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 THE *TELECONMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018* (CTH) [TOLA ACT]

08.43 AM THURSDAY, 20 FEBRUARY 2020
DAY 1

EXHIBIT LIST

Date: 20/02/2020

Number Description Page No.

Acknowledgement of Country and Opening Statement by Dr Renwick CSC SC

Ladies and gentlemen, I begin by acknowledging the traditional custodians of the land we are on, and paying my respects to elders past and present.

My name is James Renwick, and I am the current Independent National Security Legislation Monitor, or INSLM. And these are public hearings conducted under section 21 of the INSLM Act, for the purposes of my review into the *Telecommunications and Other Legislation Amendment Assistance and Access Act*, TOLA for short.

I have decided it is not necessary to require evidence to be given on oath or affirmation. The hearing is being transcribed and is being live-streamed, and I welcome all those watching it here, or online. There is great interest I think, both here and overseas, in this review.

I thank our hosts for providing this venue, and for facilitating the smooth running of the day. On my right is my Principal Adviser Mark Mooney; on my left is Laura Johnston, Counsel Assisting, and James Anderson, a senior lawyer from the Australian Government Solicitor.

Let me begin with some context, and then set out some tentative views. I welcome debate about them, because they are tentative. This is a good time for witnesses to say, "I've misunderstood the technology", or I'm proposing something unworkable or misconceived, or otherwise wrong. And for those of you watching online, similarly, please feel free to send supplementary submissions, but please do it soon. And then I'll be making a speech at the Lowy Institute on 5 March in Sydney, where I will likely set out some further thoughts.

For those of you who don't know me or my role, I'm a self-employed barrister and an independent statutory officer, appointed by the Australian Governor-General. I am required to review the operation, effectiveness, and implications of Australia's counter-terrorism and national security legislation; consider whether it contains appropriate safeguards for protecting the rights of individuals; remains proportionate to threats, and remains necessary.

I have royal commission-like powers, and I have used them, so I have a full picture about how the intelligence agencies and the police are using their TOLA powers. It is one of the key parts of my role that even though members of the public can't see classified material, they can be assured that

I can, and do. I have produced eight reports, which you will find on my website.

Usually, I produce reports of my own motion, or at the request of the Australian Prime Minister or Attorney-General. This, however, is the first time I have received a request from Australia's Parliamentary Joint Committee on Intelligence and Security, or PJCIS.

When TOLA was enacted in December 2018, there was, for various reasons, a short time for consultation, before it became law. And I think it is fair to say there was concern, even anger, expressed about that short time, especially by the designated communication providers, or DCPs, who under the TOLA Act, cover the full range of those involved in communication over the worldwide web of content and data.

Some submitters say to me, the lack of consultation of itself means TOLA should now be repealed in its entirety; I don't think that's realistic. Instead, I seek to answer the questions required by my role, principally, how has the law operated so far, is it effective in its stated aims, are there adequate safeguards, and if not, what amendments might now be made?

But can I immediately say something about the position of the State and Territory ICACs - although they're not all called ICACS - who do vital work as integrity agencies. I accept their evidence that they are affected, like the police are, say, by the phenomenon of the Internet going dark; they find themselves in a worse position though, than the police, as they currently have no access to powers under Schedule 1 of TOLA, including when they may need to investigate the police themselves. That seems unsatisfactory.

Time prevents me from producing an interim report, but noting the parliament may take some months to consider the reports by me, and then the PJCIS, I conclude the 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 may have such access; in other words, I formally commend now to the PJCIS, the idea of immediately recommending such powers with a view to prompt legislation to that effect.

If additional safeguards or new limitations, or even repeal, are what I end up eventually recommending concerning police powers, I think it is almost certain I would equally recommend them for the ICACs. I understand from the ICACs, the urgent need for them is for TARs and TANs, not the more controversial TCNs, which I will therefore defer for consideration in my final report.

This matter comes to me because in March last year, the Chair of the PJCIS, Mr Hastie, referred TOLA to me for review. And that was the first time, as INSLM, the PJCIS had referred me a review, and I hope it is not the last as our roles complement each other. I will report to them no later than 30 June; they need to report to the parliament no later than 30 September.

I note the intense media interest, industry, and public interest in this Act.

Let me then say something very brief about the threat landscape, noting that the first witness is the Director-General of Security, who no doubt will also say something about it. My website contains greater details, as do my annual reports, but in very, very, short summary, the espionage and foreign interference threat has significantly increased. The risk of an onshore terrorism attack remains at the probable level; it has been since 2014. That threat comes mainly from radical, violent Islamists; but there is also some radical violent right-wing activity. The external terrorist landscape also continues to evolve; for example, I, like many others, expect that ISIL will continue to shock and surprise.

But in this inquiry, uniquely for me, I must look beyond these areas of counter-terrorism and counter-espionage, to crime more generally, because the near universal use of the World Wide Web for legitimate private, commercial and government communications attracts criminals and other bad actors. When I speak of the web, I am conscious that it's fragmenting, if it has not already separated, due to extensive firewalls in China, Russia and elsewhere.

To give a few examples of illicit activities on the Internet, not necessarily limited to Australia:

1. ISIL has made, unfortunately, very effective use of the Internet to publicised, proselytise, and direct terrorism;
2. The Christchurch shooter live-streamed his atrocities on social media;
3. There is large scale theft of private data and corporate intellectual property;
4. There is local and trans-national organised crime, money laundering, trafficking of illegal drugs and arms, and child sexual exploitation, including in the dark web, which facilitates the commission of such crimes anonymously, and thus with impunity;
5. Finally, nation states and their proxies continue to engage in espionage and foreign interference. Mr Burgess's predecessor as Director-General, Duncan Lewis, last year said:

> *The current scale and scope of foreign intelligence activity against Australian interests is unprecedented.*

But they also work - this is to say nation states and their proxies - on their capacities to engage in cyberattacks, such as computer network attacks, not only say to disable access to another country's military to its computers and web servers, but also to have kinetic effects, for example, by releasing dam water, turning off power to hospitals, or attacking a stock exchange's records.

It is no accident that such conduct is capable of amounting to a terrorist act under Australia's Criminal Code. And it has not escaped media attention either; the New York Times Privacy Project provides many examples of such behaviour, and also of the large-scale theft of private data and corporate intellectual property. As do, may I say, the unsealed indictments filed by the US Department of Justice against, for example, members of the Chinese People's Liberation Army.

One answer to the bad actors, at least those who steal property, data or identities, is to increasingly encrypt content and metadata, whether at rest on a device, or in motion, such as a phone call. I am conscious there is not necessarily a bright line between content and metadata, but for the purposes of this morning, by "content" I mean texts, emails, phone calls and pictures. By "metadata" I mean such things as when an email was sent, the sender and recipients, their locations, how it was sent, how it was stored, and also what websites have been visited, what apps were used and so on.

There seems little doubt, on the evidence I have received, that the so-called "golden age" when such unencrypted content, or to an extent metadata, could easily be read and comprehended by police, integrity and intelligence agencies acting with lawful authority, has gone, perhaps forever. Instead, such agencies now speak of a virtual world which has "gone dark", "gone spotty", or even "gone different." And in large part, this is what led to passing the TOLA Act.

Some critics of the TOLA Act say that encryption is vital for lawful Internet use, on which commerce, banking, online shopping, and business communications for example, and personal interaction, including on social media, depend, and that TOLA will seriously undermine encryption. While I am very grateful for all the submissions I have received, I am wary of the idea there is a binary choice between encryption on the one hand, and say, law enforcement on the other.

Instead, I agree with statements countering that idea which come from two very different sources. First, there is the distinguished Encryption Working Group, assembled by the Carnegie Endowment and Princeton University, which recently said it rejects two straw men: absolutist positions not actually held by serious participants, but sometimes used as caricatures of

opponents. These are first, that we should stop seeking approaches to enable access to encrypted information; but second, that law enforcement will be unable to protect the public unless it can obtain access to all - and I emphasise the word "all" - encrypted data through lawful process.

And Sir David Omand, a former head of GCHQ in his recent book, which I have here, say this:

> *As with all hard public policy issues, there is no easy way of reconciling conflicting ethical concerns. Place the security of personal data and one's anonymity on the Internet above all else, and law enforcement is shut out, the rule of law is undermined, crime, terrorism and cyberattacks flourish.*

He insists on a right of access to all encrypted data for law enforcement and intelligence agencies, for example, through controlling or weakening encryption standards, and confidence in the Internet as a secure medium will be lost, and fragmentation of the Internet will spread.

As I have consistently said from the beginning, just as in the physical world, we don't accept in Australia lawless ghettos, where the law doesn't apply. And so also it should be in the virtual world. Intrusive surveillance powers, by all means conferred by law and with clear threshold and safeguards, which already apply in the physical world, should, in principle, apply in the analogous virtual world, unless there are good reasons to the contrary.

And one of the things I expect to hear from submitters in the next day or two is that in some respects, the virtual world is different. And I welcome that debate, but I am tending to the view that because so much data and content which we don't know about is contained on our mobile phones and computers, not least because it is generated by DCPs as they seek to monetise our personal information, there should be at least as great scrutiny and safeguards as there were pre-TOLA, where such information is made useable under TOLA.

So let me say something about pre-TOLA. Prior to TOLA, when it was often sufficient - as I have mentioned - to obtain, in unencrypted form, what was on a mobile phone or a computer as content or data. There were four main federal laws used: the *Surveillance Devices Act*, the *ASIO Act*, the *Telecommunications Interception and Access Act*, called the *TI Act*, and the *Crimes Act*.

And to give an example, ASIO or the AFP might, under the TI Act, seek access to telecommunications data, stored communications that already

exist, or the interception of communications in real time, or data in motion. That access might be given by a telecommunications provider without the need to seize the actual mobile phone. Under the ASIO Act, a computer access warrant could authorise covert access and copying of what is in a phone or computer. And under the Crimes Act, AFP constables executing warrants could search and seize evidential material, including material in electronic form.

There were, and are, important safeguards, often of long standing, for these intrusive powers. First, permission for access to data was, and is, granted by a warrant issued by an independent, eligible judge or tribunal member for the AFP, and by the Australian Attorney-General for ASIO. Metadata access is seen as less intrusive and can often be authorised by an agency head.

Importantly, complaints can be made to the Ombudsman for the AFP, or the IGIS for ASIO. Decisions could be judicially reviewed, there being a Constitutionally entrenched right to judicially review decisions of officers of the Commonwealth, our Constitutional founders having had in mind the famous US Supreme Court case of *Marbury v Madison.* And laws can be reviewed, for example by me, or by the PJCIS.

Now, TOLA, a large Act, is complex, but let me try and focus on its essence: there are five schedules, all important; most submissions focus on Schedule 1, though. In Schedule 1, the respond to going dark is really twofold: first, either by request in a TAR - a Technical Assistance Request - or by compulsion in a TAN - a Technical Assistance Notice - a DCP, a term designed to cover the whole spectrum of entities and people involved in the communication of content and data, hardware manufacturers, software and app manufacturers, cloud providers, telecommunications companies, must, for example:

> *Make the unintelligible content or data intelligible or accessible, or do another listed act or thing, but only if they have an existing capability to do so.*

And when they do so, they can't be sued civilly and they don't commit a crime.

What about where they don't have an existing capability? Well, then via TCN, or Technical Capability Notice, an agency may:

Request the Australian Attorney-General to grant a compulsory notice requiring the DCP to create a new capability, which the DCP doesn't then have, for the same purpose as the TAN.

The same civil and criminal protections apply.

The latest annual report, tabled in the Parliament, reveals that two agencies used powers under Part 15 of the Telecommunications Act, which is what I'm looking at; five from the AFP, two from the New South Wales Police. I have, or will, review all uses of Schedule 1 powers to date. I have also reviewed ASIO's use of TOLA powers, but I am limited in what I can say about that in public.

But can I make this important point: nothing I have seen to date suggests there has been anything like the idea of "mass surveillance" as a result of TOLA. To the contrary: what I have seen to date suggests that TOLA has allowed for pre-existing intrusive powers to be used in a more targeted, or limited, and therefore less intrusive fashion, against people who are not persons of interest, because the focus is on persons of interest. And that is an important change.

But - and it's a large but - none of the Schedule 1 powers can validly authorise, nor civilly protect, the DCP if it would create a systemic weakness or a systemic vulnerability. These are controversial and difficult concepts, and I expect we will hear much about them in the next day or two.

Unlike the underlying warrants or authorisations, TANs are not granted by an eligible judge or independent tribunal member, but rather, by an agency head or delegate; a departure from the normal course of the eligible judge or tribunal member granting a coercive power affecting privacy. Similarly, the Attorney-General issues the TCN, although a retired judge with a technical assistant, can be requested to give a report to the Attorney, but that is not binding on him.

There are three main focuses of the submissions I have received, and almost all of them are on my website, www.inslm.gov.au. First, the definitions in the TOLA Act of "systemic weakness and vulnerability" and related definitions, and a dispute resolving mechanism.

Second, where the current TOLA decision-makers are the Attorney or agency heads, should there be current or retired judges or tribunal members, assisted by technical experts who understand the effect of the exercise of the particular TOLA powers on privacy and the effectiveness of encryption?

And finally, the need for better record keeping requirements and clear statements of review rights when the compulsory powers are used, so that affected people and entities can exercise their rights of review, including making complaints to the Ombudsman or the IGIS.

Can I say something about the argument I've heard that the pre-TOLA laws have worked perfectly well, and the Schedule 1 powers merely make existing laws technology-proof, in the sense that the content or data has already been lawfully obtained, so it's just a matter of making it comprehensible. I remain to be convinced of this, as a matter of both law and practice, for at least two reasons:

First, I ask isn't the main point of TOLA that going dark has created a large problem for police, intelligence, and integrity agencies, to which the pre-existing law is an insufficient answer? An eligible judge granting access to encrypted content for example, might assume that the privacy impact is slight, but if a Schedule 1 power is to be used to make the data intelligible or accessible, for example, the impact on privacy may be large. Why, I ask, shouldn't both be granted in the same way?

And second - and this may be a matter more for the DCPs - doesn't the complexity of technology and the fact most people, including me, don't know fully what data and content is on their mobile or computer, and what it says about me? An example I was given in my travels was that my mobile phone or my Apple watch measure my gait or my heartrate, and they are unique, and that then links my use of those devices to me. So that is something I have learnt in this inquiry.

But as I say, we don't fully understand perhaps, as members of the public, what everything on my mobile or computer says about me. Should we use, then, the British model, of retired judges with distinguished technical advisers? Should we use something we already have, like the Security Division of the Administrative Appeals Tribunal, or AAT?

I am coming to the end. The second issue is the concept of systemic weakness or systemic vulnerability; are those definitions right? How are disputes about whether there is such a weakness or vulnerability to be resolved? I have already said, the powers can't be used under Schedule 1 to create such a weakness or vulnerability.

The definitions are critical. You will see from many of the submissions, there is criticism of them. Can I say firstly, I think there is general agreement among submitters that giving some statutory examples about what is or isn't a systemic weakness or vulnerability, rather than hiding them away in explanatory memoranda, is a good idea.

The challenge I set for all submitters is, if the definition isn't good, well what is a better one? I note there is a current bill in the Senate which seeks to do just that, and I am interested from witnesses at this hearing as to whether that is an improvement. My tentative observations are that the bill does helpfully focus on prohibited effects; it might also usefully make clear that it seeks to protect effects, not only those which compromise customers' privacy unnecessarily, but which risk their security and those of the DCP's products.

On the other hand, I am concerned about whether using the words "would" or "may in the future" in 317G(4), creates an unattainable standard because such a risk can never be ruled out.

The other aspect of this issue is how to adjudicate a bona fide dispute between an agency on the one hand and a DCP on the other, about whether the request crosses the line. Disagreements are going to happen at some point; it is undesirable to take them, as the first call, to court, the agency bringing a criminal proceeding, the DCP bringing a civil case. In either case, that would result in the risk of disclosure of what are likely to be highly sensitive police, intelligence or integrity operations on the Government's side, and highly sensitive intellectual and commercial property of the DCPs on the other.

So what are some possible solutions? In November, I had the privilege of meeting with the Investigatory Powers Commissioner's Office, or IPCO, in the UK. It was set up when my former counterpart, David Lord Anderson KBE QC, had concluded his report, "A Question of Trust." It is now headed-up by Sir Brian Leveson, a very famous and senior judge, and there are 15 senior retired judges, and some very distinguished technical advisers.

It works in this way: there is a double-lock system, so that if you can imagine a warrant and authorisation application is given first to the Secretary of State, the same paperwork is then given to IPCO. IPCO doesn't look at all the matters the Secretary of State looks at, for example, effects on international relations, but it does ask, looking at the same material the minister did, is the application lawful, proportionate, and reasonable? And if it's not, then the request is ineffective.

Having spent time with both IPCO and security and police agencies in the UK, I can say it's been very well-received, not least because it has raised the level of trust. My conversations also, on both sides of the Atlantic Ocean in the US and the UK, made it clear to me anyway, that IPCO was critical to the UK obtaining a cloud act agreement from the United States. And it has been said publicly that Australia also seeks such an agreement.

So IPCO is one such model.

And they also have a technical advisory board, allowing, in effect, a private, binding arbitration, with a retired judge presiding, and a technical expert appointed by the agency. And critically - and this is an improvement on the TCN process, it seems to me - an expert appointed by the DCP or by an industry body, to determine such matters as whether a request is technically feasible.

What if Australia wants to use something which already exists? Well, there is something which already exists, and has done for a long time, and that is the AAT; it is independent of government, headed by a Federal Court judge, its Deputy Presidents are other federal judges or senior lawyers, and it already grants some warrants, and already reviews some ASIO decisions.

So one possibility is that an application for at least a TAN and TCN - and I'm sure some will argue also a TAR - could go for approval to the Security Division of the AAT, which is accustomed to dealing with highly sensitive or secret information. Now, a DCP which doesn't object to a TAN or a TCN needn't appear; if it did object, for example, as to whether the request was reasonable or proportionate, or created a systemic weakness, you could resolve it at a contested hearing. You could use one of the alternative dispute resolution processes currently available in the AAT.

Because there is a lot of technical material to be understood, the Presidential Member could, with advantage, sit with an eminent scientific or technical expert who would be appointed as a part-time member. To the extent they could publish at least some of their reasons, that would guide agencies and DCPs alike.

Appointment to the AAT of say, half a dozen really distinguished technical experts whose expertise would cover the likely range of technical questions, could also, it seems to me, have a joint role working as consultant for the IGIS and the Ombudsman in their respective audit functions. This is effectively what happens with IPCO.

So I look forward to comments on this possible law. The written opening, which is available to you out back, also goes through comments on Schedules 2 to 5. I'm not saying they're unimportant, but they've received less attention.

I look forward to hearing evidence from you all as witnesses over the next few days, and I now welcome Mike Burgess, Director-General of Security,

and Peter Vickery, Deputy Director-General, to give evidence. So Mr Burgess, if you could press the button in front of you so we can hear you?

#SESSION 1: Australian Security Intelligence Organisation (ASIO).

MR BURGESS: Good morning.

DR RENWICK: And good morning to you both, and do you wish to make an opening statement?

MR BURGESS: Thank you, I do. So thank you for this opportunity to appear before the review today.

To begin, I'd state ASIO's overwhelming support for the *Telecommunications And Other Legislation Amendment (Assistance and Access) Act* of 2018. This legislation, passed in December 2018, was used by ASIO within 10 days of receiving ascent; that is a clear indication of its significance to our organisation.

Over 95 per cent of ASIO's most dangerous counter-terrorism targets use encrypted communications. We are now operating in an environment where almost all electronic communications of investigative value are encrypted. This ubiquitous encryption is of benefit to society in general, and critically important, but increasingly, it does make it difficult to access, under warrant, data of security interest. The Assistance and Access Act has not solved this issue, but it has helped significantly by enabling ASIO to call upon the assistance of communication providers to gain targeted access under warrant to specific encrypted data.

This is done in a cooperative way. To date, all capabilities that ASIO has requested industry assistance to develop have been carefully and methodically designed in collaboration with the providers in question. This assistance has not involved the development of any backdoors to encryption or systemic weaknesses to network or devices.

The assistance and access legislation is not a marked extension of ASIO's powers, as some observers have suggested. Rather, the legislation helps ASIO attempt to keep up with the technical developments that make it increasingly difficult to achieve our mission objectives. Nothing in the legislation displaces the need for a warrant. Any activity that would've required a warrant before the Act still requires a warrant today.

The legislation contains significant safeguards to ensure that the rights of individuals are protected. A key safeguard is the prohibition on the building of a systemic weakness or back door to break encryption for all users. The legislation expressly forbids the use. Rather, the Act's provisions help ASIO to access under warrant the data of specific targets.

Another safeguard is that decision-makers under the scheme must be satisfied that requirements in the technical assistance notice and the technical capability notices are reasonable, proportionate, practical and technically feasible. In addition, providers may refer any requirements to build a new capability for review by a technical expert and a retired senior judge.

Providers may also apply for judicial review of executive decisions as an inherent part of the Australian legal system. The legislation includes very strong accountability mechanisms. In particular, regular inspections of ASIO's use of the provisions by a main oversight body, the Inspector-General of Intelligence and Security, who can access all ASIO material. The IGIS has strong investigative powers, akin to those of a Royal Commission.

The provisions of the assistance and access legislation are proportionate to the significant ongoing security threats that we face. The Act strengthens ASIO's ability to protect Australians, and to detect and prevent attempts to harm Australia and Australia's interests. Thank you, I am happy to take your questions.

DR RENWICK: Yes, thank you very much Director-General. Well firstly, can I say to those watching this that I have reviewed all of ASIO's relevant records, no matter how secret, and thank you Director-General for giving me access to them, and I'm going to be careful the way I ask these questions. But I think you've already said something about how important you see TOLA for your purposes.

You will recall in my opening statement I talked about some of the threats on the internet, and do I take it you broadly agree with how I've set out the types of threats - the broad categories of threats?

MR BURGESS: I do, and that's why I chose not to amplify how I see the threats today, I think you articulated that very well.

DR RENWICK: Thank you. Could I ask you then just a specific question? Do you have a copy of the Act there?

MR BURGESS: We do.

DR RENWICK: Could you just turn to 317(j)(c).

MR BURGESS: Can you give me a page number for that?

DR RENWICK: That's page 34 of the print I've got. So this is the provision which says:

> *Whether a technical assistance request is reasonable and proportionate.*

And this applies also in similar terms to the TCNs and TANs. So this is what you have to consider when you issue one of these, and there's some large questions there, national security, law enforcement and so on.

So one of the issues is (h), the legitimate expectations of the Australian community relating to privacy and cybersecurity. Now, can I ask you this - well firstly, what do you think they are? And do you think they've changed markedly over the last decade or so?

MR BURGESS: Certainly. I would certainly agree the interests - excuse me, let me just find that again - - -

DR RENWICK: It's (h).

MR BURGESS: (h), I've got that.

DR RENWICK: Yes, (h).

MR BURGESS: Yes, well the expectations of the Australian community - I would no doubt have the view that Australians would have an expectation of privacy. Totally agree with that point, that's why that's a very important thing for us to consider. Cybersecurity and privacy are interesting concepts, and I mean that in terms of your point around what has changed in the last 10 or 20 years as a result of technology.

DR RENWICK: Yes.

MR BURGESS: The starting point again though would be yes, Australian citizens would have an expectation of privacy, and they would have expectations of things being secure. Sadly, I think examples almost every day in the press show that that's not the case, and that's something that we're all grappling with when it comes to use of technology.

