real risk or at least a perception of a risk that if the decisions on issuing and varying these notices, especially the TANs and TCNs, is primarily under the control of

the executive branch, that that doesn't provide sufficient oversight.

So I'd have to look into exactly how the IPCO works in the UK, but I think the idea of thinking about a way of applying an independent judicial or quasi-judicial process to the decisions would certainly be helpful.

DR RENWICK: Well to come at it in a different way, IPCO has been regarded as satisfactory by the United States for the purpose of the agreement it's concluded with the United Kingdom about the *Cloud Act*, and you've mentioned the *Cloud Act* of course.

So to the extent that Australia had something which met that standard, you would commend that, I take it?

MR RAGLAND: Yes, I mean I think - again, I think we still frankly have some questions and concerns about the ultimate implementation of the UK *IP Act* going forward, but I think that the implementation of oversight mechanisms like that would move in a direction that would help allay some of our concerns about the *Assistance and Access Act* in Australia.

DR RENWICK: All right. Can I then ask you to look at your submission to the PJCIS of 31 October 2018? Do you have that, page 6, in front of you?

MR RAGLAND: Let me just flip over to it. You said the 12 October submission?

DR RENWICK: 13 October submission, page 6.

MR RAGLAND: Okay, yes.

DR RENWICK: 31 October I apologise, 31 October 2018, page 6.

MR RAGLAND: Thirty-one, okay, at page 6. So 31 October submission I have only up to page 3, I'm sorry. Is there an addendum or are you looking at the - - -

DR RENWICK: I'm sorry, I beg your pardon. It's the 12 February 2019 PJCIS submission, page 6, I do apologise.

MR RAGLAND: Right, right, no worries, so I am there yes. This is where we propose a definition or a revision to section 317(v)(g).

DR RENWICK: That's right. Now, this is not exactly what the current Bill before Parliament talks about, but can I just direct your attention to your

proposed additions on page 6 under subsection (vi) of 317(z)(g), where you talk about a systemic weakness in a system that extends or carries the risk of being extended. The language in the Bill before Parliament talks about something which may or would create a material risk of certain things. I suppose my question to you is about the predictive concept.

In other words, it's been suggested to me that if you have a prediction that something - if you have to predict that something may create this systemic weakness, it is in truth impossible to ever overcome that standard, because you know, you can't really predict technologically what may come up in the future. So the preferable wording would be 'would create a material risk', rather than may. Do you have any comment on that?

MR RAGLAND: Well I mean I think - especially to the extent the specific questions would be reviewed by technical experts, I guess the question would be, perhaps, is there a reasonable expectation that the acts or things might introduce a systemic weakness going forward, because I think just limiting it to - it does now today - doesn't take into account the fairly rapidly-evolving technology and deployment framework that you know, internet-enabled services are operating on. And I think if you want to make sure you're not inadvertently introducing a vulnerability that could have potentially more negative effects than the problem you're trying to solve, you want to make sure that you're erring on the side of caution.

So I think that's why we were working on making sure that there is a sort of - you can capture the potential introduction of risks as well as the practical existing in the - - -

DR RENWICK: Okay, one last question from me and then I'll ask my colleagues if they have anything. On your letter to me on 13 September 2019, on page 2 you say that your recommendations cover at number 8:

> *Decriminalising unauthorised disclosures of information by employees of DCPs.*

Now, just to understand what that means, if you're there talking about the contact person in the DCP being permitted to talk to their internal lawyers or technical experts, I'm entirely with you and to the extent that the statute isn't clear - and I think it's reasonably clear, that should be tidied up.

But if it goes beyond that, why should employees be able to make unauthorised disclosures when the company they work for cannot?

MR RAGLAND: Right, well the example - and I think there have been some, I think, explanations that go to this point. Although they weren't to our knowledge clarified in the legislative text. But we were concerned about the former situation that you described, where an employee may be directed to a TAN or a TCN to implement some change in the system, and they need to or feel they need to discuss that either with colleagues or others who would be important in making that decision and implementing that request.

And it seems like without more, that could put them at potential and somewhat risk of criminal violation. We wanted to make sure that we were avoiding that circumstance.

DR RENWICK: Well Mr Ragland, I can put your mind at rest there as far as I'm concerned. When the Department of Home Affairs comes up in a minute, I will specifically be asking them about that situation, namely whether an employee is able to speak to other people within their organisation who are similar bound by confidentiality, and I would expect that if the law doesn't make that clear, they would agree that it would, or no doubt they'll tell me why not.

So just let me ask - yes, so Mr Mooney, my principal advisor, has a question.

MR MOONEY: Yes, just in relation to your submission to the PJCIS of 12 October, you talk about the acts or things that can be required from a DCP to assist with a Schedule 1 notice. And you say there that these acts or things should be narrowed and reduced to an exhaustive list. Have you thought about what that exhaustive list would be, and would there be any concerns that this would sort of unduly limit the flexibility of the notices in terms of dealing with particular technical problems?

MR RAGLAND: I guess the short answer to your question is I don't have any sort of vetted, approved, explicit articulation of what that exhaustive list would look like. But as a general matter, you know, our companies thrive on having a certain amount of legal and regulatory certainty as to what they are or potentially are expected to do, and so having it as a non-exhaustive list with a sort of 'and other items that may come up', it leaves a large amount of anxiety in terms of what may be ultimately asked.

I can appreciate that an exhaustive list is by definition narrower and more restrictive, but I guess from our point of view, if it's developed properly, you could articulate reasonably well the things - acts and things that seem reasonable, at least at this time, and minimise that uncertainty that could be imposed on the industry.

MR MOONEY: I see, well if you possibly could, we'd certainly very much appreciate, you know, just a further short submission on putting together something that would amount to an exhaustive list.

MR RAGLAND: I mean, let me - I'll have to obviously consult with our member companies on that, and I understand that you're on a fairly tight timeframe on this process, could I ask what the - how quickly would you be looking for that kind of info from us?

MR MOONEY: Well that's true, we are under a very tight deadline, so the answer really is as soon as possible so that we can, you know, take it into account when we're looking at formulating Dr Renwick's recommendations. So you know, just as soon as you possibly could would be appreciated.

MR RAGLAND: Thanks, well I'll take it on board and do what I can, try to get back to you just as soon as possible.

MR MOONEY: Thank you.

DR RENWICK: Mr Ragland, thank you very much for your time, I haven't worked out what time it is in Singapore, but I suspect it's an inconvenient time, so thank you very much and we will let you go now, thank you.

MR RAGLAND: All right, well thank you very much. Thank you, bye.

DR RENWICK: We now invite representatives of the Australian Federal Police, particularly Deputy Commissioners Kent and McCartney to come forward, and anyone else who of course is part of the team. Gentlemen, welcome, and did you have an opening statement?

#SESSION 6: Australian Federal Police

MR KENT: Yes, if you don't mind.

DR RENWICK: Yes, please go ahead.

MR KENT: Certainly Dr Renwick, the AFP values the INSLM's independent oversight of key national security laws and the recommendations that have arisen from your reviews, and we very much thank you for the opportunity to participate in these hearings on the *TOLA Act*. If there are questions that we're unable to answer today, of course we can follow up with a written response in a short timeframe.

In terms of context, the AFP sought these powers to address significant challenges posed by an increasingly complex digital environment, and we expected that by late 2020, nearly all of our communications content relevant or of value to our criminal investigations, would be encrypted. This left the Australian community exposed in terms of public safety, and Australian interests at risk because of a range of threats that I think were well-articulated in your paper.

But specifically, from terrorism, child exploitation, cybercrime and transnational serious and organised crime that remain prevalent and continue to grow in their nature. *TOLA* has served to modernise the assistance and access provisions to enhance targeted access and helps address the divide between criminals' use of technology and law enforcement's ability to lawfully access targeted information and communications.

TOLA has enabled law enforcement agencies to adapt to the use of encryption without undermining it. And as such, we believe these powers are very important and useful, and are proportionate to the current threat environment. *TOLA* has continued to provide significant operational benefit for AFP investigations into serious criminal offending, the use and disclosure provisions within the legislation prevent us from discussing in granular detail at a public hearing, particularly where investigations are not yet before the court, or indeed involve computer access warrants.

However, we can say that since *TOLA* commenced in December 2018 that the AFP has issued five technical assistance requests under Schedule 1 of the industry assistance scheme between December 2018 and 30 June 2019. These technical assistance requests assisted our investigators into cybercrime, drug importation, and the threat of transnational organised crime.

During the same period, there have been no technical assistance notices or technical capability notices issued. During that period of time, there have been no State of Territory law enforcement agencies that have sought the AFP Commissioner's approval to issue their own technical assistance notices.

As of 30 June 2019, the AFP has also obtained seven computer access warrants under Schedule 2. These warrants enabled access to electronic evidence which was unavailable by any other means, and enabled us to progress investigation, again into serious crimes involving terrorism, child exploitation and cybercrime.

We have obviously continued to use these powers in these schedules into

the current financial year, and we also used the enhanced search warrants provisions under Schedule 3 very regularly across a wide variety of serious crime investigations.

The AFP currently does not report on the number of times we use search warrant-related powers, however we can say that the new framework enables more accurate targeting of suspects, and better identification, access and collection of otherwise secure and encrypted communications and records as evidence of offending.

In terms of benefits of *TOLA* to the AFP, we also remain committed to engaging with communication providers in a consultative manner, as industry's advice, expertise and knowledge is invaluable to our work. In our experience, the industry assistance scheme has accelerated cooperation from industry.

We have found providers are increasingly willing to assist due to the legal certainties and assurances regarding the commercial scope and impact of requests, and protections provided under the *TOLA*. The fact that the AFP has not issued any technical assistance notices or TCNs to date does not indicate these provisions are not required, but rather it demonstrates the effectiveness of TOLA's tiered approach in our view as we have not yet needed to escalate to the higher levels of compulsory assistance.

I am also aware that there are some concerns of our Commissioner's comments during a National Press Club address on 19 February 2020 in relation to challenges regarding encryption and the potential that industry may not be cooperating. The Commissioner's point did not say that industry as a whole was not currently collaborating or working with police, rather that some companies were addressing this issue better than others in regards to the overall challenge of criminals utilising their platforms.

The Commissioner was raising this point in an area specifically relating to protecting children from sexual exploitation and abuse and, particularly, as it related to the dark web. I don't believe his comments related to the TOLA scheme as it currently applied.

This concludes our opening remarks and the AFP certainly welcomes the opportunity to respond to your questions.

DR RENWICK: Yes, certainly. Just for the transcript, could I just get you all to identify yourselves?

MR KENT: Deputy Commissioner Karl Kent for Specialist and Support Operations.

MR McCARTNEY: Deputy Commissioner Ian McCartney, Deputy Commissioner of Investigations.

MR PENNY: I'm Simon Penny. I'm the Acting Commander of Covert and Technical Operations of the AFP.

DR RENWICK: Thanks, gentlemen. Just a couple of general questions to start with. At the minute, as you've said Deputy Commissioner Kent, you don't provide numbers for the total number of search warrants you issue under the Crimes Act each year. If I were to make a recommendation that a total number be published each year, would that present you with particular problems?

MR KENT: No, we don't believe there would be any concern from the organisation in providing numbers as it relates to the execution of search warrants.

DR RENWICK: Yes, executed, I quite agree, not sought. Next question, and I didn't invent the numbering of this Act, but 317LA is the provision which says:

> *Where a State or Territory police force, for example, seeks to give a TAN to a DCP, the AFP Commissioner must approve the giving of the TAN.*

Now, the comment which has been made is that in our system we don't have the – the State and Territory and AFP forces are co-equal. It's not as if in any other area I'm aware of, I mean each police force has its own crimes it investigates. For things like terrorism, as Deputy Commissioner McCartney well understands, you might have a joint counterterrorism task force, but this is the first instance that I'm aware of when a State police force which, for example, doesn't need to go through the AFP Commissioner for a TI request, has to go through your Commissioner for this. To be frank, I'm a little bit at the loss as to why that provision is there.

Now maybe that's a question for Home Affairs, but if you could cast any light on it, I'd be grateful.

MR McCARTNEY: I think in terms of the relationship between the Federal Police and the State Police, I think you've described it very well in terms of that co-equal arrangement. We work on a daily basis. In our submission, the legislation actually states "approve", the AFP Commissioner must

approve, but the EM states "coordinate". I think we seek some clarity on that particular aspect.

Our preference is "coordinate", as you've noted. We don't see it as our role to second guess the operational independence of State and Territory law enforcement. It runs the potential of, in effect, creating more work for us to review the work of a State police or a Territory police and it might delay the process if one of these matters was urgent. So, our strong preference is that the focus is on "coordinate", not "approve".

DR RENWICK: The reason why you might want coordination is they may not realise, for example, that you already have a TAN which allows you to do what they want to do.

MR McCARTNEY: Again, Dr Renwick, you've described it really well. It's more de-confliction in ensuring that visibility right across Australia in relation to this issue.

DR RENWICK: Thank you, that's very helpful.

The next question I think is there has been quite a few submissions expressing concern about the capacity of AFP officers to add, copy, delete or alter data on a device during the execution of a search warrant. Can you provide some explanation and reassurance about that, please?

MR KENT: Yes, Dr Renwick, I think I can respond to that particular challenge. Certainly, we appreciate that there has been recent public commentary on the wording of section 3F which enables AFP officers to add, copy, delete or alter data in the context of accessing a computer or device that is located when executing a search warrant.

However, the provision recognises that accessing modern electronic devices to secure evidence unavoidably results in technical alterations to data by virtue of taking that out. This is not dissimilar to when we investigate any crime scene or attend any search warrant.

Police, by their very actions, or crime scene investigators, by entering a crime scene will alter it in the sense of they will leave trace components of themselves there. They will disturb the scene. Whilst they act to minimise that, those actions will occur in accordance with Locard's exchange principle, I think, which is fairly well understood in crime scene investigations.

In the physical world, when we walk into a crime scene there is a disturbance and change. Similarly, in the digital world, when we engage

with devices of this nature that can result in changes to that data. It is important that we declare that, that it is understood, and it can be examined.

Some key examples of how that might occur. So, in relation to adding data, this would include additions to computer logs that automatically occur whenever a computer is being utilised. This would include new entries being automatically added when the computer is logged on to or when a search for relevant data is conducted on that device.

Copying data would include replicating relevant data from the internal storage of a computer to a removable storage device, such as a USB, to enable it to be seized and taken from the warrant premise as evidence. Again, that alters the device.

Finally, deleting data would also include having to overwrite memory when installing forensic software to search the computer for relevant data or uninstalling the forensic software at the end of the warrant.

Also, altering data would include any of those matters I have just referred to, as well as changing the password on the computer account to enable access to the contents to search for relevant data or changes to the last access date on a file when it's viewed as part of a search. All of those aspects relate to that particular issue.

Law enforcement officers can only seek a search warrant where they have reasonable grounds to suspect a relevant offence has or will have been committed and the investigation is or will be underway, and access to the data is necessary to secure evidence or information.

Further, the warrant issued by an independent issuing authority must specify those things authorised under the warrant, including whether adding, copying, deleting or altering data is necessary to access the relevant data to determine its relevance.

Aside from those legislative limitations, should an AFP officer go beyond the scope of the warrant, this may result in validity or admissibility issues of the evidence being questioned as it is not being legally obtained. It also may result in an internal investigation into the AFP officer's conduct under our professional standards framework.

The AFP notes that these provisions do not permit alternatives for any other purpose, such as the preventing of the ongoing continuation of an office; for example, preventing distribution of child exploitation material or illicit online trading.

DR RENWICK: If I understand that correctly just to take an example, if you were to seize a mobile phone, and I will come in a minute to the powers you may have to require a password to be handed over, it would not be uncommon I imaging there or then, or soon thereafter, to take a copy of the relevant parts of the phone as it exists. Yes?

MR KENT: Yes.

DR RENWICK: I think what you've explained is the sole purpose for adding, altering and so on is to get that copy.

MR KENT: Yes.

DR RENWICK: If you went beyond that, that would breach the terms of the warrant in all likelihood?

MR KENT: Yes, that's correct.

DR RENWICK: That is something which could be tested I suppose in a court case if you sought to use the extract. The Crown could be required to produce the officer who made the copy, who would have to justify any alterations and so on.

MR KENT: That is correct and this has been also consistent with the physical world where an officer seizes any exhibit from a crime scene. If they take actions to alter that item beyond the normal process of seizing it and putting it in a bag and zipping it up, they would be accountable for that.