The other interesting thing for me though, and this is a view that rightly needs to be debated, is that in this tech-enabled world, our expectations of privacy perhaps pre-internet or in the early days of the internet, maybe we don't all quite understand what the internet is doing, as you described.

DR RENWICK: Well, can I interject by just giving you an example which occurred to me?

MR BURGESS: Sure.

DR RENWICK: So if ASIO or the police issue a search warrant for my paper diary, I know what I've written on the paper diary, I can take a photocopy, and if I think about it I would know that I have fingerprints or DNA. But that's all it says about me. If I am required to hand over my mobile phone, I have a broad idea of what text and email is there, or at least I can find out. But in truth, I have as a layman absolutely no idea about how that information is analysed, and indeed monetised, by all the app manufacturers or the person who creates the phone. If I take the trouble to read the terms and conditions, which are usually very long, I usually find that I've given away most privacy rights I've got. So the point I'm trying to make is, is it relevant when you're working out what Australia's expectations are about privacy and cybersecurity, that you've got things like the ubiquitous mobile phone where very few people know how much it says about them. Is that relevant?

MR BURGESS: Yes it is relevant, and that's the point I was trying to make, that that's something that we all need to engage in that debate. Your example of the diary and the notes you've written in the diary and the actual DNA on the book are easy to understand in this technology world what is actually in my device about me or anything else is not understood by many people.

DR RENWICK: No.

MR BURGESS: And of course that's why it's important we have this debate, because the focus tends to always be - and perhaps rightly so in part law enforcement and agencies such as my own in terms of what we have a lawful right to access and what that gives up, I totally get that, but then you think about the data that your phone manufacturer or your cloud provider has about you, absolutely we need to have a frank and open conversation about what's out there and how that's protected, and the expectations of the individual's rights to privacy. And just because you give them terms and conditions that are 20 pages long in language that mere mortals can't understand, maybe we all need to do better in that regard.

DR RENWICK: And I'm conscious, for example, the competition watchdog has in fact said just that. I mean, to use another analogy between the physical and the virtual world, if I drive into a carpark, I never read the terms and conditions, but I could. It's been worked out, I think, that on a typical mobile phone it's not just 1000 pages of documents about the terms and conditions, it may actually be 1000 documents. So very few people, when you add up the number of apps on a typical phone - - -

MR BURGESS: Absolutely.

DR RENWICK: And of course, you've also got the other problem that in realistically you can't opt out of it.

MR BURGESS: Correct.

DR RENWICK: Unless you don't want to use your mobile phone, and that makes life difficult. So with those matters in mind then - and given that these principles apply to all agency heads in 317(j)(c), how do you see concepts like the legitimate expectations, or to use some other examples, in (e), the availability of other means to achieve the objectives of the request or (f), the least intrusive form of assistance - if I can put it this way, for people who aren't subjects of interest. I mean, do you see that as something that you will develop internally and then discuss with the IGIS? Do you think you'll produce public guidelines over the years, or - in other words, how is a member of the public looking in at these powers going to say, "Aha, I now have a reasonable idea how the Director-General of Security might evaluate the legitimate expectations".

MR BURGESS: Sir, firstly I would come at that in terms of, "These the things that I and my agency do consider already today, we've used the Act, we considered this". As you've seen in our paperwork, when I am considering the brief, the information set out before me in a format that's consistent with the Act and actually in a format that we've agreed with the Inspector-General of Intelligence and Security. So we're already doing this, and we give consideration to that.

With regards to how that needs to be further explained, I would leave that to my colleagues in Home Affairs, as this body of knowledge is built up. There are no secrets in the secret world, and I would share that with the Home Affairs portfolio.

The other thing if I may in regards to the expectations on cybersecurity and privacy, the way I think about that particular point that you raised - obviously privacy, you raised this in your opening statement as well, but

for me it turns on, "I've got this power, I'm using it," access to the content comes through a warrant or authorisation, so that's in place. They set aside expectations of that individual's privacy. Not everyone else's, the individual subject to the warrant or authorisation.

And then to cybersecurity, a key part of this is actually the introduction of the ability not to introduce a backdoor or a systemic weakness, and in particular, the systemic weakness is important to me. I know that members of our society, depending on where you fall, will have a different view of what a systemic weakness is. But that's - in my mind, when I considered this, because I have no intention of introducing something that breaks the internet, no intention of introducing something that actually means whilst it may give me lawful access to Target A, I've now put every Australian's private communications at risk, because I would not do that.

DR RENWICK: No. All right, now, just in terms of people understanding their rights and obligations, one of the things - if I can put it this way, I've noticed in the paperwork across the agencies, is some agencies say more about what people's entitlements are under the Act than others. And what I'm inclined to recommend is that there be a prescribed form across all the agencies saying, "Look, if you're received this TAN, for example, here's what it can't authorised, systemic weakness and vulnerability, here are your rights to complain, depending on who's issued it, and here are some other key definitions for you." I assume in principle you would welcome that?

MR BURGESS: I would welcome that very much.

DR RENWICK: All right. In terms of oversight then, one of the things - you make the point that the IGIS has Royal Commission powers, and she looks very closely at what you do. At the minute, the Telecommunications Interception Act annual report doesn't refer to ASIO's statistics, and I appreciate in that the operational reasons why that is so. Those statistics are available to the IGIS though, and would there be any objection to those being routinely made available as statistics, not about details, say to me or say to the PJCIS?

MR BURGESS: I would not object to that. We already make them available in our classified reporting, and available to the Inspector-General of Intelligence and Security and the Parliament Joint Committee of Intelligence and Security, so no objection to that.

DR RENWICK: All right, thank you. Can I ask you a bit about the pre-existing powers you had? So ASIO, among others, has long had power to make requests of telecommunications industry providers under section 313 of the Telecommunications Act, or I understand that doesn't cover - I

appreciate that doesn't cover anything like all DCPs. So that's still there, and we've now got TOLA as well. Have you changed - I mean, do you now take a different approach about whether you'll go first to the TOLA Act or first to 313 now that you've got both available?

MR BURGESS: So we've used TOLA, as I've said, and we continue to use section 313, and there's been no change in the providers' response to that.

DR RENWICK: Okay. Can I ask you a more general question? So some DCPs say that it's very important for them to keep trust with their customers, and what they're concerned about is that they might have to agree to a request, a TAN or a TCN, but they can't tell their customers. Now, thinking aloud, they can tell the customers, I guess, a couple of things. Under the Act, they're able to say without identifying agencies, "Over the last six months we have answered the following number of requests," and indeed presumably they could also say, "We've never received one." They could also say, "If we ever received one, we would fight it."

And I suppose the final thing that might be said is that - and this is often in the terms and conditions of use, very often they say, "We would only comply with a request for information as obligated by law." Because as I understand it, many DCPs would have a lawful access function, if I could put it that way, so that it's available there to be used.

So although they mightn't be able to say, "We've helped ASIO on this matter or the police on this matter," there is still some reassurance available to their customers. Do you agree with that, and are there any other things one could point to? And this is to do with confidence. You pointed out the importance of encryption and the confidence people need to have, for example, that their banking is secure and so on.

MR BURGESS: So I'd certainly - firstly I welcome the guidance that you're giving said DCPs in terms of where they can go, and acknowledge that that is useful, so I would have no issue with that. Our experience is we've not had an issue, it's been very collaborative so far. I think as you've indicated in your opening statement, there will come a time where there will be a disagreement, and there's processes for handling that. I think the way it's set out today, there's a gradual escalation through that process.

But to your main point about would I have a problem or would I support if companies choose to say, "We've received no requests," or actually, "We've received your request and we're going to take our legal right to challenge it," I have no issue with that. I understand their position - I understand their position with their customers and why they want to do that. Of course, whenever I'm having those conversations with said carriers and others, I

would always fall back to my view that we operate under the rule of law here, and technology itself is not beyond the rule of law, and it's the law that drives what we do and enables us to do what we do, and I remind them of the oversight that we are subject to. And at least in my view, that gives the assurance that the use of our powers are always proportionate to the threat or matter we're dealing with.

DR RENWICK: All right. Can I turn to another matter? In my opening I talked about what will happen one day, no doubt, that you or another agency will disagree with a DCP about whether a request or a notice involves a systemic weakness or vulnerability. So just dealing with it step by step, you'd agree with me, wouldn't you, that it would not be a desirable first step for you to say, "Right, we're going to prosecute you," or for the company to say, "Right, we're off to the Federal Court to get a declaration." That's not a desirable first step, is it?

MR BURGESS: I agree, it's not.

DR RENWICK: Okay, so that being so, the question is how you try and resolve it if, you know, the usual discussions you have with the DCP haven't been successful. So in England - and you might use all sorts of different fora here. You could do just a private arbitration, you could do something in the AAT if the law permitted it. But do I take it that the broad concept of having a group of government technical experts, a group of industry technical experts and a retired judge in the middle might be a possible model for resolving that sort of bona fide dispute? Or should I ask Home Affairs that?

MR BURGESS: No, my intent here is to be very helpful. I am comfortable with the model that we operate under today, but actually the model we operate under is set by Government and the Parliament, so - and obviously you and this review have an important role to play in that regard. I'm open to actually what works for Parliament, because they'll ultimately set that. As I said, I'm comfortable with what we have today, we have this gradual escalation process, but I accept we'll get to a point where there will be a time we're not in agreement, and then how do we best resolve that. I think what we have today still allows that to happen, the retired judge and the technical expert assisting is a way through that, but obviously - - -

DR RENWICK: That's for the TCN, not for the TAN though.

MR BURGESS: Sure, but TAN doesn't allow us to build capability, so if you do a voluntary request, that's where we start, and if they refuse that, my objective is to get capability build, but TAN won't allow us to do that, so you go straight to the TCN and then there's a way of resolving that should

we reach that point of conflict. I'm comfortable with the system that we have, but of course that system is set by Government and Parliament.

DR RENWICK: All right, okay. I suppose really what I'm saying is that one of the complaints made, just about the process by the DCPs, is, "Look, we feel the system is stacked against us, sure it's great to have a retired judge, but it's a government-appointed industry expert." As I say, the English concept is that industry as a whole might be able to say, "Well, we approve a panel of people," if they need clearances, they get clearances. Can you see that that might actually assist in the DCPs thinking, "Well that actually appears to be a fairer system"?

MR BURGESS: I can see how people would see that as a fairer system, and I don't mean to be funny by that answer. In my view, obviously for me the Attorney-General is approving the warrants, so if the government is appointing the technical expert in that independent role, I'm comfortable with that, but again, that ultimately is a matter for Government and Parliament to set.

DR RENWICK: I understand. Can I ask you something - I haven't said anything much so far about Schedule 5 of TOLA, which allows you to make requests for assistance, which then give people protection - certain protections. Now, a couple of submitters have said that your powers under - and I'm sorry to be technical, 34AAA of the ASIO Act, which requires someone to assist ASIO in accessing data held in a computer or a mobile phone, it has been suggested to me that that might amount to a power of detention all by itself. Although I do observe that there's a similar power in the Crimes Act for the police, and it's not suggested they have a power of detention. So what's the ASIO view on whether that amounts to a power of detention or not?

MR BURGESS: Yes, I don't accept that. Home Affairs is the administrating agency for our Act, they don't believe it is, and my advice is the same, we do not agree with that view.

DR RENWICK: All right, well just a couple more questions. It may be hard to answer this, but laypeople look at the exponential rate of change in technology, and I guess legislators do too. At the minute, do you think TOLA is technology neutral in the sense that it's likely to be fit for purpose for a few years at least? In other words, if we have artificial intelligence used and things like that, is that going to be a game-changer, do you think, or does the law appear to be reasonably technology neutral as you see it?

MR BURGESS: I'm comfortable where the law sits at this point in time. As I said in my opening statement, it doesn't solve all the problems we have,

so the powers and the laws and capabilities we need to do our job are always under constant review, but as this currently sits we used it within 10 days of it coming to being. It's effective, it's actually helped us, it has made a difference. I'm comfortable where it sits today, but of course we've got one eye on the evolving nature of technology and the challenges that presents.

And of course, when I say that, I'm also very keen on security of that world in which we live in, and that is paramount. So any thought I have in that regard is about the proportionate and lawful access to targets of interest, not required in any way to jeopardise the security that we need in this connected world.

DR RENWICK: Yes, just one other question. So there are TARs and TANs, one is a request, one is a compulsory notice. Can I put it this way? Does it assist in getting a request, do you think, because a DCP is aware that at the end of the day, you could request at TAN for the same purpose? See, some people suggest that there shouldn't be requests at all, there should just be TANs, there should just be compulsory notices. Do you have a view on that?

MR BURGESS: Sure. Again, I'm comfortable. We believe it's a graduated response. Obviously the first step, lowest possible, and if that works, that's great, if we need to move through that we will, I'm comfortable with it. Remember, it also gives protections for the companies themselves. I recognise the critical importance of that.

DR RENWICK: Sure. Thank you, unless there's anything further you'd like to say, thank you both for coming in, I very much appreciate you participating in this and for the assistance you have given me, and access to documents, and I may indeed ask you for a few more, but thank you very much.

MR BURGESS: You're most welcome, and thank you.

DR RENWICK: Thank you. So I think we now have representatives of the New South Wales Independent Commission Against Corruption. At least I hope we do. And the New South Wales Law Enforcement Conduct Commission, and I invite them to come forward. Good morning Ms Dubois and Mr Butler - have I got that name right? Dubois, yes?

MS DUBOIS: That's right, Dubois.

DR RENWICK: And Mr Butler?

MR BUTLER: Good morning.

DR RENWICK: Could you just identify who you are and who you are speaking for please?

MS DUBOIS: My name is Bernadette Dubois, I'm the Executive Director of the Investigative Division of the New South Wales Independent Commission Against Corruption.

MR BUTLER: My name is Shane Butler, I'm the Director of Electronic Collection at the Law Enforcement Conduct Commission.

DR RENWICK: Of New South Wales?

MR BUTLER: Of New South Wales.

DR RENWICK: Yes, yes. Now, I'm right in thinking that in fact there were some joint submissions by, if I can call them, all the ICACs, including the LECC.

MS DUBOIS: Yes, that's correct, yes.

DR RENWICK: And you have seen in my opening remarks, I hope, that I have recommended that effectively immediately, you do have access to the TARs and TANs, at least for as long as the police are using those powers.

MS DUBOIS: That's correct.

DR RENWICK: Firstly can I start with that perhaps? I take it that the urgent need, sorry - I should go back a step. Did you want to make an opening statement?

MS DUBOIS: Yes, I do have a brief opening statement, Dr Renwick.

DR RENWICK: So please Ms Dubois, I apologise, I should've asked you that.

MS DUBOIS: That's okay.

#SESSION 1 - Independent Commission Against Corruption NSW & Law Enforcement Conduct Commission NSW

MS DUBOIS: The Independent Commission Against Corruption of New South Wales thanks the Independent National Security Legislation Monitor

for the invitation to appear at this public hearing. The Commission thanks Dr Renwick for the comments in his opening statement addressing the inclusion of State anti-corruption agencies.

The ICAC was established in 1988 in response to growing community concern about the integrity of public administration in New South Wales. The principal functions of the Commission are to investigate and expose corrupt conduct in the New South Wales public sector, and to investigate conduct that might involve certain criminal offences upon referral by the New South Wales Electoral Commission, and to actively prevent corruption through advice and assistance, and to educate the New South Wales community and public sector about corruption and its effects.

The *ICAC Act* 1988 gives the Commission broad jurisdiction to investigate any allegation or circumstance which, in its opinion, implies that corrupt conduct has occurred or is likely to occur. In deciding to investigate a matter, the Commission may use the powers it has under its legislation to gather information.

Investigations are diverse in character and can range from simple to complex and embrace past and current activities. They can require the use of various covert and overt methods of investigation. The Commission is defined as an interception agency for the purposes of the *Telecommunications (Interception and Access) Act 1979*. Commission officers can make requests for assistance under 313 of the *Telecommunications Act 1997* in circumstances where assistance is reasonably necessary for enforcing the criminal laws and imposing pecuniary penalties. Despite this, the Commission is not defined as an interception agency within 317(b) of the *Telecommunications Act 1997*.

This exclusion restricts us from accessing the industry assistance powers introduced through the *Telecommunications and Other Legislation (Assistance and Access) Act 2018*, and is a key concern area for our organisation.

ICAC New South Wales has provided comment to the Parliamentary Joint Committee on Intelligence and Security on a number of reviews, including their reviews in to the TOLA Act. The Commission has also provided comment on the comprehensive review of the legal framework of the national intelligence community.

In August 2019, you invited us to make a submission on your review of the TOLA Act. In response, we made a joint submission with the Law Enforcement Conduct Commission of New South Wales. Our key areas of concern is that ICAC New South Wales has witnessed a similar increase in

encrypted communications as reported by State and Federal police.

In a 2013 telephone interception warrant, the Commission would see approximately 20 per cent of encrypted content. The Commission now sees over 90 per cent of lawfully-intercepted information encrypted. This increase requires alternative methods of investigation, where industry assistance powers would be utilised.

In an investigation undertaken by the Commission in 2018, a member of a New South Wales public sector was receiving payments through a third-party application utilising end-to-end encryption. The Commission had an interception warrant, but from the information collected, we were unable to identify individual transactions. If the Commission had access to industry assistance powers from the TOLA Act, we would have made a technical assistance request, or TAR, to the third-party application. Information returned from the TAR would've assisted the Commission in identifying the payment gateway service and strengthened our position when seeking assistance from overseas banking institutions.

The longer we are precluded from access to industry assistance, the further the Commission will fall behind in understanding the technical capabilities of designated communication providers. Commissions without the powers may be omitted from interception agency meetings involving technical discussions, and the delay in access to industry powers could also result in unnecessary duplication in TARs or TANs to designation communication providers once we've been afforded the powers.

The LECC and ICAC New South Wales joint submission to your Office contains further information on our key areas of concern. The exclusion of State crime and corruption agencies and ACLEI from the industry assistance powers in the TOLA Act remains a matter of significant concern to ICAC New South Wales. The exclusion was only intended as an interim measure by the PJCIS, and the inability to access industry assistance continues to frustrate investigations undertaken by the Commission.

ICAC New South Wales intends to liaise with colleagues and State crime and corruption commissions and ACLEI in seeking a Bill to amend the definition of 'agency' in the *Telecommunications Act 1997*, to provide our agencies with access to industry powers.

I thank you for your time.

DR RENWICK: Thank you. Mr Butler?

MR BUTLER: Thank you Dr Renwick. I might just highlight some of the

brief points from our various submissions to the PJCIS and yourself. The LECC is an independent body exercising Royal Commission powers to detect, investigate and expose misconduct and maladministration in the New South Wales Police Force and the New South Wales Crime Commission.

The Commonwealth Attorney-General has declared the LECC to be an agency for the purpose of the TIA Act, allowing it to apply for and be issued with telecommunications interception warrants. The LECC significantly relies on telecommunication interception warrants to investigate serious offences alleged to have been committed by police officers.

The need for effective investigation of police corruption, we believe, is vital for the justice system. Police are provided with a wide array of powers, including the ability to detain, search, arrest, use force, enter premise, seize property, engage in covert investigations and surveillance. Due to these extensive and often invasive powers, the need for vigorous oversight mechanisms is evident and has been demonstrated by a number of Royal Commissions.

Corruption and misconduct of police officers compromises the confidence the public have in fairness, integrity and honesty in all police officers. Mistrust of police has detrimental effects on policing, as public involvement is a crucial element of law enforcement. Police often need members of the public to report and assist investigations.

The LECC has experienced quite an impact of encryption through its interception activity, similar to the ICAC. If you go back five years, around half of our intercepted IT communications were encrypted. Now it's well over 90 per cent. It also has an impact on our digital forensics activity, so where through search warrant, through coercive powers, we may seize hard drives or mobile phones for examination, again, some of these devices may be encrypted, preventing access to our evidence.

I finally just make a quick comment around the exclusion, as my colleague has. Both the chairman of the PJCIS, Mr Hastie, and the shadow Attorney-General did report to Parliament before the last election that the Committee fully supported integrity commissions' inclusion back within the Schedule 1 powers of TOLA. A Bill was drafted, unfortunately it lapsed when Parliament was preparing for the last election, so we concur as per our joint submission that we would very much benefit from the use of these - inclusion back within the Act.

DR RENWICK: Yes, well you've heard what I've said in - - -

MR BUTLER: And I should note, thank you Dr Renwick, we very much appreciate your sentiments in your opening remarks.

DR RENWICK: So can I unpack the problem a bit more then. So let's assume that you're doing an investigation of a potentially corrupt police officer or public servant. If you call them into a hearing - a private hearing, which you're entitled to do. Now of course, I understand you may not want to do that at an early stage in an inquiry. But if you do, you have the power, don't you, to say, "Please provide me with the password to your phone, the password to your apps," and so on?

MR BUTLER: Yes we do.

DR RENWICK: And so as a practical matter, if you're prepared to tip of the subject of interest, you can - is this right, generally overcome those sorts of encrypted issues because you can require the person to tell you what the passwords are? Now, I appreciate why you wouldn't want to do that, but is that fair?

MS DUBOIS: That's fair to say, but not necessarily operationally feasible, yes, yes.

DR RENWICK: No, I understand. So again speaking very generally, quite often I imagine the person of interest is the last person you want to get in, rather than the first person.

MS DUBOIS: That's correct, yes.

DR RENWICK: You investigate, you have tips, you have all those sorts of things. So what I take it then is of particular concern to you is if you get - someone rings up anonymously perhaps and says, "So and so is corrupt," to give the example that you gave, you know, they're getting illicit payments or whatever, and you want to get to the bottom of that, that's a good example of where you're faced with ubiquitous encryption, mainly of content, is that right, rather than metadata? Is encrypted metadata also a problem?

MS DUBOIS: It's also a problem, but mainly for us it would be the content and if we're in a covert investigation, as you've rightly said, they may not be the first person to call to a compulsory examination, and we may want to find out further evidence before we actually alert a wider range of people who are involved in the corrupt conduct.

DR RENWICK: Yes, of course.

MS DUBOIS: So it's the content early on in a covert investigation.

DR RENWICK: Yes, so I think I understand that. And do you think that encrypted metadata is going to become an increased problem over time?

MR BUTLER: Look, we find through our interception activity that we receive metadata and it's quite helpful. The metadata actually assists us in identifying what mechanisms, what encrypted means our targets are using. So we - through the metadata, going through interception, we can get an appreciation of the type of applications our targets use, so we don't see encryption of metadata as a hindrance at this moment in our agency. We find that the only tool we have to look at encryption used by our targets - and it certainly does confirm that - certainly with our targets, who are very surveillance-aware, that they tend to use encrypted means to communicate to further alleged criminal activity.

DR RENWICK: All right, another large question, you heard in my opening - I query this idea that you need a warrant, for example, to get the physical phone or to get the content, but you only need agency head's approval to get the TAR or the TAN. Did you want to make any comment about that from a policy point of view? It just seemed odd to a number of submitters, and at the minute to me, that you can say on the one hand TOLA is vital because the world's gone dark, but on the other hand, even though it's critical to unlock the content, it should nevertheless be granted at a lower level. That is to say, not by an eligible judge or Tribunal member, at the minute of course the agency head saying ICAC can give access to metadata himself, but he like everyone else has to go off to an eligible judge to get access to content under the TI Act. Do you see what I'm getting at and do you have any comment about that?

MR BUTLER: I would say, Dr Renwick, for our particular agencies, both our heads are retired Supreme Court judges, they are well-versed in applying judicial tests for the granting of warrants, well-experienced in that sort of thing. They are perhaps as qualified as you can get to consider the interference with privacy and other considerations when granting a request under this law.