DR RENWICK: All right. While we're talking about warrants then, under the Crimes Act under 3LA, I think, you can seek permission to require someone to hand their password over, and that's understandable. Is that something that you almost routinely now ask for because, after all, you don't want to have to go back if someone is uncooperative and get further permission?

MR McCARTNEY: If we can gain access to the phone ourselves, obviously that's the best course of action. But if we can't, then we look at the option of the 3LA order to ask for that password, Dr Renwick.

DR RENWICK: I suppose what I'm getting at is that because an investigation may move rapidly and because you may not have the time to go back and ask, is it your general preference to get that permission at the same time as you get the section 3 warrant?

MR McCARTNEY: Correct.

DR RENWICK: So that you have the facility if someone is intransigent, as I dare say they are from time to time.

MR McCARTNEY: That's correct.

DR RENWICK: All right. Just as a practical matter, have you found – I think there are increased penalties for failing to hand over passwords and the like. I mean have you found increased cooperation since TOLA came in?

MR McCARTNEY: We have. There has been a number of cases, including in the counterterrorism field, Dr Renwick, which has been, from our perspective, extremely positive.

DR RENWICK: I suppose, and I appreciate you're not the Border Force, but I imagine if I asked them, they would have a similar experience because their penalties I think at the border to ask for passwords also, if you fail to give it, the penalties have increased for them as well I think.

MR McCARTNEY: I believe so. It makes sense, Dr Renwick.

DR RENWICK: Deputy Commissioner Kent, you said that one of the reasons there had been no TANs and TCNs to date is that the TARs had been effective and there was no need to escalate the powers. Now, I entirely understand what you're saying there in relation to TANs because the TARs and the TANs cover the same territory. One is voluntary and one is compulsory.

The TCNs go further than that, of course, because they ask or require a DCP to produce a new capability to do a listed act or thing which they don't already have. I suppose going to one of the questions I'm required to answer, is the necessity of the TOLA amendments. If, for example, in three years' time no one had asked for a TCN, would you say that indicated that perhaps the TCN powers weren't needed at all. I mean what I am to conclude, in other words, from the fact that so far it would appear there haven't been any TCNs?

MR KENT: I think at this stage it indicates that industry would prefer to cooperate voluntarily against a known scheme than be compelled by something over which they have less control. Having an escalation framework changes the nature of the discussion that law enforcement can have with industry in and of itself and also provides some protections for industry where changes to their capabilities may be required into the future.

We think that the tiered approach as it exists now is assisting those conversations, I think both from a law enforcement perspective in better clarifying the requirement, the specific requirement that we are seeking in accordance with the warrant that exists for access to that information, and better assists industry in defining how they could respond to that, simply by those tiers being in existence. I think it reflects the nature of the existing relationship between policing and providers of these telecommunications.

DR RENWICK: Just while we're talking about TARs, for example, and TANs, you may have read that I intend recommending there be a standard prescribed form so that the recipient, the DCP who receives any schedule 1 notice, regardless of who issues it, has certain standard information about their rights and obligations and I assume you'd only support that. I mean that assists you, doesn't it?

I mean I'm not trying to be tricky about it, just a standard document which says, "These are your rights and obligations. These are your abilities to complain to the Ombudsman, the IGIS and so on". That makes perfect sense, doesn't it?

MR KENT: We are supportive of prescribed details of what's required in a form that would meet the core requirements. Clearly, the current flexibility that exists to better articulate the nature of the capability sought or the access sought is valuable. So, a prescribed form, so long as I guess it doesn't restrict the nature of the conversation that needs to be had with the telecommunication provider, would be strongly supported by the AFP.

DR RENWICK: Well, I think as a practical matter what I'll do is I will circulate suggestions as to what might go in the prescribed form and please tell me if it's right or wrong.

MR KENT: Excellent.

DR RENWICK: While I am talking about pre-existing powers, as you also know, you've had powers for I think 20 years under section 313 of the Telecommunications Act in relation to telecommunications industry providers. I appreciate that is not as broad as the DCPs but, again, could you say anything about what has TOLA meant for your continued use of 313 Telecommunications Act powers?

MR KENT: Dr Renwick, it is our view that section 313 continues to have some utility as the AFP can and still does use this legislation in specific circumstances, particularly as it relates to prevention activities, crime prevention activities.

We also note that section 313 is broader in scope than TOLA. For example, it enables us to support requests that relate to assisting international courts and tribunals and in assisting in the enforcement of pecuniary penalties.

As an example of where AFP continues to use 313 requests, we have issued a number of requests under section 313 for service providers to block IP addresses and/or websites, particularly those containing severe child exploitation material. In 2019, for example, we called on 25 Australian telecommunications companies for their voluntary members of the access limitation scheme which seeks to block websites on Interpol's "worst of" list.

The AFP in that process provides the list of domains to Australian ISPs and relies on them to block the identified websites in Australia. The number of domains included on the list fluctuates as they are detected and defeated and taken down. We see that as a key crime prevention, if you like, activity that is enabled through this legislation.

DR RENWICK: Just expanding on that, on the counterterrorism field it sounds to me like that could have some potential to equally apply to problematic websites which proselytise or encourage terrorist activity or recruitment.

MR McCARTNEY: Absolutely, Dr Renwick.

DR RENWICK: I think I know what you will say in answer to this but I think I should ask it anyway. Mr Burgess yesterday, the head of ASIO, said that firstly encryption is of benefit to society and he is not seeking to use TOLA to create back doors. I take it you would agree with both those sentiments.

MR KENT: Yes, absolutely. We're not seeking to create systemic weaknesses via back doors. In fact, I believe the legislation specifically stops us from doing such act.

DR RENWICK: My final sort of topic is the proposal that you have seen, and it may not be my final proposal, in relation to approvals of schedule 1 powers and it may be that you say that's just a matter for Home Affairs which administers the Act, rather than you. Firstly, is that right? Is any proposal that, for example, an AAT member, as already occurs with TI content requests, might grant schedule 1 powers? Is that something I should be asking Home Affairs rather than you, or do you have a view on it as well?

MR KENT: Our sense on this particular matter is that it seems that the current arrangements are working well. Therefore, we are supporting the current arrangements in that we obtain a warrant for the access to the content and that the nature of these requests, as they currently stand in the way in which they are authorised, is providing us then with the access to the material that is the subject of an existing warrant issued by a judge.

I guess our concern in any arrangement where another judicial process is introduced could leave us in a circumstance where one process is almost at odds or as arguing with the other potentially.

We know that that's not the case in the British environment, in the UK environment in particular that you refer to, so we're obviously interested in exploring those matters. Currently, under the current process from a policing perspective, we see the process is working in accordance with the law and is proportionate and balanced.

DR RENWICK: You may have heard me express this yesterday but I am familiar obviously with the argument that everything works perfectly well and there's no reason to change it. But one answer to that it seems to me might be that technology is the game changer.

In other words, the example I gave yesterday, and forgive me for raising it yet again for the audience, is that I have a search warrant for my paper diary. I know what's in it. I know what I've written. I know I've got my fingerprints and possibly some DNA over it, so I know what the police can do with it.

That's not true at all if my phone is seized by the police under the Crimes Act because I know some things which are on it, but exactly how that's analysed, because that's analysed, sold off, applied by algorithms and so on by the DCPs themselves, that is one thing which makes the content of the mobile phone just fundamentally different from my paper diary. That's one thing and that is relevant, I think, to public trust.

The second thing is this, I am concerned that no matter how able the eligible judges are, they simply may not be able to fully appreciate the technical consequences of what they're doing, unless they have some technical assistance available to them.

Now, I appreciate that an eligible judge who receives a TI application from you may well say, "Look, I don't understand paragraph 10 of the affidavit. Please explain", and you go back and you give more detail. That's all fine, but it is, as one of the people this morning said, it's the sort of unknown unknowns if you don't know. Well actually, there's a much less intrusive

way of doing it, for example, which the judge might not know at all, or simply mightn't understand what the technology means.

I guess I'm looking at two things. One is, is it a good idea for the eligible judge at any stage of the process to have access to an independent scientific person or technical person who can say, "Well, Judge, this is what it means". You might like to ask the police for more details about this or that.

So, just deal with that question first. That's what they do in Britain. Is that, in principle, something useful, providing it doesn't clog things up and make things take a lot longer?