DR RENWICK: Well, can I you - sorry, did you want to say anything, Ms Dubois?

MS DUBOIS: I agree that our Commissioners are eminently qualified, but if you want, I have no objection - I'm sure the Commission wouldn't - to have it as a more impartial law outside the investigation itself, to be an AAT member.

DR RENWICK: All right.

MS DUBOIS: I don't see that as a difficulty, but of course our Commissioners are qualified.

MR BUTLER: And I think the LECC would agree. If further scrutiny was applied independently, I don't think we would have a problem with that.

DR RENWICK: Because another way of looking at it is although I've limited my remarks so far to the TARs and the TANs, it may be that you get access to the TCNs as well. Now, at the minute of course, that's a politician, the Attorney-General, and I'm not making a political remark, but it's a Minister who's giving permission, and it just seems to me that it would be odd for ICAC to seek permission for an intrusive power from a Minister. That seems a little unusual, and if we take it a step further - and if there's a Federal ICAC, as there may well be soon.

MS DUBOIS: Yes.

DR RENWICK: Again, it's not criticising the individual in any way, but it seems odd structurally that an independent anticorruption body, which may after all be able to investigate Ministers perhaps - you certainly can in New South Wales, would seek permission from a Minister rather than an eligible judge or tribunal member.

MS DUBOIS: Yes, perhaps there should be that separation from it being a politician, with separation of powers, to it being an eligible judge who would be seen to be having more independence in relation to the grant of those. That's at its minimum, yes, I agree.

DR RENWICK: Can I ask you to turn to your submission? And in particular, to the very helpful LECC submission, which is annexure 1 to your submission to the PJCIS, and this is on the internet. And I wonder whether Mr Butler, if you could turn to page 7 and just talk me through the case study.

MR BUTLER: Right.

DR RENWICK: The Facebook case study, because that's a real and relatively recent example. Could you just walk me through what the problems were and how a TAR or a TAN might make a difference? And I appreciate also there may be some Cloud Act issues as well, but can you just unpick what you mean by all this?

MR BUTLER: Yes, so in that case study we were investigating, I guess, racist, sexist, abusive comments posted on Facebook against a Member of

Parliament. We believe that the activity - - -

DR RENWICK: This was by New South Wales police officers?

MR BUTLER: Sorry, yes, New South Wales police officers.

DR RENWICK: Yes.

MR BUTLER: It received publicity - I wouldn't want to identify people, but it received publicity at the time. We believe - - -

DR RENWICK: And just pausing there, you would regard that as a very serious matter to intimidate a Member of Parliament?

MR BUTLER: Absolutely, and also it breaches the - I think we were referring charges - I think it's 474 of the Criminal Code, there's an offence - a criminal offence about using telecommunications to threaten, harass, that sort of thing. I've used it myself formally as a police officer investigating those things. The key, I think, message for me in that example is that under the TI Act, those offshore providers are not captured in our legislative regime, and we don't have a formal mechanism to even just seek voluntary assistance, except through mutual assistance through the Commonwealth.

In that case, the data that we were seeking, which would assist us to identify the police officers posting those quite offensive posts and memes and what have you, we were seeking the IP addresses from Facebook to identify those officers. We were unfortunately unable to get that evidence, and the DPP noted that that was crucial to forming a prima facie case against those officers, so we didn't proceed with the prosecution.

Now, there are other mechanisms through mutual assistance to seek assistance offshore. In our view, they're slow, they're difficult, they're very bureaucratic. If we had inclusion within schedule and powers of *TOLA*, at least we could have a formal mechanism under legislation to go straight to Facebook and request assistance, and my experience over the years with carriers and other technical providers is that if they - there's not usually an antagonistic sort of relationship between law enforcement - where they see a just cause to support law enforcement they generally do, and we would expect that through a formal mechanism such as through Schedule 1, that exact scenario perhaps could've enabled us to gain that evidence and create a prima facie case.

DR RENWICK: So just to unpick that a bit, one of the advantages of TOLA is that it applies to designated communications providers, and that would pick up, say, Facebook, even though Facebook is headquartered overseas?

MR BUTLER: Exactly Doctor, I think that is one of the key things for our agency, to bring all those offshore providers, who operate in Australia, within a formal legislative framework. Look, we don't expect that you know, it's going to solve problems with end-to-end encryption, that even the providers in many cases won't be able to provide us decrypted information, we understand that. But certainly in cases such as this, where we're just seeking a little bit of metadata, we see that they certainly could assist, and I think the designation of DCPs is a vital change for us in certain circumstances and in certain investigations.

DR RENWICK: Turning to the Mutual Legal Assistance Treaty, as I understand it, they tend to take a long time?

MR BUTLER: They do, yes.

DR RENWICK: Including to the United States?

MR BUTLER: Yes, and my experience is that many investigators will just not bother because of the lag time. Investigations are dynamic in all investigative agencies, you're often prioritising resources and prioritising investigations, and long, drawn-out and intense processes to get one key bit of evidence will perhaps fall by the wayside when you can devote your resources elsewhere.

DR RENWICK: And as I understand it - you may not be able to comment on this, one of the reasons why Australia wants a Cloud Act agreement, as the Brits have got, is that then it is relatively straightforward to request information from, say, an American company which happens to be where a lot of the big companies are headquartered, and then they're happy enough to provide the information - the content, yes.

MR BUTLER: I definitely agree, Dr Renwick, I think if a Cloud Act agreement - legislation would be hugely beneficial to investigations. I guess we've seen quite a cultural trend away from traditional voice services and texting to over the top services, quite a trend where communications have gone onto social media platforms, and there is a substantial amount of those communications held in those American platforms.

DR RENWICK: What do you say to the argument that the use of the TOLA powers may create backdoors or inappropriately infringe on privacy and security?

MR BUTLER: I was listening to the previous witness, and in my mind I was thinking about it. I've been in this industry quite a while, and there is

a very important relationship between law enforcement and technical providers. In my experience - I understand that there may be disputes to be resolved ultimately, but where providers give us technical advice about their capabilities, I think we tend to take that advice. The providers, I think, communicate with us in good faith, and we have no reason to dispute what they're saying. If they were to advise us that by actions that we were requesting would compromise the security of any other individuals that are non-targeted through our warrants, we absolutely would not support or follow-through with that request.

DR RENWICK: Just to pick up on that, one of the themes in the submissions from DCPs is concern expressed by DCP employees that they personally might be the target. Now, the Department of Home Affairs' response is, "Well no, we have to have it referrable to people, including corporations," because after all, there could be a sole trader. But they say the normal course would be you'd go to the entity and if they need to get legal advice or whatever, there's no trouble about that. Do you want to comment on that?

MR BUTLER: Yes, look, I think - yes, absolutely the carrier or the DCP should be entitled to get their legal advice. I think it's very rare that a member of a carrier would be the target of an investigation. In that rare case, all I would say is - - -

DR RENWICK: You may have misunderstood me, it's not so much they're the target, but they feel that they're the recipient of the notice personally.

MR BUTLER: I see, I'm sorry.

DR RENWICK: Whereas Home Affairs says, "No, no, you'd be issuing it to the company, except if they were sole traders."

MR BUTLER: I see, sorry, yes.

DR RENWICK: Rather than the individual, and I assume that's what you would do too.

MR BUTLER: Yes, absolutely.

DR RENWICK: You are asking whoever it might be, Company X - although no doubt you have a point of contact.

MR BUTLER: That's right. Yes, so it's common to serve notices on, perhaps, the managing director, the CEO or something of that, but obviously that - it would go to whoever the nominated person in that

provider is, and we would deal with the nominated person who's been trained to deal with law enforcement.

DR RENWICK: Can I talk a little about oversight? So the first thing is you may have heard - I think Mr Burgess agreed with me when I said I thought it was desirable to have a standardised, prescribed form, so that a person receiving a TAR, a TAN or a TCN knows what their rights are, and I assume you think that's perfectly all right?

MS DUBOIS: Yes.

MR BUTLER: That's a very good idea.

DR RENWICK: Can you just both explain a little bit about what the - I think both of you have an Inspector-General, I think. Could you just explain on the record what the oversight mechanisms are for ICAC and LECC?

MR BUTLER: Look, there's State and Federal oversight of our activity. The State oversight falls to the LECC Inspector, which is independent of the LECC. The LECC Inspector has an inspection team, they inspect all interception agencies within New South Wales for interception warrants and use of surveillance device powers under the State Act. It's quite a rigorous oversight, and you will find that in this space, the powers for interception and collecting this type of evidence is so crucial to agencies that we take great care in making sure compliance is very strong. We employ dedicated staff to make sure that compliance is of a very high standard, and particularly in integrity agencies.

DR RENWICK: Yes, of course.

MR BUTLER: The Commonwealth inspections come from the Commonwealth Ombudsman.

DR RENWICK: So is that for the TI Act mainly?

MR BUTLER: Yes, so within the TI Act, warrants under section 46, 46A and section 48 would be inspected by the State authorities, because that's under the authority of the State TI Act. Stored communications, access to telecommunications data, any use of the *Surveillance Devices Act 2004* (Cth), would be inspected by the Commonwealth Ombudsman, and they do yearly inspections, and they're quite rigorous. The inspections that are scheduled for us are for a week. Typically they would send four inspectors, we would give them full access to our systems. Because we're small agencies and we by no means have as many warrants or authorisations for telecommunications data as the large police forces, the Commonwealth

Ombudsman tend to do a 100 per cent inspection of all our records, so it is quite rigorous.

DR RENWICK: Okay, Ms Dubois?

MS DUBOIS: And that is the same for our agency, the oversight of the inspector of the LECC and the Commonwealth Ombudsman. Shortly we're to have an inspection by the Commonwealth Ombudsman for our stored communications under the TI Act, and that's for four days, and they go through every single document, and they also on occasion interview the officers within the Commission as to the grounds on which they approve those stored communications, particularly - it is rigorous oversight, and we're required to report any anomalies in our annual report each year as to whether there were any - there hasn't been many, if any, but if they are they're slight in relation to formulas or a certain thing on a form, as opposed to any oversight of the legislation. But it is quite rigorous, and I would expect that would be the same with the TOLA.

DR RENWICK: So who would be performing the oversight for TOLA, would that be both the Inspectors-General and the Ombudsman?

MR BUTLER: It would just be the Commonwealth Ombudsman for that power.

DR RENWICK: Just the Commonwealth Ombudsman, I see. Can the Inspector-General talk to and share information with the Commonwealth Ombudsman?

MS DUBOIS: I presume so, but I can't answer that.

MR BUTLER: I don't think there's any restrictions, I can't comment on whether they do.

DR RENWICK: Could you take that on notice, because I'm interested in the idea in terms of where you've got this Federal system, it's at least theoretically possible that something that the Commonwealth Ombudsman turns up suggests a deficiency, which they might want to share with your State Inspector-General, and I just want to make a recommendation that they were permitted to share that information for that purpose. And I assume, you know, that that would not cause any difficulty?

MR BUTLER: No, we would welcome that, and we will find out and provide you with that information.

DR RENWICK: Sure, no, that's very helpful. Just a couple more things.

So you, I think, also have access under section 313?

MR BUTLER: Yes.

DR RENWICK: Now, it may be obvious, but just for the record, what are the advantages - I appreciate 313 relates to telecommunications providers, so is that a main advantage over Schedule 1 for you for a wider group of DCPs?

MR BUTLER: I think it probably would be the main advantage - yes, the wider group of DCPs is probably the main advantage. I would say that being excluded from TOLA would also send a message to carriers that perhaps government - there's a legislative message that that type of assistance that would be sought under TOLA perhaps should not be provided to agencies that aren't included in that legislation. So I suspect - we haven't tested it, but I'd suspect that would be a fair point of view put back to us by carriers if we sought a similar action like a TAR under 313.

DR RENWICK: Yes Ms Dubois, did I understand you correctly in your opening where you said that sometimes you are not permitted to stay in meetings where TOLA information is discussed, did I understand that, did you say that?

MS DUBOIS: We don't actually have the legislation yet, but that would be our concern, that we'd be exempted from those meetings and any advances in the legislation. That's my understanding.

DR RENWICK: So looking ahead for example, say there's a Federal ICAC. One could imagine a case where you might have a joint investigation with the New South Wales ICAC. That's possible, isn't it?

MS DUBOIS: Yes it is.

DR RENWICK: And if that were so, that would be a reason why you wouldn't want to have an artificial barrier which would prevent you - if you were doing a joint investigation, from talking to each other?

MS DUBOIS: Certainly, you know, if we lack the powers and it was someone in New South Wales, we couldn't apply for it. And similarly, if the Federal ICAC could, then we would be at a disadvantage.

DR RENWICK: Yes, Mr Mooney?

MR MOONEY: Mr Butler, just returning to the case study that Dr Renwick was discussing with you earlier, can you just say whether - notwithstanding

the difficulty you with whether Facebook cooperated in taking down the offensive posts, or was that not something you - - -

MR BUTLER: Look, I might take that on notice, Mr Mooney, I believe they did, but I might take that on notice and inquire.

MR MOONEY: And just finally on that case study, notwithstanding the fact that you weren't able to deal with it in the way that you had hoped, was any action taken against those police officers?

MR BUTLER: So generally - yes, and it's - most of our investigations we will advise New South Wales Police of any outcomes, and the New South Wales Police are then able to take or consider disciplinary action - or even consider the suitability of employment.

MR MOONEY: So some action was taken?

MR BUTLER: I don't recall off the top of my head the action taken by the police force, but I can find that out and advise. I would expect that they would've taken disciplinary action.

DR RENWICK: Well unless there's anything further that either of you would like to say - - -

MS DUBOIS: No, I'd just like to thank you for your time today in considering our submissions.

DR RENWICK: Yes, and so I'm hoping that the PJCIS are actually live streaming, but if they're not, I'll send them a copy of my opening remarks, and then it's out of my hands. But then of course I'll be able to say things in my final report, but I think we might just pause there. From 11 o'clock we have first the Human Rights Commission, and then we have Internet Australia before we break at 12.15 for lunch, so thank you very much and we'll just pause the transmission there.

MS DUBOIS: Thank you.

MR BUTLER: Thank you.

ADJOURNED **[1017]**

DR RENWICK**:** Ladies and gentlemen, welcome back to the public hearings on the TOLA Act, being held in Canberra. I'm delighted to

welcome to the mid-morning session, two representatives of the Australian Human Rights Commission, who I invite to introduce themselves and to make any opening remarks they wish.

#SESSION 2: Australian Human Rights Commission.

MR HOWELL**:** First, thank you for the opportunity to appear today. Increasingly, we communicate electronically. The provisions that are under review in the present review created new powers for law enforcement, security and intelligence agencies, to access electronic communications, as well as information contained in items of technology that are used to communicate.

Private communications should, absent compelling circumstances, remain private. This general rule is absolutely central to a liberal democracy like Australia, regardless of whether a conversation or some other transfer of information is in person, or by phone, by text message, or by some other electronic means.

Devices that we use to communicate, such as computers and mobile phones, also contain or may allow direct access to, a wealth of personal information, beyond interpersonal communications. Encryption is now a vital tool to allow privacy and private life to survive in the digital age. By allowing for decryption of text messages, telephone communications and access to computer files, the industry assistance powers necessarily intrude on the rights of privacy, freedom of expression, and other human rights.

These rights are not absolute. In some circumstances, they may be subject to legitimate limitation, however, for that to be so, the measures limiting rights must be prescribed by laws which must be detailed enough to confine them within predictable and justifiable bounds; they must serve a pressing, legitimate purpose; they must be necessary, for instance, they must not duplicate existing measures; and they must be the least rights-limiting measures available to meet their permissible objectives; they must also be proportionate. Any limitation on human rights must be weighed against the urgency of the objective.

In our written submission to the review, the Commission has expressed its view that the powers which are under consideration do not, in certain respects, satisfy all of these requirements. We have identified five key concerns relating to:

1. The lack of a requirement for judicial authorisation for the industry

assistance powers;
2. The scope of the prohibition on creating systemic weaknesses and vulnerabilities;
3. The relevant objectives for which the industry assistance powers may be used;
4. The breadth of the mandatory assistance powers introduced by Schedule 5 of the *Telecommunications and Other Legislation Amendment Assistance and Access Act 2018*, which we may refer to from here on in as the TOLA Act, if that's acceptable?

DR RENWICK: Yes.

MR HOWELL:

5. And the breadth of the concealment of access powers introduced by Schedules 2 and 5 of that Act.

We welcome the present review. Intelligence and law enforcement agencies play a vital role in protecting Australians; it is vital, however, that the powers they exercise in pursuit of that goal are appropriately drafted and contain robust safeguards to ensure they do not unnecessarily limit human rights. In particular, the Commission urges the review to scrutinise closely any claims advanced on the basis that the classified security material, which is said to support the continuance of the provisions in their present form.

We would welcome any questions you may have.

DR RENWICK: Thank you very much. And I should've said that I regard, as I always do, the Human Rights Commission's involvement in my reviews as central to the review, and I very much appreciate you being here.

Let me start with a philosophical question, using an example I gave to the head of ASIO before the break. If I have a paper diary and that's seized under warrant, I know what's in it: I've written it. Fingerprints, DNA, but that's about it. If I have my mobile phone seized, the starting point is, I do not fully know - and it may be unknowable - what that says about me; sure, I know the content, or I can find out the context of texts and emails, web searches, photos and so on.

But because designated communications providers monetise my personal information - and yes, I click "yes" or I agree to all of that. And pausing there, I note the ACCC are looking at the question of informed consent. It just seems to me at the minute that that is something which has, for people who say, "Look, nothing much has changed in recent years," a vast amount

has changed because of the unknowable aspect of technology.

And while, in a commercial context, it may be acceptable for me to click, "I agree" - because after all in theory, I don't have to click, "I agree" - when you're talking about compulsory access by law enforcement, particularly if it's not with your knowledge - and many of the TOLA powers will be done without one's knowledge - that creates a new element which requires perhaps a new or heightened approach to scrutiny.

I mean, in broad terms, would you agree with that?

MR HOWELL: Yes, we certainly would. I think there are two considerations for us, and one is the technical/practical consideration you've referred to, which is simply the amount of personal information which may, for example, be stored on a mobile phone.

But to me as a lay person, I'm constantly surprised to hear about how much further can actually be inferred or induced by either analysis of that data, or by comparison of that data with other datasets. And that does mean that access to that pool of information can now be extraordinarily privacy-intrusive, in a way that wasn't technically feasible perhaps 10 or 20 years ago.

The second I think part of our thinking is that in practice, a request to remove, or a direction or a notice to remove encryption for example, which would allow the removal of encryption, may not be limited to a particular communication, for example, a content of one text message exchange, or one telephone call.

DR RENWICK: No.

MR HOWELL: It may be, for example, a measure which allows for, I think as your monitor has referred to, a mobile telecommunication device to be accessed, opened, and all of the information therefore be made accessible. And what that I think demonstrates is that in deciding whether it is appropriate to allow for encryption to be mandated under the particular provisions we have through this TOLA provision, it's important to be aware of all of the privacy consequences that may flow; that goes beyond, probably, reading one particular communication or a chain of communications, which may be relevant to a particular set of intelligence inquiries or law enforcement inquiries.

DR RENWICK: So, thank you. Just to unpick that, perhaps you could look at section 317JC of the TOLA Act, which is on page 34 of my reprint? And what that sets out, in terms which you can also find for TANs and TCNs, is

what the decision-maker must have regard to when making a decision, because they're not able to request or issue a notice which is not reasonable or proportionate.

And just to reprise again what I asked the head of ASIO a little earlier; I asked him to look at subsection (h):

> *The legitimate expectations of the Australian community relating to privacy and cyber security.*

Now, at the minute, we just have the words of the statute, and as lawyers, I suppose we sit down, we look at the explanatory materials and so on, and we try and work out what they mean. There haven't yet been any court cases about all of this, and it's of the nature of these things that you know, court cases might not come along for quite a while, actually.

But it occurs to me that there should be some greater explanation about what those expectations might be, because it's almost certain that they have changed over time. To give an example, as we find out over time that some of the big companies are using our information in ways we might not have appreciated, even though we may have clicked "yes", that may have an impact on the legitimate expectations of the Australian community relating to privacy.

But we have those rather bland words and we know no more. So I take it, you know, in-principle, you would be in favour of some greater explanation, perhaps by way of example, about what that might mean?

MR HOWELL: I think we would certainly agree that some greater clarity around the meaning of that phrase would be useful. I think I might make two further remarks.

DR RENWICK: Yes, sure.

MR HOWELL: Which I think show, and unpack a little bit, what I understand lies behind your question; one of those is the question of how well-informed are the expectations of the community.

DR RENWICK: Yes.

MR HOWELL: And you've alluded to the fact that it is often very difficult for somebody who is a non-technically qualified user of modern communications services to really have a good understanding about how the use of those services may impact on their privacy. And that really raises

the question of whether the expectations of the community are the best yardstick in a legislative context such as this.

I think for us, as the Australian Human Rights Commission, the more important consideration obviously that it is vital to protect human rights, including the human right to privacy; and that will not necessarily be coincident with the way agencies interpret the legitimate expectations of the community about privacy.

Now, I'd like to just refer to a document I cited the other day, which is relevant, which is some guidance which has been issued by the Department of Home Affairs.

DR RENWICK: Yes.

MR HOWELL: And it does actually discuss how the phrase "legitimate expectations" may be interpreted. And it says that factors that may be relevant include for example, in some cases, opinion polling or media coverage. Now, from a human rights lawyer's point of view, those are matters that are very unlikely to have any relevance to the question of the scope of the right to privacy protected in international covenants, civil and political rights.

They may, however, either in fact, inform what the legitimate expectations of the community are, or how that phrase is interpreted by the agencies which are applying the powers introduced through the TOLA Act, which shows that the considerations which are currently being taken into account in the exercise of these powers don't fully line-up with the requirements of human rights law.

DR RENWICK: Yes. And is it a corollary of that also, that the Human Rights Commission would like to see an independent decision-maker deciding whether to issue say, TANs and TCNs, rather than an agency head or a minister?

MR HOWELL: That would certainly address the concern about whose idea of what expectations are legitimate, giving the community some comfort in knowing that an independent mind was brought to bear on that particular question. Of course, the mandatory considerations for that independent person to consider are also vitally important.

DR RENWICK: While we're on 317JC, I think you touched on the proportionality in relation to people who aren't subjects of interest. So I suppose subsections (e) and (f) are very important:

(e) the availability of other means to achieve the objectives of the request;

(f) whether the request, when compared to other forms of industry assistance known to the - - -

Person issuing it - - -

- - - is the least intrusive form of industry assistance.

Concerning the people who aren't, effectively, the subjects. So that is, in-principle, a good factor to take into account, you'd agree?

MR HOWELL: Absolutely, yes.

DR RENWICK: But again, I think you'd agree wouldn't you, that from a community expectation point of view, there's a lot to be said for that being issued by someone independent from the executive government?

MR HOWELL: Again, I think having these orders issued by somebody independent is a vital safeguard in many respects with this regime. I would make one, again, further short remark, based on international human rights law, which is that from the perspective of international human rights law, the existence of alternative, less intrusive means to achieve an objective is very relevant. But it is, in fact, a mandatory consideration, not simply one factor, to which regard must be had by a decision-maker.

And so there is, again, a point of difference between the requirements of human rights law and this particular provision.

DR RENWICK: Yes, it is a notable thing isn't it, in 317JC, there's a lot of factors; they may all point in different directions, or at least be intentioned with each other, and there is no hierarchy as to which is the most important and which is the least important.