MR KENT: I can't see any reasonable objection to that approach. Simply ensuring that members of judiciary are better informed to make better decisions by necessary technical advice seems more than appropriate.

DR RENWICK: The more general question I think is perhaps one I should put to Home Affairs. I mean you've given your answer I think about how the powers work and so on. If you just bear with me for a minute. Ms Johnston has some questions.

MS JOHNSTON: I had a couple of questions. If I could take you back to section 3LA orders for a moment which are, of course, the power to compel people to provide assistance. Taking up a point that was raised yesterday in submissions and ventilated somewhat with the Australian Human Rights Commission, there isn't at present, on our understanding, any particular protections around the issue of section 3LA orders in respect of juveniles or at least nothing that arises directly from section 3LA itself.

So, noting that from just the prosecutions themselves that have been in the public domain, in counterterrorism in particular, a number of suspects are juveniles. Noting at the same time that there are special protections for investigation periods and the like for the arrest of juveniles in that context, is there anything in the legislation or in the AFP governance framework that applies a different standard for the use of those coercive orders against juveniles?

DR RENWICK: If you wish to take it on notice, that's fine.

MR KENT: I think I can answer the question but there may be other aspects we need to take notice on. As we understand it, the TOLA itself did not amend the processes or protections that already exist and are afforded to individuals during the execution of search warrants under the Crimes Act 1914.

The section 3LA is an order issued by a magistrate requiring a specific person to give police information or assistance that is reasonable and necessary. Such assistance, in summary, is for the purpose of enabling police to access, copy or convert data held or in accessible form from a computer or a storage device, subject to a search warrant.

We think in practice if police came across a child in possession of a mobile device while executing a search warrant and suspected it contained evidential material, they would consider seeking the consent and any required information from a parent in guardian in lieu of seeking a section 3LA order on a child.

In other circumstances, it might be appropriate that the person aged under the age of 18 might be named in the 3LA order itself or is the registered owner or user of a computer. Whether there should be specific protections for children is probably a policy question best asked of the department, but in practice, I think police would continue to apply the normal provisions of the Crimes Act in executing a search warrant if children are involved.

DR RENWICK: Can I just ask one follow up. If you were to go down the 3LA route for a child, presumably the fact they were a child, if you knew they were a child and I appreciate you might not, is something you would reveal to the magistrate in the application?

MR KENT: Yes, absolutely.

MS JOHNSTON: Just again on section 3LA orders, and I take your point that section 3LA predates TOLA from the AFP's perspective, as I am sure you are though, one of the things that has occurred in the TOLA reforms is that an equivalent or comparable power has been extended to new agencies, and that includes in particular powers under section 64A of the Surveillance Devices Act and section 34AAA of the ASIO Act.

It was raised in submissions by some other submitters and it was discussed again yesterday in the hearing that some of those submitters have taken the view that the power that ASIO now has under section 34AAA might amount to a power of detention, and in particular there, because of the fact that an order must specify a time and place at which a person must provide assistance in order to comply with the order.

As you might be aware, and again, I'm happy for you to take it on notice if you can't answer it on the spot, a provision to that effect already exists in the AFP's Crimes Act power, section 3LA(4). The question I have for you is relatively limited, in the AFP's execution of that power pursuant to order

to date, has it been the AFP's practice to treat that as a power of detention independent of for instance a power of arrest?

MR KENT: Yes, I will take that on notice in order to give you a better – I think a more fuller response to that question.

MS JOHNSTON: Just one final question from me on a different issue, and again I appreciate we'll be speaking to Home Affairs later, but something that's been raised over the past day and a half has been the breadth of objection to the fact that the threshold for a serious Australian offence under the TOLA reforms is three years and that the equivalent concept of a serious offence under the Telecommunications Interception Act is seven years.

From the AFP's point of view, would it cause any significant concern if there were to be a recommendation that it be reformed such that the Telecommunications Act serious Australian offence definition is also seven years?

MR KENT: We're obviously comfortable with the current arrangements, but we would understand if that needs to be considered in the broader context of other legislative requirements. I think that's probably more of a matter for policy and department's views.

DR RENWICK: Just one final question then from me. One of the things I've learnt in this inquiry is how quickly technology changes, in ways we perhaps can't predict. At the minute do you think the TOLA legislation is sufficiently technologically agile to cover your likely requests?

MR KENT: I think the legislation is – no legislation is a silver bullet in this environment, and we certainly don't hold that expectation, but it demonstrates incremental improvement into enhancing law enforcement's ability to keep pace with technological change. It's suitably agnostic to the technology that is evolving at such a rate. And I think that is reflected in the nature of engagement that it encourages with industry.

So from my point of view, and I defer to my colleagues, but from the AFP's perspective it is more agnostic in its approach, so that it does enable the rapidly changing environment to be better addressed. We see TOLA as a key incremental improvement in the current legislative framework to support law enforcement investigation and action.

DR RENWICK: One just footnote to all of this, although I'm not reviewing this, I mentioned the possibility of an Australian CLOUD Act agreement with the United States, Britain now has one. I take it that because mutual legal assistance requests take a long time, and the CLOUD Act does not,

in principle that would be a significant operational advantage to you were it be negotiated.

MR McCARTNEY: We strongly, strongly support that legislation, and again, Dr Renwick, in terms of – particularly in terms of the complex cases that we investigate, the majority of them have an overseas nexus where we have to obtain evidence from overseas by way of MAR, and I think the ability for us to obtain that evidence in a quicker fashion we'd strongly support.

DR RENWICK: I don't think it's giving anything away operationally to say that the head offices and the storage areas for many large internet companies is America, hence the significance of a CLOUD Act – a possible CLOUD Act agreement.

MR McCARTNEY: Correct.

DR RENWICK: Unless you had anything further, gentlemen, that's all we've got, and may I continue to thank you for your assistance to me.

#SESSION 6: Department of Home Affairs

I invite the representatives of the Department of Home Affairs forward, and I particularly welcome Mr Hamish Hansford, the Acting Deputy Secretary Policy of the Department, and forgive me if I don't pronounce this correctly, Ms Rebecca Vonthethoff – is that correct? Close – Acting Assistant Secretary National Security Policy.

Obviously you're the department which administers the TOLA legislation, there's a reason why I wanted to hear from you last, because I want to hear your responses, if any, to what's happened so far in the hearing. So, Mr Hansford, did you have an opening statement?

MR HANSFORD: I did.

DR RENWICK: Please go ahead.

MR HANSFORD: Well, thank you so very much for the opportunity to appear before you as part of your inquiry. I thought it would be helpful to canvass five issues that we see that have come up in evidence before you, Dr Renwick.

DR RENWICK: Thank you.

MR HANSFORD: So the first issue relates to systemic weakness and systemic vulnerability. One of the major points of discussion has really been around the definition of both of those terms within the Act. The current protection is designed to prohibit agencies from asking for or requiring technical assistance from industry that would introduce a systemic weakness or vulnerability, and it's designed to prohibit agencies from asking or requiring industry to build back doors. And I think we've seen that repeatedly throughout the evidence.

The current protection prevents assistance being sought where it is likely that this will weaken a form of electronic protection used by a non-target individual. The current definition and prohibitions were developed following consultation with agencies and industry, public exposure draft of the legislation and the recommendations of the Parliamentary Joint Committee on Intelligence and Security.

The present construction in the legislation is complex. But a more prescriptive or specific model raises significant risks like failing to protect cyber security by not applying equally across technologies, and making the industry assistance framework impossible in practice for agencies to use, and the use of the industry assistance powers to date has not revealed issues with the current construction, and you've just heard from the AFP and their evidence.

But the government is open to look at what you find throughout your evidence and consider alternative models put forward by both you and the PJCIS. So that's the first issue.

The second issue relates to judicial or AAT authorisations of requests and notices. So concerns have been raised in evidence regarding the lack of independent authorisation of industry assistance requests and notices. It is important though to remember that industry assistance powers do not by themselves allow agencies to obtain content or telecommunications data. This only continues to be available subject to warrants and authorisations, and Schedule 1 of the Act did not change this requirement.

There are also tangible limits on what assistance may be requested or compelled to prevent the authorisation of technical measures that would undermine cyber security. Technical assistance notices are about existing capabilities, not building new capabilities. Assistance may only be sought where it is reasonable and proportionate, where compliance with the request or notice is practical and technically feasible, and when it will not introduce a systemic weakness or vulnerability.

Then the layer below it, about technical capability notices, they don't involve the creation of – they have a strong authorisation framework for the creation of a new capability, with the Attorney-General, the Minister for Communications both having to agree to the issuance of a notice, and respectfully, looking at their different portfolio interests, and the consultation requirements that are required within the legislation and the panel arrangements that are described to the legislation that include both a technical expert and an ex-judicial officer are the safeguards inherent in the legislation. So that's the second issue.

The third issue relates to the impact on Australian and international technology – the Australian and international technology industry. The government has said publicly that it strongly supports the communications industry and encourages the responsible use of technologies. The industry assistance framework is designed to ensure agencies can operate in light of new and emerging technologies without imposing an undue burden on providers, and without compromising the competitiveness and reputation of industry products and services.

The legislation does not impose any standing obligations on industry or require providers to change their operating practices or the design of their products and services. Assistance powers are subject to detailed decision making criteria and consultation requirements designed to protect business interest data security and have minimal impact on industry.

Agencies must take into account the interests of the provider and consult on new capabilities being developed. To the extent that the perception of the Assistance and Access Act is causing harm to Australia's technology industry, and it is impacting business decisions, the government is making every effort to try and address this perception. These efforts include engaging with key industry stakeholders, and we continue to do that consistently, particularly those impacted by the Act, identifying and correcting common myths and misperceptions, and publishing fact sheets and administrative guidance, all of which are on the Department of Home Affair website.

We contend that any future changes to the Assistance and Access Act may counteract the work being done to dispel the misconceptions about the intended purpose of the Act to the detriment of the Australian and international technology industry.

It is difficult to rebut or grapple with anecdotal reports of lost business that have appeared in some submissions from industry, without having an understanding of the specific facts, and we'd encourage specific examples

to be tabled to your inquiry or separately to the Parliamentary Joint Committee or the department. That's the third issue.

Fourth issue, the service of requests or notices on individual employees, and I know you've asked about this today, is not now and it has never been intended that individual employees would be asked or required to provide assistance without informing or consulting their employer. While an individual employee may receive a request or notice seeking assistance, for example where the individual is their organisation's law enforcement liaison officer, it is the corporate entity, not the individual, who is being asked to assist. That individual can and should discuss the request or notice with their employer, as required, to consider and provide the requested assistance.

The fifth issue, compatibility of the Assistance and Access Act with the CLOUD Act, and you canvassed that with the AFP. We've been in intense discussions with the Department of Justice in the United States, and they have not identified any issues with the Assistance and Access Act that would prevent Australia from successfully negotiating a bilateral agreement with the United States under the CLOUD Act.

Such agreement would facilitate for the reciprocal cross border access to communications data or content of communications, as you've discussed with the AFP this morning. It is in complete contrast, and they are very two separate and distinct processes in place between the Assistance and Access Act and the CLOUD Act, and we can discuss that in further detail if you have further questions.

In conclusion, we'd like to just reiterate our gratitude for the opportunity to appear before you today, and really want to support your inquiry and provide you with all of the information that you need to make judgments, and I know the government's asked you to look at the inquiry and we'll consider the findings both of your inquiry and the PJCIS, and look forward to discussing with you today some of those issues.

DR RENWICK: Mr Hansford, thank you, that's most helpful. Can I start with perhaps a discrete issue, which is the individual employees issue. So the particular question I think I was asked yesterday, and I don't know the answer to it, and you might want to take this on notice, is what if say the DCP is a relatively small entity, they don't have a large technical capacity in-house, or they don't have lawyers in-house, is it your view that they're permitted under the current law to go and retain a solicitor, to go and retain a technical consultant, who would of course, or should be, bound by the same secrecy provisions, and if the law doesn't say that is there any problem

with a recommendation that it should? Providing everyone's bound by the secrecy.

MR HANSFORD: So our view is that support staff within a business do extend to professional advisors such as lawyers, where they're materially having an involvement in the business. I think the issue on the face of the legislation, why the word "individual" is in there is to capture individual who will be provided with a notice and individuals who are sole traders. So on the face of the legislation you can read it and think, oh, it's just one individual, and you're right, the secrecy provisions are quite daunting when you look at them. And those two issues have been both difficult to reconcile, but we're trying to provide better communications to say that it is the whole company and it is not bound by one individual. But, Bec, would you like to add anything?

MS VONTHETHOFF: Yes, so just to clarify, I think the word in question, if I have it correctly, that's caused some concern is the use of the word "person" in the description of designated communications provider. And we've sort of explained that that needs to include sole traders for example, but when it comes to a notice that is issued to a legal person that is a corporate entity, then the person in question is the corporate entity, and whichever individuals within that entity need to deal with the notice can and should do so.

On the separate point about legal advisors and that kind of thing as well, I'll need to go back and confirm maybe on notice the detail of it, but from memory there are provisions in the use and disclosure provisions that provide exceptions if you need to seek legal advice and that kind of advice.

DR RENWICK: Well, there are, I can give you the reference. So at page 77 of the reprint, 317ZF(3B) does indeed permit one to obtain legal advice, and presumably that's external legal advice as well. So I think you're right, that does cover that.

MS VONTHETHOFF: Correct.

DR RENWICK: What about though the situation where a smaller DCP says, well look, for example, I don't know whether this creates a systemic weakness or not, I'd like to talk to both a lawyer and a technical consultant to work that out. Would it be a problem to amend 317ZF(3) to extend it to technical advice which isn't available within the entity?

MS VONTHETHOFF: Yes, I think that is something that we'd like to take on notice if that's okay, and get back to you.

DR RENWICK: Sure. Yes, but that I think is the concept. I accept the point that you need to be able to target a DCP who's a sole trader. I understand that point. The next thing is the impact on industry, and I'm pleased, and I'm not surprised your engaging with stakeholders. In case you are not aware of it, yesterday there was an offer made, certainly by Internet Australia, and I think perhaps also by the Communications Alliance Group, to – at Atlassian, to sit down with Home Affairs and, given that, as Mr Kent said, TCNs don't seem to have come up much yet, to discuss the TCN mechanism. And all I can say is I pass that offer on and it sounds like something no doubt you will consider.

MR HANSFORD: I think we've worked with – when you look at the industry guidance, we've worked really closely with industry in developing the guidance and we're always happy to sit down with companies who offer great interest in sitting down with us and working through different proposals and different issues with the legislation, trying to clarify it, making sure the language is appropriate for industry. We'd very much encourage that.

DR RENWICK: All right. Can I come then to the question about the judicial model and so on, and I think there's a number of issues here. So the first matter it seems to me is the TCN, if we can just start by looking at TCNs. So I must say my view at the minute is that that is quite an intrusive and substantive power, it's not an insignificant power. You're asking a DCP to do something new, and I think we all agree that's obviously one thing which sets the TCN apart from a TAN. They're asking for a new capability.

Historically, when there's a coercive requirement to positively do something like that, I think it's fair to say that's generally been done by – ASIO's in a different category with the Attorney – but if it's the police, that's generally done by way of warrant, and generally done by way of an eligible judge or an AAT member.

So my starting point is that a different course is being taken in this Act, that's not to say you can't take a different course, but it is certainly open to argue that it's really quite similar in intrusiveness to other powers where there is eligible judicial or AAT approval. So that's the reason why I start with the TCN as an example.

The next point I think in the argument would be it is true that the Attorney-General must consider the views of the eligible judge – or sorry, the judicial reviewer, sitting with a technically qualified decision maker. I think it's fair to say that a lot of the submissions say well, that's the government

appointing the technical advisor. I think everyone would accept, if it's an eminent former judge, that's an independent person. Put that to one side.

But there is some unhappiness, I think it's fair to say, about the fact that the technical advisor is appointed by the Attorney and there is no capacity for industry to nominate a technical advisor. In the United Kingdom, for example, with the Technical Advisory Panel, I think I've got that right, as opposed to the Technical Advisory Board, there's a retired judge in the middle, and government nominates a technical advisor, and industry as a whole nominates a technical advisor.

And so there's a panel of people who industry, perhaps Aust-Cyber, perhaps someone like that might be the conduit, they nominate the people. Sure, they can be required to have security clearances, but I think it's fair to say that there would be a lot of support from industry if they felt that they had a capacity, albeit through an industry body, to nominate a trusted technical advisor to form part of the assessment process. So I just – that's the next step in the argument.