MR HOWELL: Indeed. And it may well be the case that all of those are relevant factors; from our perspective, some of those factors will have more weight than others, in almost all circumstances.

DR RENWICK: All right. So can I ask you then, if you look at your submission at paragraph 17, you say:

Overall, the TOLA Act created broad new powers to enable government agencies to gain access to information that would otherwise remain private, for example, by virtue of encryption.

So one of the things you will have noticed from my opening is my scepticism with the idea - not put forward by the Human Rights Commission - that in effect, TOLA is just making intelligible what's already been authorised by warrant, and therefore, you do not need to have the same level of independent oversight for TOLA as you do for the original warrant.

And I take it, again speaking generally, if you have an existing level of oversight for the underlying warrant for example, in-principle, that ought to apply to TOLA because that is what may make unintelligible content, intelligible, and it's the intelligibility of that which particularly impacts on privacy.

MR HOWELL: I think it's certainly the case that we would say that simply because a warrant is in existence, and it may be justified that a warrant has been issued to intercept certain communications, that doesn't mean it automatically flows that all of the encryption and decryption powers potentially available under the TOLA regime should automatically be available without some further equivalently independent decision being made about whether it's appropriate in the circumstances, that's right.

Which I think is a long-winded way or saying, we agree with you.

DR RENWICK: Yes, thank you for that. So can I just tease-out some of my thinking, tentative thinking, about oversight, relating to your first point: there is no requirement for judicial authorisation. Now, AAT authorisation, I accept, is not judicial in the traditional sense. But may I suggest there are some problems with judicial authorisation which can be overcome if you had independent tribunal members?

And they include the following, I think: there are sometimes concerns about the Constitutional validity of persona designata provisions in relation to judges. Secondly, there is a policy argument that it's a distraction from judicial duties. Another point is this, I think - and this is a point which has been made, I think in some of the current media campaigns - that sometimes, the judicial officer who is authorising things is actually a very junior judicial officer; they may technically be a judge, but they're really a deputy registrar.

And I take it in-principle, the Human Rights Commission would want a more senior and experienced lawyer exercising these intrusive powers, if there is a choice in the matter?

MR HOWELL: I think for us, the two really important criteria that must be met for a decision-maker to be well qualified are that they be independent, and seen to be independent. And one reason why either judges or retired judges are seen to appropriate decision-makers is that they are trained in independence, they often either have tenure or they no longer require ongoing employment from the government; that guarantees independence. But also, they're well-practised in making the right kinds of decisions involving independence, withstanding scrutiny on that basis.

So the guarantee of independence and the perception of independence is crucial. And there is also the question of who is technically well-qualified to make good decisions? And again, judges and former judges or superior courts are uniquely well-qualified to make the kinds of decisions that would be made under the regime that's currently under review.

So certainly, we would say that a regime that avoids very junior officers making relevant decisions would be a better regime. In terms of whether a model involving the AAT directly in one of its jurisdictions, or people who are members of the AAT, would be a good model, we would need to consider the detail a bit more closely.

DR RENWICK: Sure.

MR HOWELL: We do note that the qualifications for ordinary members of the AAT are very different from the type of qualifications one would need to be a judge or former judge of a superior court in an Australian jurisdiction. We also note that AAT members don't, for example, at least in general, have tenure.

DR RENWICK: No.

MR HOWELL: So they are in a different position. But those factors may be able to be addressed by appropriately crafted legislation; we would have to see drafting and see if we thought that it passed muster.

DR RENWICK: So to unpick some of those, you'd want to see in-principle, the same qualifications as for a superior court judge, which is normally seven years' experience, or more, as a lawyer; that would be one of those. There may be you need some tenure, but the AAT members just don't have as long tenure as judges, so that's intrinsically a problem.

Can I raise this, though? One of the things I found impressive in the IPCO model in the UK, firstly, there are incredibly senior and impressive judges: I mean, Lord Hodges, a former member of the UK Supreme Court, so you've got the most senior judges possible, retired judges. And the second thing which was striking was that there is the opportunity to specialise about the relevant agencies. And thirdly, they've got technical assistance.

So when I look at the Telecommunications Interception Annual Report, recently published in the parliament, what is striking to me is how many different judicial officers are issuing warrants; a small number from the Federal Court, a larger number from the Family Court, a really large number from the Federal Circuit Court and the AAT.

None of them have technical advisers. And in this area, one of the things which concerns me as a simple lawyer is, how do you really understand the full impact of something unless you at least have access to - not bound by it - but access to, a really well-qualified technical person in whatever discipline may be appropriate, to say, "Actually, that's very intrusive"? Or, to put it another way, "There's a much less intrusive way of doing this, which can focus on the person of interest."

So just on that, would you agree generally it is desirable for the independent decision-maker, if you're going to have one, to have access to a really able technical adviser? Whether they're a co-member of the AAT, or whether they're a technical expert seconded.

MR HOWELL: Well, I think we might frame things at a slightly higher level of generality, and say that from our point of view, to protect human rights in this context, it's vital that the qualified and independent decision-maker turn their mind to the substance of the matter that is before them. This is one query we have about how an IPCO model might work.

DR RENWICK: Yes.

MR HOWELL: If the words of the statute were imported into Australia, which provides for a judicial review standard of a decision, rather than the substantive decision. We're aware that legislation, judicial review, in the United Kingdom works differently than it does in Australia.

DR RENWICK: Yes.

MR HOWELL: We won't go into the sort of details about those differences, but the question is, within the Australian context, we need a model where the substance of the issues that are relevant to making a decision is investigated and decided upon by the decision-maker. And that decision

needs to be well-informed, which means that the relevant technical information needs to be before them, and they need to be able to meaningfully interrogate it.

It seems to me, speaking generally, that one way that might be facilitated is by having a decision-making model involving perhaps, multiple decision-makers, one with judicial qualifications, and one or more with technical qualifications. One could conceive of different models, for example, contested decision-making models, where parties might be able to either nominate or appoint their own experts to an arbitration panel, or call expert evidence.

So there are a number of ways that the objective could be achieved.

DR RENWICK: Yes.

MR HOWELL: But it is important that that information be available to the decision maker and, as I say, they can interrogate it.

DR RENWICK: Another strength, as IPCO sees it, of its model, is that of the 15 or 16 retired judges, three or four as a group tend to specialise in particular agencies; you might have the MI5 specialists, the GCHQ specialists and so on.

And again, it seems to me there are arguments each way. On the one hand, there's always the fear that if you have a very small number of decision-makers, they get, in theory, captured, or there is the perception of that. On the other hand, if there are detailed technical matters to understand, it's desirable that someone says, "Oh yes, well look, we've been through this before. I do understand that's the way you do business, and my technical adviser has explained it to me."

So you'd agree, broadly, that those are the sorts of factors you'd have to weigh-up?

MR HOWELL: Those both are certainly very relevant factors. I can't say I have the perfect answer to achieve the perfect balance between those considerations.

DR RENWICK: No, all right then. So can I turn then to the vexed question of systemic weakness, which one finds for example in 317ZG? And the definitions, of course, are in the definitions section. So you've got the definition sections, which define "systemic weakness" in 317B, and then you've got some explanations in 317 ZG of what is or isn't out.

So the first sort of general point is, do you agree with me that in-principle, it would be desirable in the statute, as opposed to in a revised explanatory memorandum say, to have statutory examples, non-exhaustive, or what is or isn't a systemic weakness or vulnerability, so that a judge deciding which side of the line you fall on has a bit more guidance?

MR HOWELL: These are certainly the key concepts in how these provisions will operate and how widespread their impact will be on persons who are not directly being investigated by relevant agencies.

DR RENWICK: Sure.

MR HOWELL: We certainly think that more clarity is needed about exactly what these concepts mean, and it seems to me that one way to help achieve that would be by having examples given in the statute itself; and that is more important than statements in an explanatory memorandum, or in administrative guidance given by a relevant agency.

In this field, I must say, I'm still surprised by how frequently references are made to secondary material such as explanatory memoranda, as though those actually control the meaning of the statute. But it is quite rare that you will see a court referring to an explanatory memorandum to resolve a dispute about the meanings of a statute, and it's important that the statute itself be clear.

DR RENWICK: Yes. And I mean, if one wanted an example, you know, there's the famous case of *Re Bolton; Ex Parte Beane* [1987] HCA 12, 162 CLR 514, where someone tried to say that the examples in the explanatory memorandum controlled the statute and the High Court had no time for that. So, yes, I think we're in agreement that statutory examples are in-principle.

Now, the next question of course is what should they be? Does the Human Rights Commission have any particular preferred wording or changes you propose, or do you rather say, "Well, here are the principles." How those principles are to be applied is not something you wish to delve into?

MR HOWELL: We do take a principled approach. We consider that we're in general not well-placed to undertake exercises in statutory drafting. In this particular case, we have recommended that there be a comprehensive review, hearing relevant evidence from technical experts as well as people within the agencies that would be seeking to rely on these powers. It seems there are technical questions about what types of measures might, in fact, end up allowing for intrusions on the privacy of third parties, and to what extent they would.

So, because we're not well-placed to assess all of those issues, we rely on the general statements that the definitions need to be crafted in such a way to protect against agencies being able to access communications which pertain to innocent persons, and which will weaken encryption when third parties are attempting to perhaps maliciously obtain the private information of members of the community.

DR RENWICK: All right, thank you. Can I ask you to turn to paragraph 45 of your submission, and 46? So here, to give an example, just to read out 45:

> *There's a risk of digital surveillance powers being used to monitors persons inappropriately on the basis of race, religion or political opinions. Also concerning is the potential for targeting of journalists, whistle-blowers, opposition politicians, human rights defenders and persons engaging in lawful public dissent. Children's rights may also be affected by the use of coercive powers on underage providers or to compel a minor to give access to a device, and they are matters which merit further consideration.*

So is there anything particular in TOLA that causes you concern or does it relate more to the inadequacy, as you see it, of the oversight functions, who makes the decisions, and so on?

MR HOWELL: The concerns we're expressing here are I suppose two-fold. Mostly it is a general concern that all intrusive surveillance powers can be used in, for example, discriminatory ways, but can also have wide or perhaps unforeseen human rights implications. It's true that having independent oversight of how the provisions are used, so oversight by a body such as the IGIS and having a suitably independent and informed decision maker are two powerful protections.

It is also vital that legislative regimes be crafted in such a way that decision makers have to turn their minds to the question of which human rights may be involved when they're making a decision and ensure that they take the least rights-intrusive steps possible to achieve objectives and if the impact on those human rights, including rights that we may not have thought of, but go beyond the right to privacy for example, that a decision maker consider whether those rights have impacted how much and if perhaps that impact outweighs the need or the proposed justification for the measure.

DR RENWICK: I mean, just on the IGIS, I like many have the highest respect for the current IGIS and for the work that they do, but it's important not to put too much on them. I mean, they have nothing to do with prior

consent, so they don't look at – it's not as if ASIO says, "We're thinking of issuing this warrant, do you consent or not", that's not their role.

Although the current distinguished incumbent happens to be a retired judge, it's not a judicial body, and that's not always understood, I think, by overseas people.

There are some particular examples, so there is a particular provision which says nothing in Schedule 1 interferes with parliamentary privilege. So that is at least some protection of the rights of parliamentarians. But let's take the rights of children and the familiar provision that the rights of children must be a primary consideration, that's an international obligation. How might that be best vindicated? I mean, is that by having a precondition in the statute that if it's going to directly affect a child, perhaps there's a higher standard reflecting that, or a different person making the decision.

Have you got – I mean, you made submissions to me in my children's inquiry about the broad principles involved. You may want to take this on notice, but I'm just trying to come up – and I'm very sympathetic to the importance of the rights of children – but just how might that manifest itself in a statute of apparently general application? I mean, it's not facially discriminatory, to use the American terminology, but equally, it can obviously apply to children.

MR HOWELL: It's certainly the case that children are particularly vulnerable to limitations of their human rights; they're not well-placed to take steps to protect their own rights, and they may not even be legally empowered to take those steps in some circumstances. The effects of intrusions on their rights can also be particularly severe.

In terms of the best mechanism to ensure that children's rights are protected, there are a variety of measures of course that can be taken. In the broadest scheme of things, in a jurisdiction which has a Human Rights Act, administrative decision makers are routinely required in every decision they make to consider relevant human rights, including the right of the child to have the best interests be a primary consideration.

In the absence of that, a requirement that a decision maker when considering an application to exercise a power such as these industry assistance powers that may particularly affect children, there may be a provision that they apply a higher criteria or they apply special criteria, including for example simply ensuring that the best interests of the child are a primary consideration for them in making their decision.

If any sort of more detailed thoughts occur to us in the coming days, we might send something through. I can't concretely promise that we will find a perfect solution to that issue though.

DR RENWICK: No, but it is something, just looking at that, where I don't think I've particularly concentrated so far on, you know, how they TOLA powers might be used directly against children. I can see how you might ask a social media provider for information which impacts on rights generally, including those of children, but at least some of the more direct powers could be used directly against children.

I suspect, for example in the Crimes Act, the provisions with – yes, the assistance orders, for example. But I suspect the Crimes Act provisions for police constables and what they can do, there are special provisions for children already. But there may be something to be said for widening that across the schedules to ensure there's common protections.

MR HOWELL: Well, that certainly sounds consistent with the need to take measures to protect children's rights.

DR RENWICK: When you talk about adequacy of judicial review, so as we all know, there's constitutionally protected capacity to judicially review decisions; that's very different from merits review, it's very different from an appeal; and in particular when the information the decision maker acts on may be protected by public interest immunity, it may be extremely difficult to challenge a decision.

So did you want to make any more comments about the adequacy of judicial review say for Schedule 1 powers?

MR HOWELL: One further consideration that has occurred to me in recent days relates to the way in which the factors most relevant to our thinking about human rights protections are protected in the legislation. So for example, the need to ensure that certain measures are reasonable and proportionate and necessary and so on, are no strict criteria for the validity of a decision. Rather, the relevant criterion is the state of satisfaction of an executive decision maker.

It is notoriously difficult to challenge the state of satisfaction of the decision maker under judicial review, even absent considerations such as information not being available due to public interest immunity. It really relies in showing that no reasonable decision maker could have rationally arrived at a state of satisfaction, which is a much higher threshold than establishing that the measure itself was not proportionate or necessary.

So it seems to me difficult to envisage mean circumstances in which it would be possible to, given all of the impediments, successfully rely on judicial review to challenge a decision, unless there was a simple case of ultra vires for example.

We say that it's important both that there be an independent and well informed and well qualified decision maker before these powers are issued, but that there also be meaningful opportunities to interrogate and challenge that decision. That's why we have recommended that perhaps ADJR review might be appropriate and/or merits review might be appropriate.

Of course one can imagine the multitude of decision making models where there might be a contested hearing at first instance and the ability to give a nominated decision maker or call expert evidence. If that type of decision making were involved, or the criterion for the issuing of an order were changed, the type of review that might be required to protect human rights might change as well.

As things stand, we would say that a review mechanism that allows for greater interrogation of the substantive facts at issue would be very beneficial to better protect human rights.

DR RENWICK: Let me just make a – ask a more general question about review of the Act itself. It's quite often the case in the laws I review, which are usually counter-terrorism or national security specific, this of course is much broader than that, that there's either a sunset clause or there is a requirement for the PJCIS to review the law every three or five years.

Would you agree that that's particularly apt here, not least because technology changes so fast that what appears to be technologically neutral may in fact bear quite a different complexion, say if artificial intelligence is used more or there's some new technological breakthrough which we simply can't predict at the minute?

MR HOWELL: The pace of technological change is certainly a factor which means that it would be worthwhile revisiting these provisions to see if they're operating as intended. That's both to see if they're achieving the objectives they're supposed to be achieving, but also to see if they're affecting human rights to a greater extent than anticipated.

Another factor I think that would support review of the provisions after there is some experience of their operation, assuming they do remain on the books in the meantime, is that there is some uncertainty about how some of the key provisions will operate in practice.

DR RENWICK: Yes.

MR HOWELL: You've referred to the meaning of the phrase "legitimate expectations of the community surrounding privacy", you've also referred to the definitions of a systemic weakness or a systemic vulnerability, and I think that experience may throw some light on are those provisions operating in a way that we say is problematic from a human rights point of view, or are they operating, have they've been interpreted in a way that is reasonably protective of those human rights principles.

DR RENWICK: Certainly I can assure everyone here that I am very interested in as much as possible being revealed publicly and regularly about the use of these powers, and I noted earlier this morning that in fact there is greater capacity than perhaps had been or generally realised for the DCPs to say, for example, "We've never received such a request", or "We've received one in the last six months", not revealing who it's from, or nothing wrong with saying, "We never would do this unless we were forced to do it and we would fight it all the way". So those are some protections, but no doubt others can be built in.

Mark, did you have a question?

MR MOONEY: Yes, just in relation to your submission, you say that overall the TOLA Act has created new powers that enable government agencies to gain access to information that would otherwise remain private, for example by virtue of encryption. Given that, is it your position that a person's right to privacy, including through encryption, extends to a situation in respect of which there is a warrant in force authorising access to that person's devices or communications?

MR HOWELL: Well, I suppose from a human rights point of view, we would say that there's a two stage analysis. The right to privacy does pertain, all people enjoy the right to privacy at all times.

MR MOONEY: Yes.

MR HOWELL: The right to privacy may also be subject in some circumstances to legitimate limitations, and that will depend on whether that is necessary to achieve a pressing legitimate objective. In circumstances where it – after assuming a proper human rights analysis and privacy impact has been conducted – has been considered appropriate to grant a warrant to allow the accessing of a communication, then it will quite possibly be appropriate for the subject privacy to be, to that extent, limited with respect to the information captured by that warrant.

MR MOONEY: Yes. So in that sense the powers are broad in the sense that they allow a greater scope to access those encrypted communications, but they're not more powerful in the sense that they're still limited by all of those factors that you've just highlighted.

MR HOWELL: Well, correct me if I haven't understood fully the import of your question. It seems to me that the powers in Schedule 1 of the TOLA Act are not strictly only available in circumstances where a warrant has been issued, and that where powers are used in the circumstances of a warrant, they may nevertheless allow for privacy impacts that go beyond the privacy impact occasioned by reading, understanding, accessing a particular target communication, because they may allow for other personal information of a target to be read, they may weaken protections for a broader group of people and allow their privacy to be impacted.

So I wouldn't say that the privacy impacts are co-extensive that flow from a warrant or flow from the issuing of a request to a notice under Schedule 1 of the TOLA Act. But there will be some overlap between the privacy impact, and to the extent there's an overlap, the privacy impact of mandatory decryption may well be justified.

It's not the Commission's position that agencies should never be able to access encrypted communications.

MR MOONEY: Yes. So you'd reject the notion that the risk that we'd create a two-tier system where those people who have access to encrypted communication would be less susceptible to investigations in circumstances where they are a person of interest, than people who don't have access to encrypted communication?

MR HOWELL: I don't think that we would accept the characterisation of that as a two-tier system; we would say that some people have taken steps to ensure that their information remains private, and that that has consequences for how easy it is for anybody, including agencies, to access the content of those communications. That may mean that new powers are needed, but those powers will have to be subject to controls to ensure that the privacy impacts occasioned by their use don't go beyond what it needed.

I don't think I would describe as two-tiered a system which required different types of warrants to access different types of communications, for example that's the case now, the criteria that has to be met to get different type of warrant under the Surveillance Devices Act or the Crimes Act or Telecommunications (Interception and Access) Act, they're not all the same. That doesn't necessarily mean it's a two-tiered system, it might

simply mean that certain types of powers warrant certain types of factors to be subject to particular consideration.

MR MOONEY: Yes.

DR RENWICK: Just one thing to finish with, Mr Howell, for me, and if the – sorry, one thing to finish with from me, and if Home Affairs is listening to the live stream, I intend to ask them this tomorrow, just getting back to the rights of the child, and if you did have the time to do something very brief on this. I simply note that the power – the search warrant power under section 3LA of the Crimes Act, which was inserted by Schedule 3 of TOLA, amended by TOLA, talks about a constable applying to a magistrate for an order, for example telling someone to unlock their mobile phone, I'm conscious that in the Commonwealth *Crimes Act 1914* there are special provisions whereby a magistrate may order the carrying out of certain forensic procedures on a child or incapable person, for example 23XWU.

I suppose my question specifically is in relation to the police powers, amended by Schedule 3 of TOLA, and the Border Force powers, amended by Schedule 4 of TOLA, does the Human Rights Commission want to see specific protections for children who might be the subject of those compulsory powers at the border, for customs or, more generally, from the police, and the ASIO powers of course equally in Schedule 5?

Because at the minute, and I stand to be corrected on this, there doesn't seem to be a differential regime for children, rather, it's a reference to "a person". So presumably, because there's a criminal sanction, it wouldn't apply to anyone under 10, and there would be *doli incapax* between 11 and 14. But even so, that means everyone between 11 and 17 is liable to this, presumably a magistrate would, as a practical matter, take into account the fact it was a child.

But I just wonder whether something should be made more explicit about it, and you may have a provision in another Act which you say is a good model to think about using. Can I ask you to take that on board please?

MR HOWELL: Yes, thank you, we'll have a close look at those provisions and send in something in writing.

DR RENWICK: Unless there's anything further, which I don't think there is from my team, unless there's anything further from you, may I thank you again. Please pass on my thanks to head office as well, if I can put it that way, and we look forward to hearing further from you. Thank you so much.

MR HOWELL: Thank you.

DR RENWICK: I invite the Internet Australia representatives to come forward. I now welcome three representatives from Internet Australia: Mr Paul Brooks, who chairs Internet Australia and who is a founding member, indeed, of it and on the board of a number of organisations; the chair of the Policy Committee Internet of Internet Australia, Ms Holly Raiche, who also teaches at the University of New South Wales; and Mr Keith Besgrove, who is the Vice Chair of Internet Australia, who has extensive experience in the field.

#SESSION 2: Internet Australia

May I welcome you all, very much, and invite you to make any opening statement you wish.

MR BROOKS: Thank you, Dr Renwick, for your invitation to expand on our submission and answer your questions regarding our concerns about the TOLA legislation, in particular about Schedule 1. We in the internet society represent the concerns of the global internet technical community, the bodies of engineers, data scientists, application designers, infrastructure and software builders around the world who are appalled at the risks and dangers of real economic and personal harm that are enabled by this legislation, by its overly broad reach, its vague or missing definitions, and its inadequate safeguards.

Confidential and trusted communications secured through end-to-end encryption are essential for the ongoing safety, security and efficient use of global networks for business, for government and for personal interactions. The internet technical community has spent decades introducing strong encryption and authentication methods into the very fabric of the networks and the applications that run over it, such as web browsers and email systems and messaging applications to ensure that sensitive data, such as banking details, medical records and trade secrets can be transferred without being eavesdropped, and we continue to strengthen the global infrastructure to ensure that communications remain secure, even over public, insecure networks.

If not used extremely carefully, the TOLA Act has the potential to undermine the trust and weaken the security of Australians and the rest of the global community by enabling agencies to weaken systems, introduce deliberate vulnerabilities and undermine security measures. There is no digital lock that only good guys can open but the bad guys can't.

Once lawful access back doors or vulnerabilities are created, knowledge of those vulnerabilities is at risk of leaking and, once leaked, they're at risk of being discovered by criminals and other governments and being replicated. Once knowledge of lawful access capabilities created using the powers provided under a TCN or a TAN escapes, it will make it easier for others, including criminals and hostile governments, to gain access to sensitive data stores on the same types of devices and systems worldwide.

The consensus among information security experts is that exceptional access mechanisms always add more complexity to systems, leading to vulnerabilities, especially if they're required to be created in haste. These vulnerabilities can create points of entry that anyone can discover, possibly years later.

Many major systemic vulnerabilities have been created by accident through software bugs and haven't been recognised or discovered as such until years later, by which time that vulnerability has often spread through a significant proportion of the global infrastructure, and experience is it takes decades to fix, if indeed it ever gets fixed entirely.

The impact of a leaked vulnerability is not limited to Australia. In an increasingly globalised supply chain the same make and model devices supplied in Australia are often also supplied globally. If the Australian Government requests or requires a provider to make changes and install a vulnerability into a system, it's then open – or even a single device, it's then open to every government around the globe to request the same capability in their jurisdiction, including jurisdictions where that same capability would harm the security of Australian citizens and corporations living and transacting business there.

There's nothing in the TOLA legislation that restricts the introduced vulnerability or back door to only be required within Australia's borders, only the word "for use or likely to be used in Australia". Each foreign jurisdiction may take slightly different approaches and require different capabilities, which a device that is then manufactured by a lawfully compliant organisation that tries to comply with those different requirements in all the different jurisdictions around the world.

As expressed by the global Internet Architecture Board, the concern is that that approach, if applied generally, would result in the internet's privacy and security being limited to the lowest common denominator permitted by the actions taken in the myriad of judicial context around the world. From that perspective, this approach of the TOLA Act drastically reduces trust in critical internet infrastructure and affects the long-term health and viability of the internet itself.

The ability to compel compromises to the mechanisms that provide security, privacy and trust on the internet, erodes the trust in the internet as a whole. That erosion, multiplied by the number of political and judicial contexts in which similar approaches might be adopted, represents an existential threat to the internet's security and integrity.

Without independent, qualified, unbiased experts that scrutinise and validate each notice or request, the well-meaning exercise of the powers embodied here has a very real risk of opening a Pandora's Box of harm that could reduce security for millions of people and businesses around the world that may take decades if ever to rectify. This has already occurred in the past, one example being the US Government's export restrictions of strong encryption and requiring only weak encryption to be exported to other nations.

Law enforcement agencies refer to encrypted communications as "going dark", but we note that law enforcement agencies are still able to have access to metadata about messaging patterns, even if they can't access the content. As we saw in the introduction of the metadata legislation in Australia, for many agencies the metadata is often more important than the contents of the communications itself.

The metadata can still reveal who a person is communicating with, their circles of acquaintances, the sizes of messages which goes to the form of content that it contains, the dates and times and frequency of messaging and other data that's valuable to law enforcement. These patterns and metadata about messaging behaviour are important in criminal investigations. So we believe it's misleading to refer to encrypted messaging as "going dark". At worst, it's going grey.

The reality is that these capabilities are not being used in many cases deliberately by the general population, they're being deliberately introduced by the system designers to happen by default for the safety and security of the general population.

We believe that the safeguards that are often talked about in this legislation are illusionary. The TOLA legislation was originally developed in secret, with no consultation or input from industry, and presented as a fait accompli and, as a result, includes technical definitions and terms such as "systemic weakness", "systemic vulnerability" – which actually appear to be the same thing and I'm not sure why it's duplicated – and the term "the class of technology", which is ambiguous, vague and subjective and doesn't actually mean anything to the technical audience of the organisations that

are required to implement the notices. They can be interpreted and argued to mean almost anything.

The legislation relies on these subjective terms for many of its protections. Many of the safeguards are illusionary because they rely on self-assessment and self-restraint on the part of the agency heads or the Attorney-General weighing up anything up to 11 different conflicting aspects, which will be challenging to do in an impartial manner, especially if time is so short that an oral notice is envisaged to be given because there's no time for a written notice.

Many of the other safeguards rely on the recipient of the notice or request lawyering up and pushing back, which large organisations may well do, but very small backyard shops that are creating a particular product or a small part of a service may not have the resources or the money or the nerve to push back on a large government law enforcement agency.

The legislation does include oversight by independent bodies, but this is of little practical protection in the heat of the moment, because there are significant time delays that preclude those bodies actively intervening in an inappropriate or a – use of powers. For example, there are several sections in the Act that requires agencies to notify the Commonwealth Ombudsman within seven days of any new issue or change to a notice of a TAR, a TAN or a TCN.

But the ombudsman in his submission to this inquiry identified their inspection is retrospective for their regular reporting. The notices are not assessed at the time that they're received. So if there are any irregularities with a notice or request, it won't be identified by the ombudsman until well after the conduct has occurred.

These are several reasons why we believe the safeguards considered as such and described as such by the Department of Home Affairs are actually illusionary and aren't actually real safeguards in the legislation at all.

We believe the legislation, particularly Schedule 1, is unworkable, at least as far as industry assistance measures, as far as compulsory changes to systems are concerned, and that set at least should be set aside in its entirety without band-aid amendments and a working group of government, industry and civil society of the providers that were required to respond to these notices, to get together and collaboratively work on words that are actually meaningful to lawyers and to engineers so that everyone can be confident that when a notice is issued it's issued for the right reasons, it doesn't overstep the boundaries, it is reviewed by competent independent people who can make a judgment on whether an inadvertent consequence

of this may be a significant amount of harm to the global community. Thank you.

DR RENWICK: Let me unpick some of those. So you were here I think this morning when Mr Burgess was here, and you heard him say that encryption is of benefit to society, so that at least is common ground I think.

MR BROOKS: Yes.

DR RENWICK: He also says that from his point of view he would never seek to create a backdoor.

MR BROOKS: Yes.

DR RENWICK: And I appreciate backdoor's a related term and we can come to it. So to that extent there's a measure of agreement about things.

MR BROOKS: Absolutely.

DR RENWICK: So perhaps, going back to my opening statement, there are perhaps three broad things to look at if – and I think this is more realistic – Schedule 1 is unlikely to be immediately repealed if we're - - -

MR BROOKS: I was referring just to the TCN portion.

DR RENWICK: Were you?

MR BROOKS: Yes.

DR RENWICK: I see, I'm sorry, thank you, that's very helpful.

MR BROOKS: An information request for learning how a system is put together for use for other purposes, that is unlikely to cause any damage. It's the ability to compel a system change that may have inadvertent consequences, that is where the danger lies.

DR RENWICK: Thank you. Well, I'll come to TCNs then directly. But in broad terms it seems to me there are three – as I mentioned in the opening, three categories of concern by groups such as yours. First is, as you say, there's definitional matters, the second is there are the question of who authorises, and the third is how to improve oversight mechanisms, just speaking very, very broadly for a minute, and let's just park TCNs to the side.

MR BROOKS: Sure.

DR RENWICK: Can I just ask you, just before we get into that, do you accept that not only content but also metadata is likely to become increasingly encrypted?

MR BROOKS: For the commercial systems that are often mentioned, in terms of criminals using systems such as WhatsApp, the current request by the agencies for Facebook not to introduce strong end-to-end encryption in its messaging systems, no, that metadata is always accessible by the service provider, if you like, and in fact is more secure because it gets handed from the operator of the service to an agency using effectively an authenticated mechanism. So we know that that information is very difficult to leak out for criminal elements, for cybercrime, organised criminals to be able to get access to that, because they would have to go to the operator of the network rather than sniffing the packets on the fly, as they go past.

So for most messaging systems that I've seen mentioned in despatches for terrorists and paedophiles, which are the two main classes of people that often get mentioned these laws are aimed at, they tend to be commercial messaging systems where the metadata is controlled by the service provider and isn't encrypted and is available to the service provider to give to an agency, notwithstanding international aspects such as whether the organisation is offshore or not.

If the criminal element is operating their own messaging system, then obviously that metadata is going to be difficult for law enforcement to access, if not for the reason that it's going to be difficult to service them with a notice in the first place.

DR RENWICK: What about the fact, as I mentioned in the opening, that the internet is already fragmented? You know, there – as we all know, there are quite different companies which operate in China, for example, because there's different rules there.

MR BROOKS: Yes.

DR RENWICK: To what extent is that information treated differently?

MR BROOKS: It's vulcanised to an extent. So yes, organisations and communications in some countries is often limited within those borders and then that's up for that country to do so. Our main concern is with Australian companies operating here and the impact of these laws in Australia. I'm not sure how these laws could be used to impact communications in China or in Russia, which are those two examples who tend to operate fairly restrictive border controls on data. But ultimately, all of these

communication systems rely on a common set of agreed protocols for communications, or two systems just can't work at all.

So to an extent there is common ground, it's really a case of at what level does access to certain sites and types of information get blocked completely. And that blocking of content or blocking of access isn't really something that is subject to these provisions.

DR RENWICK: Thank you. Well, then let me come to who authorises these matters. I take your point that when you look at the different factors which a decision maker has to take into account, I think we are both in agreement they pull in different directions.

MR BROOKS: Yes.

DR RENWICK: I've already debated with a couple of people about the legitimate expectations of cyber security, and you'd agree with me that that's not an easy concept to pin down and it probably changes over time. I see you're all nodding.

MR BROOKS: Yes. It changes over time but it also changes on your perspective. And our concern is that a person in an agency, at the head of an agency, has a job to do, has incentive to get the investigation going, the weight that they would place on those different criteria is likely to be different than the weight a man on the street would apply to those same criteria.

Your suggestion in your opening statements about that independent body of technical experts is absolutely along the lines that we were thinking of, it takes – both the inspection of whether the requirement is reasonable and whether it's necessary, takes it out of the hands of effectively a biased decision maker to an unbiased decision maker, to have some clear eyes, and that would absolutely be – we would welcome that.

DR RENWICK: So just to be clear, what I had in mind was an independent lawyer, Tribunal member, sitting with, as it were, an independent technical person.

MR BROOKS: Yes.

DR RENWICK: And that would be a desirable thing?

MR BROOKS: Absolutely. We believe the independent technical person or even potentially several people, depending on the nature of the request and the level of expertise required, is what is required to try and mitigate,

prevent the risk of unintended harm from something else that is not foreseen but turns out to become a vulnerability.

DR RENWICK: Thank you, that's very helpful. Well, can I - - -

MR BESGROVE: Excuse me - - -

DR RENWICK: Yes, Mr Besgrove.

MR BESGROVE: Can I just add to that? One of the reasons why we've been advocating the sort of additional changes that we have and why we're responding so positively to some of the things you put on the table this morning is we believe, given the unpredictability of some of the changes that have been introduced into communications systems in the past, which are sometimes created unwittingly, new vulnerabilities, it's prudent for the Australian Government to adopt a stronger risk management approach than is currently the case in the TOLA Act.

So we believe that there is a strong case for additional safety measures. We can't rule out unwitting changes, I mean – but we heard this morning from the Director-General of ASIO that he would never deliberately set out to create a systemic vulnerability. We would expect him to say that, nevertheless it's reassuring to hear him say that.

Our concern is that a legitimate invention by that organisation or another security or police organisation, specific to an individual communications device or a communications user, has the potential to unwittingly create unforeseen vulnerabilities. We can't make that not happen, but we can take measures to limit the likelihood. And the sorts of things that Dr Brooks is talking about are part of that risk management approach.

DR RENWICK: So you draw a clear distinction between the TCNs and the TANs. So broadly speaking, do I understand for a TAN, you're asking the DCP to do something they can already do? And to use a simple example – as opposed to a TCN. To use a simple example, you know, from a law enforcement point of view, something might be unintelligible, but Facebook or Google or whoever, in their hands it's intelligible.

MR BROOKS: Yes.

DR RENWICK: So that by itself, with proper safeguards, with an independent decision maker and so on, that is more palatable to you. But the TCNs, what you feel is this unintended consequence.

MR BROOKS: That's correct.

DR RENWICK: That's the key concern you've got.

MR BROOKS: That's the nub of it, yes.

DR RENWICK: All right. So just a couple of things there, you may have heard me put I think to one of the earlier witnesses that I think some DCPs said that they felt their whole business models were undermined because they tell the world that either we'll never create a back door or a law enforcement function, that's one example, or they wouldn't be able to say that they were required to assist.

Now, just to unpick that, as we read the provisions, there's nothing wrong, indeed you're able to say as a DCP, for example, we've never received any requests. So that's something, is it not?

MR BROOKS: It is, up until the point where they can no longer say that because they have received a request, and the issue goes to reputational risk, that at purchaser of those products and systems knows that according to the secrecy provisions in the Act the provider couldn't tell them what the nature of the request they received is, and even – so from a purchaser's perspective, there is a risk, whether there's been a notice issued or not, there's a risk that that supplier is subject to requirements to have made changes to the system that weakens it, relative to a product available from a different manufacturer from a different jurisdiction.

DR RENWICK: So just to unpick that again, and it may depend on what sort of DCP we're talking about here, but I – as I understand it, many DCPs in their standard terms and conditions would say we only provide information to government authorities when compelled by law, or we have a law enforcement switch, or something like that. That would not be an uncommon disclaimer or disclosure in terms and conditions, would it?

MR BROOKS: To the extent that it went to providing information to law enforcement agencies, that is a very standard disclaimer, absolutely.

DR RENWICK: Yes.

MR BROOKS: But it's not possible to make that sort of disclaimer against a TCN, and changing of the system that potentially makes its functionality less secure or less suitable for the prospective purchaser in a way that the supplier who is subject to the notice is not permitted to describe to the potential supplier – potential purchaser.

So many of the suppliers that could potentially be subject to a TCN, whose products are in the security space, are subject to – who are selling to foreign governments and agencies, and I was speaking to a couple of them only a day or so ago at a conference in Melbourne, are actively looking at needing to set up a subsidiary in a foreign country, only hiring people from – or not Australians, and effectively separating their businesses, their Australian business from their international business, so that a potential purchaser is dealing with the international business that only deals outside Australia and is therefore not subject to these requirements and is not tainted by the risk or a perception that it might be affected by a requirement to weaken the functionality of the system.

DR RENWICK: I can see how unattractive that is obviously to the DCP. But let me just again try and focus in on this. So I don't know if you've got the statute there, but – do you have a copy of the statute?

MR BROOKS: Yes, we do.

DR RENWICK: Yes. So if you look at 317ZG, and I'm not responsible for the numbering, page 84 – we can provide you that. S 317ZG(1)(b) says that none of the Schedule 1 things, including a TCN. So firstly – well, let's just look at (b), and I suppose what I'm talking about is patching. So presumably it is commonplace for all DCPs that while they don't intend to create a systemic weakness or vulnerability or a back door, occasionally some clever person finds such a problem.

MR BROOKS: Of course, yes.

DR RENWICK: Of course, and so it's patched. And this happens routinely all the time.

MR BROOKS: All the time, yes.

DR RENWICK: So my reading of subsection (1)(b) is that what you cannot do is prevent the DCP, even with a TCN, from rectifying a systemic weakness or vulnerability in a form of electronic protection. In other words, to me that means at any time, when they discover it's a problem, they can patch.

MR BROOKS: They can, but – and again, this would obviously be different for different situations, for different providers – to what extent would they be permitted by the agency to the patch the very vulnerability that the agency asked them to create in the first place?

DR RENWICK: Well, that's the question, but I must say - - -

MR BROOKS: That is the question.

DR RENWICK: No, no, but I must say my reading of it, and we will certainly put that directly to Home Affairs tomorrow, but my understanding is what it can't do, what this Act can't do is it can't prevent you catching. So step 1 is no systemic weakness or vulnerability.

MR BROOKS: Yes.

DR RENWICK: We can debate definitions, we can debate how to resolve the dispute about which side of the line you fall on, and I gave some examples about how you can do that today, and I welcome, just generally from anyone here, I welcome suggestions about how to improve those definitions. But I must say, my reading of it at the minute, when you read (1)(b), assuming the systemic weakness permitted you to create a weakness, and I don't think it does, it couldn't by (1)(b) prevent you from patching it.

MR BROOKS: No, absolutely. And that would absolutely be a normal course of events and is a normal course of events for mistakes, bugs that are found to have crept into the system through the normal course of product design and implementation. To the extent that someone tried to patch and repair a system change that was actually requested as part of a TCN, agencies would probably be – require some notice that that was going to happen, and it does rely on the organisation or the agency, if they're going to give permission for that to happen, to recognise that that is in fact a systemic weakness and systemic vulnerability.

And that goes to the whole issue that there actually is no real agreed definition of what systemic actually means in these definitions. So the definitions themselves actually need to be reworked so that it's actually clear to both the provider and the agency and we don't end up with this "that's systemic vulnerability", "no, no, no, that's just an ordinary vulnerability, it's not systemic", which is where those disputes can come from.

DR RENWICK: So just a couple of things I suppose is I've already said I'm very sympathetic to improvements to the definitions, I strongly think there should be examples, in the statute, not hidden away in explanatory documents, about what is or isn't a systemic weakness or vulnerability. Obviously they can't be comprehensive, but they could be important indicia.

So I don't require any convincing as to the wording, I welcome it. As you know, there's a Bill before the Parliament at the minute which talks about

effects, and I think there's something to be said for defining things in an effects-based way. The problem is this, if I can be very frank, you want the TCN provisions to be immediately revoked and reworked. If that were not – I think that's what you want.

MR BROOKS: Put on hold and put on a stay so that they effectively are not going to be used until we can work through the - - -

DR RENWICK: All right, okay. But when you talk about working through, there's two levels isn't there. There is the definitions and whether they're adequate, and that may well involve sitting down and talking to Home Affairs and the other agencies and working through scenarios, and I'm very happy to make recommendations that that should happen in any event, but those - - -

MR BROOKS: We think doing that collaboratively between the law makers, the law writers and the experts who know what terms are actually used in industry and do that collaboratively would be an excellent process to go through. Would have been an excellent process to go through back at the beginning.

DR RENWICK: Certainly. So yes, as I say, I'm happy to indicate that – I'm happy to recommend that there be such collaboration, there's no difficulty with that. I suppose the second question to improve the definitions or the understanding of definitions. The second thing though I think is that in broad terms you're indicating that independent decision markers, not the Attorney-General, independent decision maker sitting with suitable technical experts.

MR BROOKS: Yes.

DR RENWICK: You could do that a number of ways. Sometimes in statutes it says things like, you know, a Tribunal should be set up with the following people, and you could have it, I suppose, so that the government nominates a technical expert to sit, and then, if not the DCP, but an industry body, nominate a group of technical experts. And that is more or less what ITCO or the TAB does in the UK, and I see you all nodding, that's a good thing, because that gives industry and your sorts of groups a buy-in as to who the people are.

MR BROOKS: It does, and one of our concerns and one of our recommendations in our original submission is that the legislation currently envisages that a DCP could engage legal support to assist them professionally in evaluating when they receive a notice. But currently it doesn't allow them to engage any other sort of specialist advice, such as

technical support or technical advice, that provision is limited to legal advice only.

So our recommendation in our original submission was that that be reworded slightly to allow a DCP to engage professional advice in general to allow legal, technical, whatever other form of professional advice a DCP might need, in evaluating how they will respond to when they receive a notice or a request. Recommendation 5 in our submission.

DR RENWICK: Well, you can assume I'm in favour of that, and I mention again for the benefit of Home Affairs that I welcome their reaction as to why that would not be a suitable matter.

Just to be clear, there's a concern about individuals versus companies. I mean, Home Affairs do say that the reason they say the DCP has got to be able to cover individuals is because, after all, you could be dealing with a sole trader. But they say, and you heard the ICACs for example, say today that dealing with an entity, they would always go to the entity.

MR BROOKS: Yes.

DR RENWICK: And the entity could no doubt draw on internal advice and so on. There's no suggestion from Home Affairs I think that they would want to pick on individual engineers and so on.

MR BROOKS: I think that is certainly a concern from industry in initial reading of the initial drafts when they first came out, that use of persons, particularly being reviewed by people without a legal context, where that word "person" has very much a personal meaning. And as a business owner and potentially a recipient of notices myself, that clarification, if that could be reflected in the legislation itself, I think that would go a long way to alleviating that concern.

DR RENWICK: Well, look, I'm deeply grateful to your very thoughtful submissions, both in writing and today. You've only had a day or so to look at my opening remarks, if in the next week or so you did want to comment on anything I've said in my opening, I would welcome that, because you're a very important group.

MR BROOKS: We'll absolutely look at it and looking to provide some comments. One of the things that struck me in looking through many of the other submissions, particularly from the agencies, is this, there appears to be a perception and, as an engineer not a lawyer, I'm not too sure why this is or not, that there must always be a warrant for something afoot before the provisions in this legislation can actually be enacted.

As an engineer I'm not sure that that's actually true, there are an awful lot of people listed in the DCP-type list of things and some of the listed acts and things they can be asked to do, which don't appear to be the sort of things that would be subject to a warrant to allow them to do. But in any case, one of the things that occurred to us that a – that whole what is systemic, what is not systemic, if the aim of the legislation, according to a warrant, is to access the device of a named person or a particular device for a particular person, then it would seem logical that a systemic – or something that you shouldn't be allowed to do is anything that would affect the data or systems that affected anybody else that was not that named person or that named device.

That seems to strike me as a – whether it could affect somebody else's data or somebody else, a device or not, is actually an incontrovertible truth that should be evident to all parties that are making that evaluation. And maybe that's a possible way out of the dilemma.

DR RENWICK: Do you mean by affected, do you mean by – do you include in the idea, concept of view? So in other words, I'm trying to find out all the people who – so I'm trying to find out the person who used a mobile phone within this area, I do a triangulation search, there's 10,000 people, but I want to use some method to narrow it down. So – I mean, you're not affecting people's data by doing that search. Is that the sense in which you're using it, or are you talking about affecting it in a different way? Do you see what I mean?

MR BROOKS: I guess the scenario that the industry is concerned with is where an agency may wish to access a particular person's Android phone, and instructs the manufacturer of that phone, because the manufacturer and supplier is a DCP, to introduce something into the software of that phone that then gets loaded into all phones of that type.

DR RENWICK: That I understand, yes.

MR BROOKS: Those types of scenarios. And everybody in the industry will have a different scenario, I'm just saying that is an exhaustive – but that is the type of concern. The scenario you raised is more likely to be covered through metadata collection anyway, which is somewhat a different exercise, until it can get narrowed down to it was this device with this special hardware ID that was within the cell area in those times. Which is probably when these provisions will then kick in with that device identified.

MS RAICHE: Just a clarification. I think stating it another way, we're talking about – when we're talking about systemic, maybe think of it in a

different way than perhaps the way that the amendments talk about. And that is the bottom line for, certainly for Internet Australia, is you should first get judicial permission to do whatever. That will mean that you have already specified an individual or a target group or whatever, and they've probably been identified through metadata or whatever means.

The use of this is systemic, but I'd probably put another word. What we don't want is that whatever is being asked to do, whether it's information or whatever, that it goes beyond the bounds of what the warrant allows.

DR RENWICK: Sure. That I understand.

MS RAICHE: So it's perhaps, just stating another way, you're allowed to do that much and that's all that you should be doing.

DR RENWICK: I understand. Just to finish with the idea of the warrant, I think strictly speaking my reading of the Act, and indeed what the agencies said, is not that every single listed act or thing requires a warrant, but rather that if it did require a warrant, it still requires a warrant.

MR BROOKS: Yes.

DR RENWICK: That's 317ZH.

MR BROOKS: Yes, and that is reassuring. Then leaves open the question of what is the authoriser, what is the process.

DR RENWICK: Sure.

MR BROOKS: What is the process for all of those listed acts or things that don't require a warrant?

DR RENWICK: I understand.

MR BROOKS: And the effects that could cause. That's possibly a different discussion.

DR RENWICK: That I understand. Can I just say that's been immensely helpful for me so thank you all for making the effort to come.

MR BROOKS: Thank you.