The next step in the argument of course is well, some people have described the role of the Minister for Communications as a double lock. It is true that that is a different minister and there are slightly different requirements that that minister is considering. But leaving aside the personalities and the people who might fill those offices from time to time, nevertheless the A,ttorney and the Minister for Communications are both members of the same Government, and the same Cabinet and there's at least some administrative law which suggests that in those circumstances they might both be bound by a Cabinet decision. As a matter of principle you understand, I'm not talking about anyone behaving improperly or anything like that.

So I think that's the next step in the argument. And the final thing of course is it's the Attorney-General who's issuing a coercive power when otherwise the Attorney only does so, coercively, in relation to ASIO. And that's been seen up to now as a special case and we can come to ASIO in a minute.

So those are the steps in an argument I think which is at least for TCNs, give they're coercive and given those other matters, it should be going to an eligible judge or Tribunal member, by all means, and I think very importantly, with technical advice. Because my very firm view is that some of this technical stuff is going to defeat your average lawyer, myself included, and it really is important they have access to technical advice.

So that's the argument if you like, taking TCNs as an example, that it's something more than, quite significantly more than what's the warrant

granted for say the content in the mobile phone. Would you like to respond to that?

MR HANSFORD: Sure. I might start off and be supplemented with some further information. The oversight arrangements in the legislation are premised on the escalating regime and the cooperation with industry. So by the time a TCN would be contemplated to be issued, there would have been significant engagement with a DCP, there would have been significant amounts of discussion involved, in order to, both from a law enforcement and intelligence community side, to understand the precise configuration of a DCP, and to understand what might be possible.

So that's going to the first point. The second point is that in issuing a TCN, the cost lies with the agency that is asking the Attorney and the Minister for Communications to consider a TCN. So any thought that a company would be required to build a significant capability that they would have to fund, which may have a major impact on their business, is actually – the fiscal burden is placed on the authorising agency that's asking the Attorney and the Minister to consider issuance of the notice. Which I think goes to a counter argument perhaps that there are existing mechanisms about how practically, would this legislation work and then is it appropriate for a double lock or for judicial oversight of the TCN.

So I'm trying to mount a counter argument. So that's going to the second point. The third point is that notwithstanding both an Attorney and Minister for Communications are members of a Cabinet, they are also independent decision makers under statute and they need to exercise those responsibilities independently, if you like.

The third point is that a technical advisor must be a consultant with a company, so it is not like the government will appoint someone without any regard to the DCP and their advice. And that should be taken into consideration by the Attorney-General. I think you've mentioned the ex-judicial officer being independent by virtue of their previous position and standing in the community.

And all of these elements I think go to significant mechanisms that have been put in place prior to obviously original jurisdiction in the High Court and judicial review. So they're some parts of the counter argument, but I might ask Rebecca if she'd like to add to any of those points.

MS VONTHETHOFF: Thanks for that, Hamish. I'd just add, and I think it has been discussed yesterday and today as well with the AFP, another element of intrusiveness you might argue is the intrusiveness of the access to the content or the telecommunications data itself. And I'd just use this

opportunity to sort of reiterate again that it remains the case that a warrant or an authorisation under for example the Telecommunications (Interception and Access) Act or the Surveillance Devices Act is required for that.

So to the extent there are concerns I guess in submissions about the intrusiveness of that power as it relates to obtaining content, I think there is, you know, appropriate oversight under those underpinning warrants and authorisations.

Something else I think I'd add as well is just wanting to be careful, particularly I understand with technical capability notices it is the development of a new capability, it is the more significant power I guess in that respect. For reasons that have been discussed before with the AFP and I think ASIO as well yesterday, I don't think anyone is anticipating that that power will be used, you know, at all frequently in terms of weekly, you know, potentially or something like that. So that needs to be considered I guess in the frameworks that kind of sit around it.

In relation to the two powers that weren't mentioned in your question but which I will mention now for completeness, so technical assistance requests I think, via the nature that they're voluntary, I guess we wouldn't see that it's necessary to have that kind of independent technical expertise or sort of judicial oversight, simply because if a company is concerned about what the request is or the potential impacts of them actioning that request, then they would just decline on that basis.

Technical assistance notices I think, as you were saying before, Dr Renwick, it's important to note that those are about the use of existing capabilities of a designated communications provider, so I think the concerns there around the development of new capabilities and what might be the sort of flow on technology impacts of that are significantly less for technical assistance notices compared to TCNs.

DR RENWICK: So that's really why I started with TCNs, because that's if you like where the policy conundrum is most acute. Just to pick up one point so far, yes, I agree, TCNs may be expected to be relatively rare. And that might be a good reason why I wouldn't recommend the creation of a brand new entity like an IPCO.

But is there anything at all, if I were still minded, despite your submissions, to recommend say, if I can put it this way, beefing-up the Security Division of the AAT with some eminent part-time technical members, who could assist the Deputy Presidents? And by the way, there, it's always open and indeed, historically there were Federal Court judges

other than the President, who were appointed as presidential members of the AAT.

So if you were to do that, then I don't think one could argue that that would be particularly onerous from a financial or logistical point of view, because you've got an existing tribunal. And I see you nodding, so I mean, you agree with that point.

So that then really leaves us with the policy argument about taking TCNs as an example, and given the seriousness of the steps of TCNs, and by analogy to what we've done historically for equally serious intrusive powers, is there anything more that you wanted to say about why the AAT in particular, in the manner I've discussed, wouldn't be a suitable model?

MR HANSFORD: I think the point that you've alluded to about ASIO and the Attorney-General, and indeed, other ministers of state, already have approval processes in place, without a double-lock or an IPCO-type model for more intrusive powers, arguably. So it is a policy that government would have to consider about why would you provide a double-lock for one element but not another? And I think it is a broad policy issue.

But obviously, you're open to recommend the consideration of the secure part of the AAT and government would kind of look at that in a broader context, I would assume. But the point is, the Attorney-General and other ministers have access to more intrusive powers to make decisions about more intrusive powers, and this would be an aberration in the overall framework.

But the secure part of the AAT I think is an important consideration, if you're so minded to recommend that in your inquiry, particularly because companies have very sensitive information that might be revealed, commercially sensitive, and the ability to protect that capability might well be a critical part of a TCN.

And perhaps the point we also didn't mention is, we envisage, in the framework that's been set out, that companies may well request a TCN, and may well say so they can defend to their own internal business processes, and own business model, "We would like a TCN, compelling us to provide a new capability, that we have the ability to develop,: and the government would pay for it, potentially, through a contract negotiation.

So I think the element about a TCN in that circumstance, and then having a secure part of the AAT fails to take into account companies might

actually request a TCN. So I think there are a couple of issues that we consider there. But Rebecca, anything else?

MS VONTHETHOFF: No, not really. Just to say - and it's probably more of a question for industry I guess, and I'm not sure what the comments are that you've received to date, yesterday and today, in the public hearings - but we had heard ourselves from discussions with industry that there might be some concerns with a compulsory mechanism, whether it be the AAT or another, where their technical information, whether they want it to or not, has to go outside, I guess of those direct agency to industry discussions.

DR RENWICK: Well, hold that thought, because I do want to discuss that with you as well. So just to finish off the possible thoughts there: I suppose two things which might suggest a different approach is called for; one is the social contract theory of government. You know, the idea that the government actually needs to justify its use of powers, more now than it has historically. Let me give you an historical example:

When Sir Garfield Barwick, long, long ago, became Attorney-General, he discovered, as he says in his memoirs, that ASIO didn't have warrant powers to read the mail. And as in England, what they did is, they said, "Well, it's the Royal Mail. We're the Crown, we can open it," and he said, "No, no. In Australia, we need to have that all set out in legislation." And so sometimes, different approaches are called for because the world has changed, and people's expectations have changed. And that is relevant, and that's what I'm hearing from a lot of the DCPs.

The other thing, which you will have seen me set out in my opening, is that the other thing which has changed in the paper diary compared to the phone is just the unknowable nature what is being handed over, and the need to reassure people about what is being done.

And the final point I think is this: you talk about the TARs being in a different capacity because they're voluntary, and that's true. But I suppose the person, or the interest which is not represented in that instance is the customer of the DCP, both their privacy and the security of the products they use. Again, the use of an eligible judge say, or an AAT model, it seems to me, might give reassurance to that notional person. I'm not suggesting they personally would be heard, but it could be taken into account.

Perhaps we might just deal then with the point about security of both agency information and about security of intellectual property of the DCP. So let's take a TCN as an example: on the one hand, the agency -I assume

you would agree - doesn't want a model which would reveal at all, their current operations.

MS VONTHETHOFF: Yes.

DR RENWICK: You're nodding, you agree with that. And equally, you can imagine, depending upon the sensitivity of the material, the intellectual property, you know, the source code of companies which do protect their source code; equally, they're going to be extremely reluctant to have that go outside the company.

MS VONTHETHOFF: Yes.

DR RENWICK: And you agree with that. So it seemed to me that there needed to be - take the example of systemic weakness, take the example of a bona fide dispute between the agency and the DCP where there is a disagreement about whether the red line which applies to all Schedule 1 of systemic weakness, has been crossed.

In my opening, I suggested a couple of possible models. Of course, you have the Constitutional right to go off and get a declaration, but as I mentioned in my opening, that's hardly a desirable first port of call for either government, or the DCP. And I mentioned two possible models; there may be others. One is in effect, a binding arbitral arrangement, which you may not need legislation for at all, where you have, by agreement, say the respected retired judge, industry expert, government expert, who give a ruling.

The alternative, whether it's part of a larger AAT process or just a standalone one, might also allow that to be determined. And in the Security Division, as you know, there is the capacity to hear from one side and send them out, and the other side; whereas in court, there may be Constitutional reasons why you can't hide information which is evidence, from the other.

So do you have any thoughts about how else you could solve that particular problem of say, a bona fide dispute about whether it's a systemic weakness or not?

MR HANSFORD: Can I just respond to some of the issues that you raised just immediately prior? And in relation to the social contract, the government's view in discussing this legislation was that the Attorney-General and Minister for Communications were politically accountable to the parliament.

And so notwithstanding your comments about the social contract and the expectations that I know have been reiterated by industry in some of the evidence they've provided you, that there is a counter-argument to that, that increasingly, the executive branch is becoming more and more accountable to the parliament. And the oversight mechanisms that have been put inside this Act, I don't think are contrary to some of those changing expectations. So that's the first point.

The second point in relation to the comments you've made around a paper diary versus a phone; it's an interesting scenario. It is, in a physical world, the lawful execution of a search warrant. If you applied the assistance and access regime over the lawful execution of a search warrant, you'd look at a house and say, "Well, what are the types of things industry might want to assist with?"

Well, you might require a locksmith to try and unlock the door; you might require an industry who is providing a CCTV service to the property, to cut off the CCTV service for a particular period, noting that that's for one individual and not creating a systemic weakness for all the CCTV provision for the security company more generally.

You might then enter into the house and find a computer which is not connected to a network, it's not connected to any of the outside world; and the search warrant would then allow you to look inside the computer. And that's all within the execution of a search warrant.

So how is it that the digital world creates such a different environment? And you've got an extremely valid point around potentially the 5G impact, the amount of data on phones, but equally, you might have a safe in that house with equally as much data, which is still able to be lawfully executed to receive information for the purposes of a criminal investigation, for instance, under a search warrant.

So whilst it is a valid point that a paper diary and a phone are two very different things, I think if you use the context of maybe the physical world and the lawful execution of a search warrant, versus the lawful execution of a TI, surveillance device, computer access warrant, and apply the same types of industry assistance, it is a more comparable argument between those particular theoretical kind of concepts.

In relation to the comments that you've made around systemic weaknesses, and if there is a dispute; I think the escalating regime that has been set out in the legislation is in stark contrast to the 313 provisions in the *Telecommunication Act*, which apply to domestic carriage service providers and carriers. And so what we were trying to do with the

legislation is say, "How do we give ore guidance for industry, noting that the extent of industry has increased, the changing technology has meant that communication is much more about over the top providers, international companies, and the whole communications supply chain?"

So how do you give more guidance in an escalated fashion, than merely relying on largely voluntary compliance in 313, although not only? And the model that we've tried to put in place is one - and I think the AFP spoke to you just previously about trying to work with companies and trying to resolve conflict at every step of the way.

DR RENWICK: And I accept that's what - I'm just talking about what if you get to the point where you can't agree?

MR HANSFORD: I think when you get to the point where you can't agree, you'll have had so much discussion by virtue of an agency putting a request to the Attorney about a capability, and having technical advice and an independent judicial officer providing advice. I take your point, it is not binding on the decision-maker, but it is an important - - -

DR RENWICK: This is for the TCN example?

MR HANSFORD: For the TCN.

DR RENWICK: Sure.

MR HANSFORD: But it is an important consideration.

DR RENWICK: Yes.

MR HANSFORD: And I think that agencies kind of deal with this type of conflict in a whole range of different areas, every day. But the way and the process that has been put in place, I think allows companies at every step of the way to raise objections, to have a 28-day period, to put in place all of the mechanisms that if you have a particular dispute, would try and resolve it prior to going to the ultimate decision-making, in a court.

So I think the way the legislation is set out, it actually provides a whole range of opportunities for amelioration of the dispute. And ultimately, an independent decision-maker and the Attorney and the Communication Minister making a judgement is an arbiter of a particular issue.

DR RENWICK: For a TCN, I get it.

MR HANSFORD: For a TCN.

DR RENWICK: I get it. What about though, for a TAN and a TAR? So you know, the agency says, "I'm not asking you to do anything new, so therefore we're not in TCN territory." But still, with the best will in the world and it's bona fide, they're at loggerheads.

MR HANSFORD: Sure. So I think in a TAR, it's really easy: they would refuse to co-operate. And then a Technical Assistance Notice, I think that there are consultation requirements already in the legislation. And I think in order for an agency head to issue a TAN, you have to have a level of understanding of what a company can already do'; if a TAN was served on a company and they said, "We can't comply with it," I think the agency head - and it's important also to see that it's the head of the agency too - I think they would be obliged to work with the provider to try and resolve the issue.

Because you're right, you're at a loggerhead and it serves no-one's purpose. And being punitive and saying, "You have not complied with a TAN," actually doesn't resolve the underlying issue of access to a particular thing.

DR RENWICK: Okay. Just one thing. My counterpart, David Anderson, former counterpart, in his question of trust report, thought it was highly significant when it came to public trust, that the relevant ministers (a) are much busier than they used to be in the past; and (b) have to grant large numbers of warrants already.

And effectively, if I can put it in the vernacular, Joe Public might say, "Well, the minister is just a very busy person. They aren't able to give the same amount of time that say, a retired judge might." Now, I appreciate it's a secret how many warrants and authorisations the Attorney-General gives, but you and I both know that that is not a small number; I think I'm not giving anything away there.

Is there anything you want to say about, just again, leaving personalities aside, but just public perception that ministers are very busy people and they can't give the time that a retired judge say, could give to something?

MR HANSFORD: I think the administrative changes that the Prime Minister both announced in July 2017, the then Prime Minister, and that were enacted in December 2017 and then in May 2018, to create both a Home Affairs portfolio and an Attorney-General's portfolio really reiterated the focus of the Attorney-General of the nation as the first law officer of the nation. And to solidify his or her role, to counterbalance the operational focus of the Home Affairs portfolio.

So notwithstanding ministers are extremely busy, the Attorney-General has taken on a much stronger oversight and accountability role, through the administrative arrangements that the government has decided to implement, and included in the Attorney's portfolio of a whole range of oversight functions.

So I think that construction can give the Australian public much greater confidence that the Attorney is one-step removed from the operational minister who has the day-to-day runnings of an agency. So I think that's an important point to realise.

DR RENWICK: Sure. You would be aware of what I said about the urgency of giving access to the state ICACs; is that anything you want to say anything about/

MR HANSFORD: Well, the government did introduce a bill in February, to extend the regime to the state and territory corruption agencies, and ACWIN. But I think the government is looking also at your inquiry and the PJCIS to look at holistic reform, if that's required, to assistance and access, and to consider it in a considered way.

DR RENWICK: So in other words, I don't need to say a great deal in the report about the desirability of ICACs having this power?

MR HANSFORD: No. And I think originally, they were in the legislation but were removed.