DR RENWICK: It's now 12.27, we'll come back at say, five past one if that's convenient. Thank you all.

LUNCHEON ADJOURNMENT [1227]

RESUMED [1302]

#SESSION 3: Electronic Frontiers Australia

DR RENWICK: Ladies and gentlemen, welcome back. I'm delighted to welcome Mr Angus Murray, who is the Chair of the Policy Committee of Electronic Frontiers Australia. Did you wish to make an opening statement?

MR MURRAY: Yes, thank you. Good afternoon Doctor, I would like to make an opening statement. Firstly, thanks for the inquiry and the process that you're undertaking. Electronic Frontiers Australia appreciates the role of your office and the ongoing consultation in relation to this Act.

It's useful and probably relevant for me to mention that I sit as the Chair of Electronic Frontiers Australia's Policy Committee, but also the Vice President of the Queensland Council of Civil Liberties. Before I start, have each of you had the opportunity to review the submissions that were put to you?

DR RENWICK: Yes indeed.

MR MURRARY: Very good. Putting Electronic Frontiers Australia into context, EFA was established in 1994 as a national, member-focused not-for-profit organisation. EFA's major objective is to protect and promote human rights and civil liberties for users of digital technologies, so called, 'digital rights'.

The TOLA Act, or the *Telecommunications and other Legislation Amendment (Assistance and Access) Act* 2018 engages a large number of digital rights. In this opening address, I'll briefly touch on the three submissions that were made to the committee, or in the process. The timeline of this I think is relevant.

The first was a submission to the Department of Home Affairs dated

10 September 2018. That was a comprehensive submission put together in a very short period of time. The second submission was a submission to the Parliamentary Joint Committee on Intelligence and Security in October 2018. That was supplemented by evidence I gave to that committee in November last year. The Bill then passed, as I understand, and came into force on 9 December 2018. That was a very short period of time.

The Parliament Joint Committee on Intelligence and Security has had further consultation rounds, and a third submission was submitted on behalf of Electronic Frontiers dated 1 July 2019. You have regarded the submission that I sent to this inquiry dated 21 November 2019 that attached each of those three submissions.

I intend to briefly run through those submissions and then invite questions on those submissions, however for the purpose of this inquiry I repeat and reiterate the totality and the substance of each of those submissions. After I run through that summary of the submissions, I'll make a few comments in response to the opening remarks, and Dr Renwick, I appreciate the opportunity to have reviewed that before this inquiry.

DR RENWICK: Thank you.

MR MURRAY: Before I start on any of this, I need to reiterate - because this is extremely important in terms of the report that comes out of this process, the overarching concern that I have is the way in which this legislation has come into force, the rushed nature of it, and the extreme disregard to the Civil Society Organisation's technology providers and industry that provided advice and guidance to the Department of Home Affairs. It was, in my respectful submission, irresponsible of Home Affairs and irresponsible of the Federal Government to push this legislation through in the rushed manner that it did without completing the proper consultative process. The fact that this process is ongoing is clear evidence and demonstration of that fact.

In terms of the legislation, I take issue with a number of aspects of it, but for the purposes of this hearing, I think it's useful to summarise these. There are 38 recommendations that were made to the Parliamentary Joint Committee on Intelligence and Security in the October submission. Each of those recommendations have equal force. The recommendations are put in the context that this legislation should not have passed, this legislation should not be enforced. It is appropriate and responsible for government to repeal this legislation, and do so until such time as Australia has a federal enforceable human rights framework that brings us to stand with other Western democratic societies and countries.

I'll come back to that point, because that point of enforceable human rights frameworks is extremely important in Electronic Frontiers Australia's submission. The first proposition in terms of the recommendations is quite simply that the Act is not proportionate to Australia's reasonable expectation of fundamental human rights. There are a number of comments made about foreign jurisdictions see this Act, perceive this Act, and treat and deal with Australia in terms of multilateral and bilateral trade agreements.

This must be understood in the context that Australia does not have a federal enforceable human rights framework, and this legislation cannot be proportionate to the reasonable expectations of Australians absent of such a framework. That is a fundamentally important submission.

In terms of the operation of the legislation itself, there is a complete lack of - or at least an insufficient consideration of public interest in relation to technology assistance notices, technology assistance requests, TANs and TARs, and the more controversial technology capability notices. I'll return to them, and I understand that there are questions specifically that the Security Monitor might wish to have in terms of TCNs.

The other aspect of the Act - and I appreciate that in the opening remarks, focus was primarily put on the Schedule 1 amendments - the Act also introduced a number of things to other legislative frameworks, including the Surveillance Devices Act. Operatively, into that Act came the expanded definition of a word, 'computer'.

Computer is now defined effectively to be access to the internet. Those covert computer access warrants may be issued retrospectively, are done covertly, and with the consequence of the amendment to the definition at section 6 of 'computer', is access to what could be, retrospectively and covertly, the internet at large.

In the same vein as definitional issues, there is a broad and inappropriate scope of the definition of 'designated communication provider'. If I draw the Monitor's attention to item 5 of the definition of a designated communication provider, the scope of that is effectively any person that provides, directly or indirectly, or ancillary to, an electronic service - which I'll come to in a moment in terms of its definition, that providers that electronic service to an end user, is a designated communications provider.

The context of these inquiries has largely been this is about big tech, this is Google, this is Facebook. This is not Google, this is not Facebook, this is a legislative provision that has a broad, almost unlimited application, which has significant consequences that flow from failing to comply with - or as

you've heard in evidence today, commercial consequences of providing services to people and the inability to give certain guarantees and surety in terms of the quality of the service and the manner by which services operate. That definition is unacceptably broad.

The definition of electronic service is equally broad, it's open to amendment in regulation. That needs clearer and more specific, targeted definitional terms attached to it. I accept for the purpose of these inquiries there is a lot of discussion about the intent of government and the intent of ministers. You would appreciate, each of you today, that legislation is construed on its face as a text in context exercise. Ancillary or explanatory material that sits around the legislation is only used for the source of context. It is the text itself the courts will interpret, and that is the purpose of this submission. These need to be certain definitions that are clear and provide safeguards to Australians to ensure that both the providers of services and the consumers of those services, as well as the population generally, are certain that they are not being subject to what is effectively a mass surveillance regime.

Acts or things is a further definition that is extremely broad. It opens itself up again to amendment or further inclusion under the regulation. You'd appreciate that's something that doesn't have to pass the House, and something that could be done very easily in the future, although I accept for the purpose of this inquiry that this may not have been used particularly prolifically. This has every scope and potential to be used and abused in the future with very little oversight, very little consultation, and in a manner that would be very difficult for a court to read around.

I've already mentioned, but I'll repeat - the definition of 'computer' in section 6 of the Surveillance Devices Act is equally inappropriate, and that it requires clear and appropriate consideration in terms of whether that scope is responsible, and whether that scope is in fact technologically feasible.

In terms of the definitions of 'systemic weakness' and 'systemic vulnerability', I don't bring a technology background to this, I'm not with sufficient knowledge to be able to properly assist with how those definitions may be redrafted, however there is clear work that is required there.

I also draw to your attention to the concept of target technology. There's been some discussion about how and where a person would be affected by these TCNs, TANs and TARs. Target technology requires clearer guidance as well in terms of how broad the scope of this is. For instance, is this an individual instance of say, Facebook Messenger on a single device dictated by a Mac address, or is it more like the computer definition in the Surveillance Devices Act, that it would be the totality of the network or something located on a server, is it within Australia, is it outside of

Australia? Target technology requires consideration.

In terms of the Bill, you would all appreciate the relatively recent decision of *Big Brother Watch v United Kingdom*. That's a decision that's referenced in submissions put to the Monitor. I believe that that's probably the most useful way for the Monitor to consider or construct the concept of oversight for this legislative regime.

In that decision - and I will read this passage so it's clear where I come from with this - that decision deals with oversight of covert surveillance technology or covert surveillance legislation in the United Kingdom. And I appreciate, Dr Renwick, your work in the United Kingdom recently, so this probably bears particular relevance. I quote from that decision, *Big Brother Watch v United Kingdom*:

> *Review and supervision of secret surveillance measures may come into play at three stages. When the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself, but the accompanying review, should be effected without the individual's knowledge.*
>
> *Consequently, since the individual will necessarily be prevented from seeking effective remedy of his own accord, or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide an adequate and equivalent guarantee safeguarding his or her rights.*
>
> *In a field where abuse is potentially so easier in individual cases, and could have such harmful consequences for democratic society as a whole, I have emphasis it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and proper procedure.*

I'll come back to the concept that you raised in relation to the oversight via the Administrative Appeals Tribunal.

I take those as overarching points in terms of the submissions that have been put to you. The submissions are fulsome, the submissions cover off on each aspect of the legislation insofar as Electronic Frontiers construes a digital rights issue or a digital rights impact as a consequence of the introduction of this legislation, and I commend those submissions in full to the Monitor.

In terms of your opening remarks, Dr Renwick, as I stated - this is in the context with great respect and appreciation from this being provided to me early - and it is useful to see your mindset as a preliminary assessment of the legislation and where you might go in terms of questions.

DR RENWICK: Yes.

MR MURRAY: Firstly, it's difficult for me to agree with your proposition in relation to ICACs and the legislation empowering the corruption commissions to effect the same form of surveillance on police, because that in itself accepts the validity of the legislation. With that caveat in mind, if the legislation is to remain, with the overarching submission being that the legislation ought to be repealed in full, oversight of police and law enforcement should occur, and I comprehensively agree with the proposition that this is not something that should be subjected solely to - or Australian citizens alone should be subjected to.

This form of legislation or this form of covert oversight should also be possible for not only law enforcement, but government itself. If such a recommendation is to be made, that recommendation is supported and expanded to include government itself.

In terms of the illicit activity you mentioned, you give a number of examples, and one such example was corporate intellectual property.

DR RENWICK: Yes.

MR MURRAY: That may have been a slip in terms of the scope of the legislation or where the legislation might go. The Monitor would appreciate that the mandatory metadata retention scheme received a fair bit of scrutiny when it was introduced in 2013 and then subsequently passed in, I believe, late 2014 if not 2015. One aspect of that was a promise by the then Attorney-General, George Brandis, that it would not be used for civil proceedings or for civil purposes, and would be alone in the criminal jurisdiction.

Almost immediately after that was passed, there was a proposition that it would be expanded to include intellectual property enforcement. Intellectual property theft, as you put it, is not an appropriate context for this legislation. This is not power that should exist in the hands of corporate bodies, this is not a power that should have its scope creep into the enforcement of civil proceedings, and certainly not in the context where a number of these rights holders would be US-based.

With respect, I fundamentally disagree with any proposition illicit activities within the scope of this Bill should be construed in a civil context, as it completely misapplies the intention of the legislature, and if the legislature's intention is to widen the scope to civil proceedings, that must be made abundantly clear, and separate consultation should occur in that regard.

In relation to your comment about lawless ghettos and the importance of ensuring that digital law enforcement is akin to physical law enforcement. That proposition is, with respect, somewhat misguided. The traditional physical surveillance of people and the traditional surveillance mechanisms that were used before this technology became a particularly great problem in the eyes of government or law enforcement was very different.

That form of surveillance - or that form of legislation was targeted towards individuals in a closed environment. What you have before you is legislation that is so broad that it contains almost limitless definitions, secret powers, the ability to survey Australians en masse, and significantly erode the prospect of Australians every being able to enjoy what should be already in existence, being a fundamental human rights framework that is enforceable at a federal level.

DR RENWICK: Can I just stop you there? You've said a couple of times that this is effectively a mass surveillance regime.

MR MURRAY: Yes.

DR RENWICK: No one else has said that, what have you got in mind? What do you mean by that?

MR MURRAY: This legislation does not limit itself in terms of its scope, this is not specifically to target an individual, this is to target services. What I have in mind is although - and I accept as at the current date, this has not been used as a mass surveillance tool, the legislation does not prevent that from occurring. If a person, for example, was engaged in some form of illicit activity and was conducting that on a computer, as this legislation is targeted towards, the definition of 'computer' in section 6 of the Surveillance Devices Act now allows, retrospectively, an AAT-issued warrant, access to the internet - or if you take that definition, the four read together, it is a network of computers across any number of computers and any number of network locations. That warrant would allow surveillance across the whole - en masse. That is mass surveillance. The legislation doesn't specifically preclude that. It doesn't authorise it, but it doesn't restrict it.

DR RENWICK: So what you're referring to there by 'mass surveillance' is

the changes to the Surveillance Devices Act effected by Schedule 2?

MR MURRAY: I've taken that as an example, and to be clear on what I've just said, that is - it doesn't authorise mass surveillance, but it doesn't prevent the possibility of mass surveillance. The same thing could occur in relation to a technical capability notice that feeds into some service that again, could be very broad given what a designated communication provider's definition is.

It creates surveillance that may be inappropriate in terms of the target towards those DCPs. If a law firm, for example, a large law firm was the subject of a DCP or a software provider to a law firm was subject to a DCP, you would end up with surveillance, essentially over a number of people who were subject to arrangements with confidence, and there is no limiting factors in this legislation.

DR RENWICK: But there are limiting factors. I mean, what about section 317(z)(h), which says effectively if you needed a warrant before, you need a warrant now? I mean how does that square with this idea that this Act effectively permits mass surveillance?

MR MURRAY: You wouldn't need a warrant in relation to a TCN or a - not a TCN rather, a TAN or technological assistance notice or request, and that widens that possibility.

DR RENWICK: Sorry, to do what? You better give me a specific example - so just give me an example of what you say could be done by way of mass surveillance under Schedule 1.

MR MURRAY: If you had, for example, a requirement to say, Facebook or its Messenger service, to provide all information in relation to the services or communications that are occurring over that network, that facility already exists, it wouldn't require breaking any encryption, and that would effectively allow monitoring of a mass number of people. There is nothing in this that specifically draws law enforcement to target this legislation towards an individual.

DR RENWICK: But you'd need to have an underlying warrant to get that content from Facebook, wouldn't you?

MR MURRAY: In a broad sense. In a practical sense, I'm concerned there isn't a limiting factor. On the issue of the warrant, there isn't a limiting factor. There are examples - and I don't have the Act in front of me, which would probably assist me, Dr Renwick. My concern with this - and not to be drawn on specific examples - my concern with this is simply - as

chairman of Electronic Frontiers - is this is something that could be used and abused in the form of a mass surveillance regime.

DR RENWICK: What about section 317(p), which says the issuing officer has to be satisfied that the requirements imposed by the notice are reasonable and proportionate, and that compliance is practicable?

MR MURRAY: You touch on another definitional point that is of relevance and contained in my submissions, Dr Renwick. There is no definition of 'reasonable and proportionate'.

DR RENWICK: Well there is, there is a definition of reasonable and proportionate, and examples are given.

MR MURRAY: (Indistinct) sir.

DR RENWICK: Anyway, I mean, for example they're found in section 317(j)(c). Anyway, all right. Just a couple of questions then. You say in your October submission in page 19, second paragraph:

> *While we appreciate the extent to which encrypted communications can sometimes introduce friction into intelligence and criminal investigations, we encourage much greater evidence-based discussion on these matter as a vital starting point for any legislative reform.*

And you refer to a CSIS study that other issues are more likely to frustrate law enforcement's ability to effectively access, analyse and utilise digital evidence, including an inability to effectively identify which service providers have access to relevant data.

MR MURRAY: Could you take me to the page sorry, please?

DR RENWICK: Yes, sorry. Page 19 of your October submission, paragraph 2. Just have a read of that to yourself.

MR MURRAY: Yes.

DR RENWICK: So that's an interesting observation, given the agencies say, "Well, encryption is the thing that's having the greatest impact," why is it that these things would in your view create a greater problem than encrypted data - sorry, content or metadata?

MR MURRAY: In the sense of the volume being the issue rather than the encryption being the issue, if I understand the question correctly? This is a submission that was made in the context - as well with the mandatory metadata retention legislation - the problem that you create here is with any form of mass capture or the ability to mass capture information, you widen exponentially the haystack. If you don't have a clearly-defined pin, the exercise of identifying the pin that you're seeking becomes exponentially more difficult.

The point that's being made there is simply encryption is an issue, but the volume of information that's being captured is a greater issue, and the ability to discriminate and discern where issues exist or persons who are engaging themselves in unlawful conduct exist within a greater dataset is a bigger problem than being able to break through encryption. The intention behind this, I assume, is preventative, rather than retrospectively for the purposes of prosecuting.

DR RENWICK: Do you have any particular observations about the AAT model?

MR MURRAY: I don't have - this is the AAT model that you proposed in your opening remarks, Dr Renwick?

DR RENWICK: Yes.

MR MURRAY: I think it's a prudent approach. But I think it's a prudent approach that is again (indistinct) in the sense that this legislation should be repealed. I think it's a prudent approach, however if this is to go ahead, there is a specific jurisdiction set up for the purpose of overseeing the manner by which anything in this legislation is issued.

The problems that I would have with it are simply that - in a number of directions. The first is the reason why I quoted from *Big Brother Watch v United Kingdom* is to emphasise the importance of judicial oversight. As you would appreciate, the Administrative Appeals Tribunal is not a court, it's an administrative function. I appreciate it's an independent body, but it doesn't sit as a court, it doesn't operate the curial function.

DR RENWICK: So it's an objection of principle, not an objection that they're not going to do a good job?

MR MURRAY: It's an objection, yes.

DR RENWICK: Right.

MR MURRAY: And I don't in any way, shape or form impugn the members of the Tribunal or the role that they serve, simply that there is a difference fundamental to our society and the operation of our society that separates the judiciary from the executive.

DR RENWICK: Okay.

MR MURRAY: The second issue that I have with that is it's well and good to say that the DCP could turn up and could have an argument about the scope or the manner by which something is input into their system, however that requires funding, and that requires a person or a body to be able to properly address the issues and properly ventilate that through the Tribunal setting. That presupposes that the DCP to which this process would be subjected is capable of funding and capable of meeting those arrangements.

As I said, this is something that isn't targeted towards Facebook and Google, and it is improper to suggest that this is Google, Facebook and big tech, it's much, much broader than that. And the final proposition is - - -

DR RENWICK: Sorry, who's suggesting that it's just focused on Google?

MR MURRAY: A lot of the media around this has been, "This is about big tech." This isn't about big tech, the scope is significantly greater than that, and that's what's important to understand here.

The final point is - and I deeply encourage this - and this would be feasible under the AAT Act, is the ability to have the oversight by way of written reasons or decisions handed by the AAT in terms of the way in which DCPs are subjected to this legislation. That would be an incredibly useful guidance, both in terms of DCP's certainty, but also in terms of the ability to seek challenge of this legislation if there was some point where judicial review was desirable or possible in certain aspects of its operation.

DR RENWICK: Thanks Mr Murray.

MR MURRAY: I greatly appreciate it, thank you.

DR RENWICK: Thank you for coming.

#SESSION 3: Atlassian

Next we have the representatives of Atlassian. I invite them to come forward. Mr Patrick Zhang, Head of IP, Policy and Government Affairs.

Ms Georgie Skipper, Director of Global Policy. Mr Julian Lincoln, a partner of Herbert Smith Freehills, and Ms Anna Jaffe, a senior associate of Herbert Smith Freehills. Can I thank you all for your extremely thoughtful and helpful submission. I think all of you who have travelled from somewhere else, some of you quite a long way to be here, and I very much appreciate that. Would you care to make an opening statement?

MS SKIPPER: Thank you, Dr Renwick, we would. And good afternoon, we are really pleased to participate in this important review of TOLA. My colleagues and I are here representing Atlassian, one of Australia's great start-up success stories. Over the past 17 years, Atlassian has grown into a leading global software business, with over 4000 employees in 12 locations around the world, and over 160,000 customers; we are proud to say that Cochlear and NASA are among them.

We consider an important part of our role to highlight the views of our employees and our customers, and also our fellow business colleagues in the technology and software sector. Atlassian has engaged over the course of this parliamentary process relating to the Act for a very long period of time now, including directly by Scott Farquhar, our co-founder and co-CEO.

We have been pleased to come together with other participants in the sector throughout this process, noting that we are also a co-signatory to an earlier submission by StartupAus. We care about this legislation for four reasons:

1. The policy issue of balancing national security with Australia's growing tech sector;
2. The potential impact on our business, including our role as custodians of our customers' private and commercially valuable data;
3. The reputation of Australia's tech sector internationally;
4. The interconnectedness of the global tech and national security ecosystem.

In this statement, I will refer to each of these elements. I will start with the broader framing, in terms of the importance of the tech sector to Australia's economy, because we think this is absolutely fundamental.

The tech sector contributes $122 billion a year to the Australian economy, making it the sixth largest industry contributor to our GDP, and employing over half a million Australians; thanks to the report by Digi. We believe the sector can grow and become a backbone of Australia's economy, and our export capability.

In the past years, policy settings have encouraged significant rise in venture capital investments into the Australian start-up tech space, and that has been incredibly useful. We have seen a rise of Australian start-ups: according to start-up Blink ecosystem rankings, their 2019 report, Australia leapt forward six places to become the fifth most start-up friendly country in the world.

As such, our export capability to respond to global demand and things that improve standards of living - including ag-tech, med-tech, energy-tech, space-tech and so on - is increasing. This reinforces the importance of consistent legislation and administration across the matrix of tech policy. And importantly, the need for those to be created and implemented, keeping in mind the ways we can best position Australia for the future.

Atlassian understands the factors motivating the introduction of the Act, and appreciates that the private sector has an important role to play in working with the government to address and minimise threats to national security, and to combat serious crime. We are conscious of the government's concern that it faces risks of going dark; at the same time, we believe government needs to have regard to the commercial realities in which companies operate, and ensure that the requirements imposed are proportionate.

In today's technology environment, an ever-increasing volume and variety of information is stored and processed electronically, and an ever-increasing proportion of corporate and consumer transactions are conducted entirely digitally. Therefore, the scope of transactions and information which falls under the Act's reach is far greater and far more intrusive into the activities and operations of companies and their customers than yesterday's equivalents. In fact, the scope and impact of measures which the Act introduces represents a fundamental policy shift in Australia.

Further, the continued liability and growth of tech innovation, will, in a large part, be based on the actual and perceived security of the technologies that underpin the digital economy and its ecosystem. Everything is interconnected, and any system is only as strong as its weakest link.

Our submission outlined our specific concerns with the Act, which I'll go through briefly now, and then my colleagues Patrick, Julian and Anna are ready to engage with you on specific examples and amendments to improve this framework.

Atlassian has significant concerns about the operation of the prohibition on systemic weakness and systemic vulnerabilities, and the associated definitions in the Act. Atlassian is a trusted steward of its customers'

information, and the powers that are given to the government under the Act are extraordinary, as it stands.

There is a vast confusion in relation to what the boundaries of these powers are, because the current provisions are unclear. We support your, Dr Renwick's, view, of including specific examples to assist in clarifying the concept and its application. Furthermore, we believe that it is critical that TCNs are specifically identified as a last resort, to be used only where access is not reasonably available through existing means of co-operation.

Also, given the scope of the powers outlined in the Act, it is vital for transparency and public confidence in the Act that additional approval and oversight mechanisms be adopted. Accordingly, we believe that TANs and TCNs should be the subject of independent judicial oversight, and independent approval prior to their issuance.

We continue to also believe that the threshold for engaging the powers under the Act is too low; given the nature and extent of these powers, the threshold should be raised to those crimes punishable by seven years' imprisonment.

Atlassian also remains concerned about the interaction of the Act with foreign laws, including the limitations on the defence available to designated communications providers, only where they are located in a foreign country and compliance with a notice would breach the laws of that country.