DR RENWICK: They were, yes. Just a couple of other things: so if you look at something like 317JC, whether a Technical Assistance Request is reasonable and proportionate; one of the points I've been trying to make yesterday and today is that some of those concepts are not easy. The legitimate expectations of the Australian community relating to privacy and cyber security, (e) and (f), are also important.

But take (h): the legitimate expectations. Is it Home Affairs' intention to give some examples, perhaps in policy documents, about what those expectations might be, so that people can say, "Well, we agree," or, "We don't agree with that"?

MR HANSFORD: We tried to work with industry on the industry guidance that I mentioned. Bec led that process; I might get you to talk to some of the detail.

MS VONTHETHOFF: Thanks for that, Hamish. So as Hamish alluded to, we worked with a range of industry and bodies to develop some fairly detailed administrative guidance on the operation of Schedule 1, or part 15 of the *Telecommunications Act.* That was uploaded to the Home Affairs website on 8 July, and sort of remains up there.

We've also worked very closely with colleagues from across the Commonwealth, and with industry as well, to put up some more, I guess sort of plain English and accessible fact sheets, question and answers, scenarios, and just general information pages on the website like that as well. We are continually looking for ways to add to that information, or to clarify anything further, so I would encourage anyone who is making submissions, or you know, take any comments from yourselves about ways that we can improve that material, and any information that's not there already.

DR RENWICK: I mean, philosophically, you will have heard me say I think already that as a cautious person, a cautious lawyer, I prefer to have some examples in the statute itself, if that's possible, because there's always a risk that a judge may say, "Well, that's the supplementary explanatory memorandum," or, "It's just a departmental guideline. Why do I have to have regard to that?" So I think you can expect that I will be saying, in-principle, it's a good idea to give examples. Of course, they can't be exhaustive.

Just a couple of other things. Thank you for your patience. My understanding - and you may want to take this on notice - of 317ZG, which extends the definitions, or it clarifies the definitions of systemic weaknesses and vulnerabilities, is, it doesn't prevent people from patching a vulnerability.

So you may want to take this on notice, but for example, if there was a TCN which gave a new capability, it wouldn't prevent the DCP, immediately afterwards, patching that vulnerability, if that's what they saw it as. But again, you may want to consider that, because that is obviously quite important for the DCPs to think, "Well, we want to, in the normal way, if we discover a vulnerability, patch it."

MS VONTHETHOFF: Yes, we will take it on notice, just to get back to you with any sort of additional detail. But I'd agree with the principle, and I think it is set out in the legislation clearly, that an agency can't stop a company from patching any kind of systemic weakness or vulnerability that it identifies. I would say though, that you shouldn't have a Technical Capability Notice that introduces a systemic weakness or vulnerability.

So I think what I'd need to come back to you on is, if you're talking about weaknesses that don't reach that point.

DR RENWICK: Yes. Just a couple of other things, then. And again, you may want to take this on notice. Is it fair to say that you've said in your supplementary documents to me, what you want to say about a different definition of "systemic weakness and vulnerability," the idea of an effects-based definition or not? But you will have heard the debate, and if you did want to say anything further?

In other words, I've said in my opening, I think there is something to be said for an effects-based definition, and there are things which appear to have merit on their face in the existing draft bill. On the other hand, I didn't think there was much to be said for the idea that something would or might create the risk of, because that's a standard which really could never be overcome. But I realise that's very technical drafting. If there is anything more you want to say on that, in addition to what you've said, please feel free.

And can I add this to it: weakness and vulnerability are synonyms in the dictionary. Do we really need to have both? Could you just have a definition of "vulnerability" or "weakness"? And while you're looking at that, I must say "class of technology" is something people have raised again and again, consistently. What on Earth does it mean? And again, a statutory example might be helpful, you know: is it all i-Phone 10s, is it all i-Phone 10s in Sydney, whatever it might be. And some sort of guidance.

If this gets to court - and eventually it will - you don't want to be in a position, surely, where the judge says, "Well, I just have no idea what the parliament's intention was."

Now, I'm conscious of the time, but I'll just ask my colleagues whether there's - oh yes, the three years versus seven years point; did you want to say anything about that?

MR HANSFORD. Yes. Just on the definitions, I think it's a real challenge, and we worked really closely with industry, to try and nut out weaknesses and vulnerabilities, and the construction of the legislation. And one of the critiques we invariably get in developing legislation is, we don't make it technology-neutral.

So the big challenge is, how do you try and create an Act that is technology-neutral that has broad applicability, and doesn't lock law enforcement and the intelligence community into things that are

unattainable, and they'd start to use other powers? So I think that's really the challenge. But we all take on notice some of your thoughts, and give you some more reflections, if that would be helpful.

In relation to the three and seven years; I think if you honestly look at the *TIA Act*, and look at the seven years and then look at the exemptions, I think you'll find that actually, the standard isn't uniformly seven years, and that the exceptions have increased over time. And that that relates to content of information, and both includes seven years and other periods, I think down to two years.

So actually, it's not a direct comparison just to look at seven years and three years. And the reason why we landed at three years is because it's the assistance to an investigation, potentially, and that it is not access to the content. But I think you've heard some of those arguments from both AFP and ASIO about the difference between the type of information requested under the *TIA Act* for example, and the assistance regime under this legislation.

DR RENWICK: That's very helpful. Sorry, did you want to add to that?

MS VONTHETHOFF: Yes, sorry, but if you'll bear with me jumping around a little bit, I just wanted to also comment briefly on the definitions sort of issue. And more just by way of a general sort of statement, I think there has been a lot of focus on the definitions in the current legislation of "systemic weakness, systemic vulnerability."

But you know, we do have the separate prohibition, which as you said, is in section 317ZG. And I think sometimes there's a bit of misunderstanding out there that the prohibition is in that separate provision; it's not in the definitions itself.

DR RENWICK: You'd agree, it's not perhaps the most perfect Act to easily understand?

MS VONTHETHOFF: I have spent a lot of time reading the Act. The other point I think about that discussion around class of technologies and that sort of thing, we'll definitely take on notice and have a bit more thought about that. But one point I think I can make today is there's also very clearly in the legislation, the concept of a "target technology," which is really a piece of technology, a device, a service, as used by an individual.

So noting that sometimes these analogies are imperfect. But to build on, you know, Hamish's analogy before, in the real world you'd be looking at how do you get into one house without affecting the other houses?

DR RENWICK: Yes.

MS VONTHETHOFF: Or you know, something of that nature.

DR RENWICK: Well, look, my last question, which I am happy for you to take on notice, in view of the time, is, you will have heard the questions we had to the AFP about the possible use of the powers against minors; and if you would just please talk to the AFP and perhaps come back with a joint response about that?

I'm conscious you will have seen my earlier reports on children in terrorism; you're obviously aware of our general obligation to treat the rights of the child as the primary obligation. And all I'm really thinking is, you know, is that something we need to have a safeguard in the legislation so that when a 3LA is sought from a magistrate, the magistrate needs to ask themselves, "Aha, this is a child. Do I need to be particularly certain of things?" Something like that.

You've heard the AFP say they would always identify that it was a child if they knew it was a child. But I think it's a point of principle which I think the law should deal with.

#Thank you and Closing Remarks - Dr Renwick, CSC SC.

Well, unless there is anything further you want to say now, ladies and gentlemen, those of you who sat through the last day and a half, I hope you found that as interesting as we have. It's enormously helpful. I appreciate the great assistance from Home Affairs in explaining how the law works, and is intended to work.

Just for the benefit of those here and for the record: the process from here is that we will continue to have discussions, including with Home Affairs, coming up with ideas. And can I include in that the idea of prescribed form, which I assume, you know, the concept is something you'd be happy to talk about?

MR HANSFORD: Indeed. We've circulated some forms to help agencies, but they have kind of modified them. So certainly open to exploring that.

DR RENWICK: I mean, the reason I raise it is, that having looked at the documents, I find marked discrepancies in the documents, and I think there is something to be said for a uniform baseline.

And I'll be giving a talk to the Lowy Institute in Sydney on 5 March, where I hopefully will have some firmer views. And then, I would hope to report to the PJCIS by early-June. And then it's time for another Monitor.

So at that point, ladies and gentlemen, thank you very much. And I thank Home Affairs very much.

MS VONTHETHOFF: Thank you.

MR HANSFORD: Thank you so much.

ADJOURNED INDEFINITELY

[1245]