Finally, we are also concerned about the perception for the Act to apply to individual employees of a technology provider, particularly given the current war for talent in a global tech industry. We appreciate that the government has indicated this is not the intent of the Act, and indeed, today we acknowledge that that has also been indicated. But we support that this be clarified in the legislation and any other further messaging, to remove all doubt.

To conclude, we understand that it is tempting to consider that much of the vocal opposition to the Act in the media, given its ardent and unequivocal nature, is based only on perceptions or myths of how the Act operates, however, we would urge caution in adopting this approach, both on principle and in substance. To the extent that the Act or its effect are unclear, there is no disadvantage, and indeed, a considerable advantage to using this opportunity to clarify the intent and operation of its provisions.

In an environment of increasing mistrust in the technology sector, and indeed in the context of a lack of trust in government as well, it is clear that

perceptions matter. We remain concerned that the effect of the Act has been to erode trust, limit the ability of the Australian tech companies to compete internationally, and in particular, their ability to protect their data and systems from compromise. Combined, this has had a corresponding effect upon the reputation of the Australian tech industry, globally.

We look forward to seeing some positive changes to the Act in the near future, and thank you for being able to participate in this process.

DR RENWICK: Thank you very much, that's most helpful. Well, can I start then with this question of perception? We know from the Telecommunications Interception Act annual report, tabled recently, that there has been no TCNs, no TANS - this is by police, ASIO's information is classified; there have been five TARs from the AFP and two from the New South Wales Police.

Now, this is early days; it may be that will change over time. But if that were the level of use of these powers, would that slightly mollify your concerns?

MR ZHANG: Yes, I don't think that the lack of use of the powers under the Act in the past year kind of mollifies our concerns, especially when certain actions are not known to use due to secrecy.

DR RENWICK: Right.

MR ZHANG: I do think that, you know, our goal should be to clarify the law and make good law and fair procedure, and that should be the goal, kind of regardless of what the early days of an enforcement actually look like.

DR RENWICK: Well, let's then talk about possible amendments. So you don't need to convince me there should be examples in the statute, rather than an explanatory memoranda; I agree. I will also recommend; the question is, what we recommend.

Turning to systemic weaknesses for example, we've got definitions in the Act; we've also got definitions in the bill before the Senate, which I have attached to my opening remarks in the endnotes, on the last page. And I'm happy if you wish to take this on notice, but I mean, are there particular reforms you have in mind?

MR ZHANG: Yes. Yes, we took to heart some of what we discussed in Mountain View during our last engagement, and we did go back and consult with some of our security team, and also listen to the concerns of others around us, around what they think the impact could be under the AA Act.

And what we heard was twofold I think, primarily; one is a fear of building of portals, or "backdoors" that would then be exploited down the road, by black-hat actors, whether private or governmental. Another aspect that we heard is a fear that the Act could be used to prevent us from improving our security methodologies and encryption methodologies.

So turning to the current definitions, I think we do agree with a lot of what Internet Australia also said earlier about the definitions being ambiguous and unworkable. I think the definition of you know, a whole class of technology is certainly problematic, in that it can be read so narrowly as to basically erase much of the protection that was intended. And similarly, the allowing of selective introduction of vulnerabilities into targeted technologies that are connected with a person, honestly, can be construed very broadly to allow a multitude of ways or accessing our systems in an intrusive way.

I think we understand that there are clarifications and limitations to that, but we don't think they go far enough, or, in some instances, they conflict with what is seemingly allowed in the first portion of the Act. And so we do support the proposed amendments, the so-called Repair AA Act Bill. We agree with you that it very helpfully focuses on prohibited effects, and so I think that is a good starting point for us.

But we would still like to add additional examples or amendments, however they can be framed, of specifics that go back to the earlier points that I mentioned in terms of portals and preventing us from improving our systems.

So one specific amendment or example, however you want to frame that, would be to I believe section 1B of what was proposed in the Repair AA Act.

DR RENWICK: Yes, I've got that in front of me.

MR ZHANG: Okay. So currently, it says:

> *A technical assistance request or TCN must have the effect of preventing a DCP from rectifying a systemic weakness or a systemic vulnerability.*

DR RENWICK: Yes.

MR ZHANG: We find the circular reference to "systemic weakness" and "systemic vulnerability" problematic, given that that is a loaded term that people have struggled to define. So instead of saying that, we would rather just say, "Should not be prevented from rectifying or improving its security or encryption capabilities."

And so that is the fear. I know that there was a discussion around patching earlier, and we recognise that there is a prohibition against patching. But against that, that again is loaded with the systemic weakness and systemic vulnerability term. And there are instances where we're not merely seeking to react to a particular issue and patch; rather, we may be rolling out a new system to improve our capabilities. So our fear is that the Act could be used to maintain a certain level of capability that is not in line with our customer's security interests.

DR RENWICK: And just pausing there, that is particularly focused on a TCN; that is to say being required to create a new functionality. In other words, if you've already got the functionality - - -

MR ZHANG: That's right, yes.

DR RENWICK: - - - provided you could patch things, that's all right.

MR ZHANG: Yes.

DR RENWICK: But the TCN is the particular - - -

MR ZHANG: Yes, yes.

DR RENWICK: I understand that, thank you.

MR ZHANG: There is a second point that we wanted to make with reference to section 2 of the Repair AA Act, which currently refers to prohibiting the implementation or building of a new decryption capability. So we appreciate that limitation, certainly, but we would go one step further to also say, "Or bypass existing encryption capability."

The reason being, that there are end-to-end encryption systems, however, there are also mini-systems that are partially encrypted, where the way into the system is to find the joint in the armour, if you will, and where the system is unencrypted. And to ask a DCP to identify and build an exploit into the weakness of its own armour is something that we are afraid will cause a systemic weakness if found down the road, by black-actors.

DR RENWICK: Okay, so just to take an example - and I'm not asking you about this for your company - but let's say you have a single key, a single unlocking key; you would object to say, ASIO coming along and saying, "Please create us a law enforcement or intelligence key, which only we can use"? Is that an example? I'm just trying to move from the very theoretical to an example. Is that the sort of thing?

MR ZHANG: I think if we hold the key to certain information that we can then decrypt, I think there is no need for us to create another key for law enforcement. I think we can use that key to provide the information to law enforcement.

DR RENWICK: I see.

MR ZHANG: we would actually have a concern about creating a second key and giving it to law enforcement, because then that is out of our hands, and we don't know where that key may end up.

DR RENWICK: So that's an important distinction, isn't it? So if law enforcement comes to you with sufficient legal authority, and you can say, "Well, we either can do that," or, "We can't." And if you can, you can provide it, then that's less of a problem?

MR ZHANG: Yes. And I think that's the existing co-operation.

DR RENWICK: Yes, indeed. Can I just ask you to look at subsection (4) of the same section you're looking at?

MR ZHANG: Yes.

DR RENWICK: Second line:

> *Building a systemic weakness or vulnerability includes any act or thing that would or may create a material risk.*

Well, "may create" it. I mean, from a technical point of view, how could you ever say that something "might not" create a technical risk? I mean, it's in the nature of your world, isn't it, that all sorts of unintended things happen.

MR ZHANG: Yes.

DR RENWICK: That's what you issue patches for. In other words, I'm concerned that that's just an unrealistic standard which can never be met.

MR ZHANG: I think the word "risk" itself contains some of what you're referring to already, in terms of obviously risk is not a known impact; risk is an impact that could happen. And so I am not as troubled by the word "may." I do think that - - -

DR RENWICK: That "may, with risk."

MR ZHANG: I'm not particularly tied to this language; if there are ways to improve it that would satisfy you, I think we would be open to that. But I think the point is for language to express the idea that whatever it is that we are being asked to do will create a material risk, which is a thing that may or may not happen. But perhaps what that line is for, is it may be for the technical experts, with the judicial officers to decide, in practice.

But I think that is our concern. Our security engineers' concerns are really that our systems will be compromised in a way that makes it easier for our customers' data to be stolen, and our customers include high-tech, you know, NASA and Cochlear, who had trade secrets that may exist on our systems. And you know, your opening statement very helpfully referred to the current environment of national actors, private actors, stealing intellectual property, and that is somewhat of a potentially self-inflicted wound, if we open our systems to that kind of exploit.

DR RENWICK: Well, let's then talk about safeguards. You've mentioned judicial oversight, and I well understand you know, I know a little bit about the US fourth amendment jurisprudence, and I understand the need to have judicial involvement in the States.

But here, we have one of two things on the pre-TOLA front: we either have judges or tribunal members acting in a personal capacity, not as members of the court; that's a bit of a Constitutional fiction which the lawyers will understand. And so I am concerned that you may have heard this when I discussed this with the Human Rights Commission: personally, I think it's a diversion from the role of a full-time judge.

There is a lot to be said for the British model in this sense: you have a group of very senior, very able lawyers, with very good technical assistance available to them, so they understand what's being talked about. And they build up some expertise in what's being talked about, rather than receive you know, a warrant at 6 o'clock in the evening with some summary and pressure of time, and all the rest.

And so I suppose there are two things there: from your point of view, would the Administrative Appeals Tribunal - which is independent of government

- providing they're properly informed, would that go a fair bit of the way to meeting your concerns about an independent person issuing or authorising the warrants or TOLA powers?

MR ZHANG: I'll actually ask Julian to take this one on as well. But I think initially, I'll just say that our primary concern is around having a rigorous approval process, and a rigorous process for review and appeal. We've discussed the British model, I think at our meeting in Mountain View, and we are certainly open to that, and I'll let Julian kind of comment on some of the specifics.

DR RENWICK: Please.

MR LINCOLN: Thanks, Patrick. As Patrick says, Dr Renwick, we do think it is important that we have a clear independent oversight. We are less concerned about how that is achieved, and there are different ways and different models. There are obviously pros and cons to adopting an existing structure such as the AAT model, versus putting in place a new structure such as the UK, although that's obviously a policy question for government, how it wishes to implement it.

I mean, I think we do still feel that having the judiciary involved, and using the existing processes, noting your comments and concerns around the expertise, but also on the other hand, noting the judiciary is well-experienced at handling urgent interlocutory matters, hearing complex technical evidence, and processing those. And of course, as we see in the Federal Court, you have particular judges being assigned cases in expertise.

So I think that there are ways to solve those problems, using the existing judicial systems, which is our preference. But ultimately, at the end of the day, our objective is to ensure that independent oversight, if that can be achieved through one of the other means that you've suggested, we are comfortable with that as well.

DR RENWICK: And the other thing I mentioned in my opening is, you use that method, whichever one it is, to resolve bona fide disputes about whether the systemic weakness or vulnerability line has been crossed.

MR LINCOLN: Correct. Thank you, that's a very important point: we think it should be both as part of getting the order in the first place, and then to determine any dispute. And we think that I guess as you've noted, building up that expertise within that organ, however it's constituted or structured, so that you do have those people with that expertise looking at these issues as they go through the system, both pre-and-post, and handling those disputes, yes.

DR RENWICK: Right, thank you.

MR ZHANG: Dr Renwick, if you don't mind, actually I had one more proposal about the - - -

DR RENWICK: Yes, of course. Sorry I cut you off.

MR ZHANG: No, no worries. So the same section 4 of the Repair AA Act that we were just talking about, where it states that:

> *TCNs should not be used to build a systemic weakness that may create a material risk that otherwise secure information would, or may in the future, be accessed… by an unauthorised third party.*

We would propose, given our colleagues' concern with the building of portals, and given the government's stated position that they're not looking to build backdoors or portals into our product, a further clarification that says that a TCN will not be used to build a new point of access, or modify an existing point of access into our electronically protected products and systems.

We read Home Affairs' response to your questions, and although we come out differently on whether the definition should be kept or amended, we do agree with them. We're heartened to see that they agree that they don't want to compel system modifications that degrade security for other users. And for our engineers, their view is that the building of a portal into our system is the very definition of a system modification that would impact the security for other users.

And so that is something that we would put forward as an additional amendment, for example, if you were.

DR RENWICK: That's very helpful. One of the things you're concerned about is because you operate outside Australia as well as in Australia, you might be faced with a conflict of law situation where you're required to do something in Australia which is either a crime or amounts to a civil penalty, or simply exposes you to be sued by customers overseas.

And I suppose, you know, one example might be you've got the use GDPR requirements, compared to what you're required to do there. And I suppose that can be looked at. I mean, Home Affairs do try and deal with that in their response, but I suppose you can look at it in a couple of ways: one thing is, insofar as the Schedule 1 powers have criminal sanctions for non-

compliance for the TANs and TCNs, often there is a provision saying, "You have a reasonable excuse, if," for example, "it would expose you to a criminal penalty overseas."

That can be either an absolute defence, or it can be variable, you know, it depends on the level. If you're going to get a slap on the wrist, that's one thing; if it's going to be a very severe criminal penalty, that might be another. So that's one thing I'm thinking about there.

And the other is, I suppose front-end loading it into the decision-making matrix, saying, "Well, a factor for the decision maker, the independent decision-maker to take into account is whether it will expose the particular DCP in question to criminal sanction, civil penalty in another jurisdiction." Say we're in the AAT, the DCP would put forward evidence about how that might be the case, and then you know, presumably that would be a good reason not to issue it.

It might be a reason to say, "Well, you ask for it in a different way," or, "You ask a different DCP." Because that is, I think, one of the arguments Home Affairs puts forward about the wide definition of DCPs, covering the whole supply chain. You could actually pick the one which has the least impact on privacy, or so on.

So anyway, that's broadly where I'm thinking on that, but I am sympathetic to the problem, obviously.

MR ZHANG: Well, we would welcome the ability to put that forward, pre-issuance. And also, obviously the defence, although I think the criminal defence would be somewhat incomplete, since you know, much of what we're talking about for example under GDPR are civil penalties. And you know, everyone knows the 4 per cent of turnover, annual turnover fine that is hanging over.

DR RENWICK: It gets everyone's attention.

MR ZHANG: Yes. and I think the more specific point that we made in our statement and submission is around, I think the defence being limited to only if action is taken in that foreign country; so for example, in Germany rather than in Australia. And so I think that just puts us in a very difficult situation of having to choose between two of the geographies where we're very heavily invested, and obviously upgrading.

DR RENWICK: Well, the additional point is, I think, that in an interconnected world, it's often unrealistic to say that a multinational

company like yours is only doing something in one jurisdiction; you're almost certainly reaching an agreement across boundaries.

MR ZHANG: Yes.

DR RENWICK: So I'm sympathetic to that idea as well. Just one other thing I wanted to ask you - yes, just when you were thinking further, if you wish to, about the AAT model, please keep this in mind: one of the reasons I thought the AAT might be useful in the Security Division is that the agency and the DCP both have secrets they don't want to share with the other.

I mean, take your most valuable intellectual property, your source code; you don't want to share that with an agency in Australia; the agency doesn't want to share with you the detail of a particular intelligence or police operation. And although the AAT Security Division is sometimes criticised as a matter of theory, in practice, it allows one side to put its arguments at the confidential level, and to then go outside and the other party to put their confidential arguments.

And that is something, for Constitutional reasons, you'd appreciate is a problem in a Chapter 3 court. And so it just might be that the AAT is better for this particularly unusual problem, where, as I say, you have things you don't want to tell anyone, except the independent decision-maker. So if you did want to think a little further - by all means put in a page or two extra - I'd be very grateful on that, because I do think it has the capacity to be sufficiently flexible.

And it includes the ability, as I say, to have technical people appointed as part-time members and the ability, through alternative dispute resolution before you get to the hearing, perhaps to resolve a dispute about is this or is this not a systemic weakness. You could do that. You could hive that off and have a mini arbitration before you have the hearing. It is just something worth thinking about.

MR ZHANG: We'll take that into consideration.

DR RENWICK: I'm sorry.

MS SKIPPER: I was actually just about to say thank you for raising that because it's actually something that's come up in our deliberations too about that separation of interest by those two actors and how to actually solve that. So, that is certainly on face value a very workable solution but we'll come back to you on that one as well.

DR RENWICK: Yes, I think that's right. I've got on board your idea about your staff engineers, and this is often a DCP concern, thinking they're personally going to be targeted. You've seen from Home Affairs that's not their intent but if that can be clarified in the legislation, that seems sensible. Certainly, I think the law should make clear that the DCP is entitled to get both legal and technical advice in relation to a demand. That should go without saying, but if it doesn't go without saying, then it should be there.

I'm conscious of the time. Is there anything else, Mark?

MR MOONEY: No, no.

DR RENWICK: Did you want to say anything else? Have you covered all the things you wanted to cover? I mean if there are more things to cover or you wish to put in a short supplementary document, I welcome that. I don't want to cut you off if there are other things you want to cover.

MS SKIPPER: I think we're okay. We will take the opportunity to put in a short supplementary couple of points based on this and some of the specific considerations that Patrick, in particular, has given to some amendments around language, so we'll put that in writing to you.

DR RENWICK: Just for completeness, Mr Zhang, I assume that you were here I think when Internet Australia gave their evidence.

MR ZHANG: Yes.

DR RENWICK: I take it you'd agree with the idea that assuming TCNs are not being used at the minute, that this is a good time for Home Affairs to sit down with the industry and work out how a TCN might or might not work.

MR ZHANG: Absolutely, yes. We would appreciate that as a very wise decision.

DR RENWICK: You'd be happy to participate in that process, I imagine?

MR ZHANG: Absolutely, yes.

DR RENWICK: All right then. Well look, as I say, for those of you who travelled a very long way or a very short way, thank you all, and thank you for your most thoughtful submission.

MR ZHANG: Thank you.

MS SKIPPER: Thank you.

DR RENWICK: May I invite forward the Access Now representative. Good afternoon. Can you identify yourself for the transcript and make any opening statements you would like to make.

#SESSION 3: Access Now

MS KRAHULCOVA: Good afternoon, my name is Lucie Krahulcova and I am a policy analyst with Access Now, currently working in Australia and the Asia Pacific. Previously I was based in Brussels for the same organisation for several years. I apologise for rudely having my laptop here, but just in case we want to jump through some sections of the Act, I wanted to be ready.

I do have a couple of opening remarks. I didn't want to necessarily repeat what was in our many submissions. I think we made five to the parliamentary process. So, I took the liberty of jotting down some responses to what was already discussed which I think will be most pertinent to what you're thinking through at the moment.

First of all, I wanted to say a big thank you for the effort and engagement that you've put in to looking through this. I know this is a complex topic. It bears the weight of 50 years of regulatory back-and-forth, so that's not something to be understated. I wanted to thank the staff who are working with you for being wonderful and engaging and extremely responsive.

I think one of the things that has come up today extensively has been how do we measure the necessity and proportionality test. I think the interesting part about this inquiry is that we're already debating the terms that are set forward by the legislation and I think we haven't quite established that this legislation is where the necessity of proportionality of what Australian law enforcement needs at the moment should land.

In 2018 when we were consulted initially on the Bill, as it were, there was still a discussion over whether a legislation that's targeting encryption explicitly is what's needed or whether there are other means to achieve that aim.

I would point to, because you did reference several different sources of reading, to Orin Kerr and Bruce Schneier's paper on encryption workarounds that was published in 2017 where they present several different options for obtaining evidence that is traditionally encrypted in

transit, therefore, interfering with the potential capability to intercept that communication.

DR RENWICK: Just pausing there. You can give us a copy.

MS KRAHULCOVA: I can give you a copy. Great, I would love that.

DR RENWICK: That's great. Thank you.

MS KRAHULCOVA: I would question the whole notion that this is the correct response and that it is proportional to the issue that's posed by encryption, which it definitely is. I've had this conversation with law enforcement in Europe as well, but there are other ways to circumvent it. There are times when that information is not encrypted on the devices. There are still other surveillance means and mechanisms that I have not been convinced have been exhausted in the drafting of this legislation.

That's just the place setting and I think it's worthy to talk about also because when we have these conversations at the European level, there was a real balance between the technical community, the law enforcement community and the individual capacities of the member state because they retain intelligence agency oversight that's separate. I think that balance hadn't been achieved when this was discussed in Australia, and I think that's where the whole conversation for me is skewed. So, I am happy to discuss the necessity and proportionality of the individual measures, but I think it merits attention the way this whole text is framed.

Sorry, I'm conscious I don't want to take up the whole time with my remarks.

DR RENWICK: No, no, it's very helpful.

MS KRAHULCOVA: So far I'm fine. Okay. I also think there's a real disproportionate focus on the government company relationship in this discussion. Today we focus a lot on how companies can respond and work with law enforcement and for me there's a real lack of the emphasis on the individual rights, both in the text as it stands in this and the parliamentary joint committee inquiry.

DR RENWICK: By which, for example, do you mean customers of DCPs and their rights to privacy and security?

MS KRAHULCOVA: Absolutely, but also the relationship of individuals with the State. We're talking about law enforcement and intelligence agencies but the State is also a guarantor of rights for the individual, and

because there's no direct access to remedy or redress for the individual, I think that relationship has been harmed. I will give you an example that was discussed extensively today.

DR RENWICK: Sorry, just to pause there. You mean that particularly in a case where the powers are exercised in a way unknown to the individual.

MS KRAHULCOVA: Yes.

DR RENWICK: I mean there are some powers by the police or the Border Force where the person will know because they have been told to provide their passwords.

MS KRAHULCOVA: Yes, absolutely.

DR RENWICK: But you're not talking about that.

MS KRAHULCOVA: No.

DR RENWICK: You're talking about where you don't find out about it.

MR KRAHULCOVA: Yes, correct, and I think if you used the example of the Notebook, you would probably notice if someone took your Notebook. You're not going to notice if you're surveilled whether it's through TCN or a TAN. I think that removes the responsibility and one of the key fragments of this is that the Act removes the right that I have to sue the DCP in this case. For an individual on an individual front, that's the one sort of tool that an individual would have to assert their rights in this space.

So, by removing that and saying the company can't be sued, well who has violated my rights then because I had a covenant with the company. There is a contract that they broke and I'm not allowed to sue them and there's no traceability and adequate reporting from the law enforcement side for me to understand where my rights were compromised, so that's what I mean.

DR RENWICK: Interestingly, the Inspector-General of Intelligence and Security in her evidence made the comment about the immunity, that if you give someone an immunity, you are taking away someone else's rights.

MS KRAHULCOVA: Yes.

DR RENWICK: That's really the point, isn't it?

MS KRAHULCOVA: Yes.

DR RENWICK: I suppose that's particularly relevant for the TARs, even though the company and the government may agree, that's not the end of the argument because the individual's rights, the individual doesn't have a seat at that table.

MS KRAHULCOVA: Exactly, and I think that's one of my issues with the reporting. You mentioned several times today, is it enough if they say we've received no requests or we've received this many requests. I mean that sort of reporting is immaterial to the user. As a user of Microsoft or Facebook, or whatever it is, I may look at that information and think somebody got served. But it does very little to me because there's really no notification at any point that I was targeted by one of these measures, any of them.

I think that's something that should be changed when we definitely should have judicial approval for all these things and we can get to that but, absolutely, people should be notified. Once the measure is completed, the person who was targeted by that measure should have a right to understand why they were targeted, for what length of time, and which agency was responsible. This is a fundamental right that people should be able to exercise as citizens of Australia, subject to law enforcement and intelligence agencies.

DR RENWICK: Just to unpick that a bit. I'm running a police operation. I'm trying to focus on which of these 50 people might have sent an illegal email. So, I need to look at something about all 50 to eliminate people.

MS KRAHULCOVA: Yes.

DR RENWICK: Do you really mean that the 49 people who need to be surveilled in some small way perhaps to be eliminated. All need to be notified or are you talking really - - -

MS KRAHULCOVA: Absolutely, all should be notified.

DR RENWICK: What country does that now?

MS KRAHULCOVA: No country does this. Generally, no country has this sort of access at the moment.

DR RENWICK: No. Sorry, to cut across you. What I meant was if you're talking about, as a general principle, covert surveillance must always be notified to the people surveilled, can you give me an example of where there is that universal access at some point?

MS KRAHULCOVA: I can't off the top of my head but I could come back on that point, because we've seen different iterations or it in different legislatures.

DR RENWICK: Yes, that would be helpful. I mean after all, if you end being prosecuted as a result, if you're the one out of the 50 and you're prosecuted, you find out at that stage and you've got your rights in the criminal trial.

MS KRAHULCOVA: Yes. I think there's an interesting intersection here with the metadata inquiry which was raised several times today.

DR RENWICK: Yes.

MS KRAHULCOVA: In that inquiry we heard last Friday, that law enforcement agencies, and I'm sorry I can't attribute appropriately who said it – I could come back on that point as well – but they keep data. They retain data that they obtain through warrants, even when the investigation is done, because they can use it in future investigations.

I think the overlap, given that, is the sort of – I'm confused where I was going with the overlap for the metadata. Sorry, I lost my train of thought.

DR RENWICK: No, that's okay. Can I perhaps go back to the first point you made, which is necessity and proportionality of the original measures.

MS KRAHULCOVA: Yes.

DR RENWICK: Do you have the listed Act or things in 317E in front of you, and if not we can provide you with one?

MS KRAHULCOVA: Yes.

DR RENWICK: A point which is often made to me on the government side in this inquiry is it's not really a Decryption Act, it's making content particularly intelligible or accessible. So, just looking at the listed Act or things, and I appreciate it's a long list, can I just ask you to say a bit more about why you suggested a minute ago that the necessity or proportionality of these matters has not been established?

MS KRAHULCOVA: Yes. So, I think when we're evaluating necessity and proportionality we made in one of our submissions I think a recommendation of what the language should look like on the qualifiers. I'm happy to pull that out and highlight it to you in another document.

DR RENWICK: Yes, that would be great.

MS KRAHULCOVA: One of the things I struggle with, for instance, for technical capability notices is that the necessity and proportionality test that's prescribed by legislation doesn't take into consideration potential adverse impacts on the technical eco system.

DR RENWICK: On the what?

MS KRAHULCOVA: On the actual digital eco system. It doesn't take into account potential adverse impacts of the measures.

DR RENWICK: I'm sorry to be tedious, but what do you mean by the technical eco system?

MS KRAHULCOVA: Did you mean the internet more generally?

MR MOONEY: The internet more broadly. The security of the internet.

MS KRAHULCOVA: Yes. I think that goes back to what others were saying prior regarding the sort of nature and unpredictability of what TCNs could potentially do and broader damage. I think that it's a shame that that's not a part of the weighting mechanism when we evaluate these TCNs.

MR MOONEY: That should be a factor in deciding whether or not something amounts to a systemic risk or vulnerability.

MS KRAHULCOVA: I think fundamentally TCNs are not compatible with human rights law. I don't think they can be necessary and proportionate because of the fragile nature of the internet infrastructure, but yes, if they are to remain and again, we have defended for a repeal of this legislation or strong amendments. If they are to remain, I think that should be a part of the necessity and proportionality test.

DR RENWICK: That's a pretty broad statement. I mean some of the things done by TCNs can be done by companies themselves from time to time when they want monetise our personal information.

MS KRAHULCOVA: Yes.

DR RENWICK: I mean do you say that's equally something which is contrary to human rights?

MS KRAHULCOVA: Yes, and a lot of our work actually focuses on having this discussion with companies. We have a transparency reporting

index where we track a lot of this and hold them accountable as well. I think a big issue here and it's good that I can circle back, but there is an issue in digital rights that we call privatised enforcement that's really compounded by this legislation. That's the State relying on private actors and companies to do their work in investigations and facilitating their work.

I just want to draw your attention to the new Attorney-General's opinion from the Court of Justice of the EU, case C623/17; it's Privacy International versus the Investigatory Powers Act on Data Retention. It came out mid-January, which is why it's not in any of our documents. Even though it deals with data retention - - -

DR RENWICK: Sorry, you can send a copy of that through to us?

MS KRAHULCOVA: Absolutely.

DR RENWICK: Thank you.

MS KRAHULCOVA: I'm excited. You're going to get a dossier at this point. Even though that deals with data retention, I think the two things are incredibly intertwined. The Attorney-General concludes that a national security doesn't prevail over the data protection rights that Europeans have. So, the national security justification isn't sufficient enough to back this legislation, and second, that the law enforcement and intelligence agencies shouldn't rely on private communicators, DCPs in this context, to provide them with privileged access in their investigations. It is not the role of companies to do that.

DR RENWICK: Isn't that very much dependent on the terms of the GDPR, which we don't have?

MS KRAHULCOVA: It is not dependent on the terms of the GDPR. What they're basing their assessment on is actually the 2002 ePrivacy Directive which ensures privacy of communications. So, in Europe there are two separate rights. There is the right to data protection which is governed by the GDPR and actually the police director in instances like this, which has separate rules from the GDPR. Then there's the ePrivacy Directive which separately deals with our right to privacy and that's what they're referring to.

DR RENWICK: We don't have that either, do we?

MS KRAHULCOVA: Absolutely not, but I think the international context here is important, both in terms of the requirements that the US is going to make under the US CLOUD Act and potentially any future communication

of that sort with the UK or EU level. This is something that you're going to have to come back to.

DR RENWICK: Can I ask you to look at section 31, seeing we're talking about TCNs, 317ZAA, which is whether the requirements imposed by a TCN are reasonable or proportionate.

MS KRAHULCOVA: Yes.

DR RENWICK: I appreciate you may want to say this should be varied but this does require the Attorney-General to have regard to a whole lot of factors, not just national security and law enforcement, but (E) the availability of other means to achieve the objectives; (EA) whether the requirements are the least intrusive for the persons who are not of interest; whether they are necessary, and the legitimate expectations relating to privacy and cybersecurity. In other words, proportionality and necessity are built in to the decision-making criteria here, aren't they?

MS KRAHULCOVA: I don't think so, not sufficiently, and as I mentioned the one example of, for instance, the potential impact technically of that measure is not weighed.

DR RENWICK: I'm sorry, the potential impact is what?

MS KRAHULCOVA: The technical impact of what the TCN seeks to do is not weighed in the decision making. I don't think that would fall under Australian reasonable expectation of privacy in cybersecurity.

DR RENWICK: The TCN is a case where – yes, so if you look at section 317TAAA which requires the Attorney must consult with the Minister for Communications, and in subsection 6 you've got to consider 6C, the impact on the efficiency and international competitiveness of the Australian telecommunications industry and the interests of the DCP. You say what's missing is a reference to a customer whose personal privacy is being affected.

MS KRAHULCOVA: This is a commercial consideration. I think there's a technical consideration that needs to be made. In our submissions we actually noted for TCNs there should be a specific sort of multi stakeholder assessment group with certain cybersecurity professionals, engineers, because you can definitely consider necessity and proportionality from the legal terms but you can't in that case weigh it on the technical side.

DR RENWICK: There's two parts of that.

MS KRAHULCOVA: Yes.

DR RENWICK: There's one, what the legal requirements are, and there's second, who the decision maker should be and what their qualifications are. Have I got that right?

MS KRAHULCOVA: Well, legally someone needs to validate it but technically someone should be consulted.

DR RENWICK: In other words, the idea of having say a lawyer sitting with a technical expert jointly being the decision makers?

MS KRAHULCOVA: Perhaps, I think we suggested an assessment board that would have several different members.

DR RENWICK: All right. Thank you. Of course, I accept that the local risks to digital security is something that is obviously important and you heard what Mr Burgess said this morning, that that's the last thing they want to impact.

MS KRAHULCOVA: Yes. I mean obviously they would say that. I think the issue is a little bit that this Act is circumventing a bigger more nuanced conversation about TCNs. For instance, in other jurisdictions they would have drafted vulnerabilities, equities processes or something like that, that weighs the actual technical impact, the potential technical impact versus the national security utility of the vulnerability or systemic weakness or whatever Act or thing under this jurisdiction and that's missing. There's not a weighing mechanism that I think is comparable to the way the UK or the US are looking at these issues at the moment.

DR RENWICK: When you talk about the UK, are you talking about the IPCO model or something else?

MS KRAHULCOVA: The what model?

DR RENWICK: The Investigatory Powers Commissioner's Model?

MS KRAHULCOVA: Yes.

DR RENWICK: I see.

MS KRAHULCOVA: GCHQ, to supplement that, has released the vulnerabilities equities process.

DR RENWICK: Right. So, what we should look at, in particular, is the requirement to weigh up the impact on digital security, (a), and the impact on the privacy of the individual, (b).

MS KRAHULCOVA: Yes.

DR RENWICK: They're the key focuses of that last point you've made.

MS KRAHULCOVA: Yes.

DR RENWICK: Okay. Thank you. Can I just say for those who may be listening that I don't think the Minister for Communications can be regarded as a double lock in the sense of the UK double lock. It's no reflection, of course, on any individual person, but the Minister for Communications and the Attorney-General are both members of the same cabinet and so that's not a double lock in the UK sense. Yes, sorry, any additional points?

MS KRAHULCOVA: I think we kind of jumped through my remarks that I wanted to say at the beginning but just to kind of close up, we did talk a little bit about the CLOUD Act, putting pressure on some of these things to be remedied in the text. My job is to think internationally in that context and I just want to sort of point out the precedent this is setting internationally.

When I look at a Bill like this and when we, as international NGOs, look at a Bill like this, we think what safeguards we would want there to be in some of the adversarial countries. I think we have to draft our legislation with that in mind, (a) because the legislation ends up being copied and pasted in different jurisdictions, but (b) because I think if you want to retain international credibility for your own foreign policy and your own foreign national security interests, you have to show that your money is kind of where your mouth is on that topic.

I think the way that some of these legislations, not just this one, whether it was in Brazil or elsewhere, where we harpoon specific people at the companies, it sets a precedent where I think you're putting Australians who work in the tech sector ultimately at risk in other jurisdictions, because once other jurisdictions start imposing similar requirements and being able to similarly target individuals, we're going to have a repeat of what happened in Brazil where they arrested the entire sort of admin of WhatsApp and held them accountable to having access to WhatsApp messages.

Just as a cautionary tale, I would say we can't just consider this in the Australian framework and we should because there are certain safeguards

that are missing. As you say there's no GDPR, but moreover, there's no affirmative right to privacy and there's no affirmative right to data protection. So, even a judicial review I think is slightly crippled by that fact and I think that's probably going to come back with any negotiations with the EU or UK, which is still going to be subject to the UACI at large.

On that super-optimistic note, I may well end my remarks.

DR RENWICK: Can I say I found that incredibly helpful and thoughtful and I am required to have considered international obligations as well as domestic ones. If you do have any further documents or any further points, I do urge you to send them through soon. Thank you so much.

MS KRAHULCOVA: Thank you so much for your time.

DR RENWICK: Now I invite Martin Thomson, distinguished engineer from Mozilla Corporation to come forward. Mr Thomson, welcome. Did you have an opening statement you wish to make?

#SESSION 3: Mozilla Corporation

MR THOMSON: Thank you, yes. I should point out, I'm an engineer. I don't do this sort of thing for a living. It's probably my second time in any one of these circumstances, so be kind. I am also a member of the Internet Architecture Board, but I am not speaking on their behalf today. I represent Mozilla.

The internet was built without any semblance of security in the first place and so the early internet relied on trust and cooperation. Today, it's not really enough to trust that others share our goals. There are just far too many people and far too diverse interests. Instead, what we have done is we have developed systems that safeguard our online activities and trust in those systems is crucial to the function of the internet as a whole. There are a lot of interlocking systems and they're very tightly covered in a lot of cases.

It might help you to give just a very small example of one of the things that we're talking about. Mozilla builds a password manager into our Firefox browser. We remember the login details that you use on websites so that you don't have to and this makes passwords better. It makes everyone safer on line, and we store those passwords online so that you can take them from your phone to your computer and back and forth, without having to remember them or copy them across, and subject to all those sorts of risks.

No one has to worry so much about having hundreds of passwords written on little pieces of paper hidden around the house sort of thing.

This is really sensitive information, and likely quite valuable to criminals, and probably very valuable in the case of a criminal investigation as well. So we apply multiple defences for this information. We encrypt the information when we store it on your device, we encrypt the information before it even goes onto our online services where we retain the information, and we don't have access to that information. We take steps to make sure that we can't access that information directly ourselves simply by finding that golden key that you were talking about before and using that, that's just not at all possible by design. And we know that our reputation depends to a great extent on us doing that.

So that sounds impressive, but if you take a step back and look at the overall system, the fact remains that when you run Firefox, you give it your passwords. And we built Firefox. So at some level, you're giving us your passwords. So it's basically functionally indistinguishable from a system where we didn't encrypt the information that we stored on your hard drive, we didn't encrypt the information that we stored in our online services.

What we have instead - by the way, not offering to build a copy of Firefox that would do any of that, that would be a gross violation of the trust that our users place in us. So we're acutely aware of the fact that this possibility exists, and so we create systems and processes and procedures to stop ourselves from doing any of those things accidentally, or maybe an employee who's malcontent for some reason, from accessing those sorts of things.

And it's a really difficult problem. The software supply chain that we deal in has a lot of moving parts, and a vulnerability at any one of those stages in the process can mean a vulnerability that is distributed to hundreds of millions of people. Some people point out that open-sourcing our software might be a way that people might be able to trust that our code is safe. That's not foolproof, which is why we're investing in new technologies which make the whole process much more rigorous and have much higher integrity.

So that example sounds unique, but it's exactly the same thing that applies to other applications as well. The messaging application that uses end-to end-encryption is, at least a high level, not that much different to our password manager. Fundamentally, all the systems that use data will have access to data in some way. So when data is available to the system, it's available at some points in certain cases.

And so companies and organisations use encryption as a tool to ensure that only those times when the information is needed, and to those persons that need that access, the information is available. So we then build defences, layers and layers of defences around that to safeguard that information.

So as someone who has dedicated their career to strengthening the system, one of the most problematic aspects of this legislation is the potential for the Australian government or law enforcement agencies to order the development of new capabilities in secret. The legislation imposes penalties - harsh penalties, for even discussing orders. Meaning that the scope and effective changes can't be known to the public and can't be known to the people who defend these systems. The systems go beyond just individual companies in a lot of cases, particularly if the system is the Mozilla (indistinct).

So the intent may be to make discreet changes, the effect on the interconnected system is very hard to predict. In our example, the password manager, in order to develop and deliver modified software is an attack on the system designed to prevent just that. Even the potential for an order to be given affects trust in software updates which people rely on for security patches and features, and these sorts of interventions deeply damage trust in others, in the government, in our partners and employees. I think we've addressed the employees point fairly adequately already today.

So in filings with the PJCIS and yourself, Mozilla has outlined ways that might reduce the negative effects of this. We've talked about some of those, particular judicial review and the effects of TCNs. I think we'll probably dive a little deeper into the TCNs here.

But I should be clear. Mozilla would prefer that TOLA be repealed. Declarations of intent to avoid systemic weakness or vulnerability are meaningless when the legislation grants the ability to force communications providers to circumvent security protections in secret. We'd prefer that the Australian government instead do as we've seen other governments do and help strengthen the systems that protect people online.

DR RENWICK: So to be clear then, you're talking particularly in TCN territory?

MR THOMSON: Yes, so TCNs are really the most concerning thing, and it's probably worth an anecdote on this one.

DR RENWICK: Sure.

MR THOMSON: So Google's deployed new security protocol across the internet, and they've been experimenting on this probably for almost 10 years now. And the early stages of this was entirely a private experiment, and they had some teams of very experienced engineers with lots of background in this area. And they developed a new security protocol. Very difficult task.

And they were quite happy with it, and thought it met their expectations. But then we were discussing the adaptation of this into a more standardised form, and had someone say, "What about this?" and everyone sat there for a moment and thought about that. And I realised that all along, one of the primary security guarantees that they thought they had got out of this system did not exist.

This is something that had been under the eyes of academics and engineers and people who have lots and lots of experience in dealing with these problems for years, and we then all realised that fundamentally what they thought they were able to do was impossible.

And when we talk about building TCNs and the risk management profile that we have around that, doing them in secret is the complete opposite of everything that we've strived to do in making the internet more secure. Having one person who has technical expertise and background examine this helps. It helps if that person has the right sort of adversarial mindset. That is, they set out to look for those weaknesses. And that's a skill that we train in, and it's something that we develop. Unfortunately we don't have very good tools around those sorts of things, but we're seeing that the academic community is producing that.

But it really requires a community to ensure that the systems that we build are safe against the diverse sets of threats that we're worried about, and they are diverse. And you talked about this earlier when you were talking about the breadth of communications providers that can be asked to provide assistance. That in many respects is reflective of the fact that when you're trying to defend something, there are lots of points of ingress, and you have to defend all of them, otherwise your adversary will find the one that you haven't defended in order to attack it.

And this is, if take the cynical view, the way that the Bill is structured, intentionally. It says, "We don't know what the system will look like, we don't know how it will be structured, but we will find a way to attack that system by whatever means possible."

DR RENWICK: Sure, so let's just take then the example of your own company - and I mean, I'm not particularly familiar with what you've

described, but as I understand it, you have built into your search engine you use on your computer, say, you are able to input all your passwords for the websites that you visit?

MR THOMSON: Yes, that's right.

DR RENWICK: And you have designed it in such a way that you are not able to access the passwords, they're stored in some encrypted fashion?

MR THOMSON: That's right.

DR RENWICK: Which are available only to a person who is sitting on that device who has logged in as themselves, presumably?

MR THOMSON: Right. And so the intent there is not to say, "Well, this is the only protection that we have in place." It's part of an entire system of protections.

DR RENWICK: Sure.

MR THOMSON: And the realisation is that we don't believe that we can trust ourselves with passwords for hundreds of millions of people.

DR RENWICK: Sure.

MR THOMSON: Therefore we will do what we can to remove that capability from - temptation, if you will. And put in layers of protection. And that's just one of the layers of protection that we have, there are numerous other ones.

DR RENWICK: And so to take that just as the way of an example - if I come along to you and say, "Well I'd like you to break that," and you say, "Well it's not designed to do that, and if I were to break it, hypothetically I would break it for everybody."

MR THOMSON: That would be probably one of the responses that we'd have in that case, yes.

DR RENWICK: And in that, just to take that hypothetical case, that would be the classic definition of a systemic weakness or vulnerability, because it would affect a whole class of technology. And that would be - just working through this hypothesis, I think - and we'll hear from Home Affairs tomorrow, I suspect they would say, "Well, we just could not do it."

MR THOMSON: It's interesting, because fundamentally there are a number of technical challenges involved, but it may be possible to circumvent these systems such that only one of the people at the table opposite me were affected. The question is cost, complexity, risk, all of those sorts of things, and managing risk in this environment is really what this is all about. And so it's not a black and white decision, you don't simply say yes or no, "This is safe," or, "This is not safe," it's the profiled risk that's associated with any one of these actions.

If you phrase the question as simply as you just did, then obviously the response will be that if we want to modify that system such that we would have access to that information. That would jeopardise the information of hundreds of millions of people. And so yes, under the terms of the legislation, that would be dangerous.

But there are other types of modification that might be requested that may have much less clear answers, and that's the sort of thing that is very unclear in this process, and the secrecy tends to compound that problem.

DR RENWICK: I mean, if they were to approach it another way anticipating that sort of response, I suppose they would also point to the legitimate interests of the DCP to which the notice relates, and you would say, as I understand it, that this is so fundamental to your business model that if this got out, this would ruin the reputation of your business model? In other words, it would have a disastrous effect on the legitimate interests of you as a DCP, and that would be a highly relevant reason never to order it, particularly if it was to be done under the model I've suggested, by an independent judge or an independent tribunal member, as opposed to the Attorney-General?

MR THOMSON: So that's an interesting point in that. You're almost saying then that there may be in this particular case - and there might be no conceivable way for a TCN to be issued to someone without creating that risk. And I think that's consistent with what we've said previously, in that we cannot see any way for TCNs to even exist without damaging the reputation of DCPs. And that's the challenge, right? There's a gap there somewhere.

DR RENWICK: But, if I may say so, as a non-technical person, let's just jump from the Mozilla example to all TCNs cause problems with all DCPs, and that's not necessarily right, surely.

MR THOMSON: That's the gap that I'm concerned about. I don't know what the answer is for other DCPs. Mozilla is in a bit of a unique position in that we operate open source. Imagine before source code as being

valuable intellectual property - we don't regard source code to be valuable intellectual property.

DR RENWICK: But that's an unusual approach, right?

MR THOMSON: No.

DR RENWICK: Or is it - - -

MR THOMSON: This is not at all unusual. To take a large example, Google operates a lot of source code, and a very large proportion of what they produce they do in public.

DR RENWICK: Okay.

MR THOMSON: And the same is increasingly true of other companies as well, a lot of the way the internet is built is built on open systems and software for it.

DR RENWICK: Okay, just to go back to the example again in the section - just for the purpose of the argument, one of the other things you've got to take into account is the availability of other means to achieve the objectives of the notice. So again, just using this hypothetical example, if there was a way that I, as the government agency, could in effect sit behind or next to the person, the individual who's signed in, surreptitiously mirror their copy of their device, and see what their password is, then presumably I'd be in the same position as the user to use that. And that would be, on that hypothesis, another means to achieve the objective of the notice, which would only impact upon the target.

MR THOMSON: How would you guarantee that you were only sitting behind that person? So it's an interesting example, and we see a number of cases where you say, "Okay, so Mozilla is not able to comply for various reasons, so we'll go to somewhere else, the vendor of the operating system or the vendor of the hardware of the machine, or maybe the keyboard manufacturer." We can talk to the keyboard manufacturer, and they'll tell us all the keystrokes that went into that keyboard. How do you guarantee that that goes to one person? All those questions.

DR RENWICK: I was actually thinking a much less technically-advanced idea under say, Schedule 2 of *TOLA*, which allows you to get a remote computer access warrant. So let's assume by means unknown you can remotely hop into your mobile, image it and then maybe in an old fashioned way by putting a camera behind you, read your password. All I'm saying by way of that example is that it's possible to use your example of thinking

of a number of reasons why no reasonable decision-maker could say you've got to force Mozilla to change its operating model.

MR THOMSON: Yes, I guess my point was that once you shift to some other way of approaching the problem, now we've started to really address the question of whether talking to DCPs is the right answer for investigations.

DR RENWICK: That's a good point. That's a fair point.

MR THOMSON: One of the classic statements from someone in the business a long time ago was we don't bother trying to break encryption, we look for all of the other - exhaust all of the other alternatives first, bribery and blackmail and bludgeoning and all of those other wonderful things.

DR RENWICK: I see, all right. The definition of systemic weakness and systemic vulnerability, is there anything you wanted to say about them?

MR THOMSON: I think I've already said that.

DR RENWICK: Did you have anything further?

MR THOMSON: I think they're fundamentally at odds with the ability - in the legislation to ask a DCP to modify how they operate. And - - -

DR RENWICK: In other words that's - sorry to interrupt, that's focused on the TCN, the creation of a new capacity. If you're talking though about an existing capacity, then did you have any remarks to make about systemic weakness or vulnerability?

MR THOMSON: Not in that context, because I believe that the systemic vulnerability or weakness already exists at the point that that information is available. And from my perspective, if I ever had access to any one of the many millions of people who use Firefox, any of their private browsing information or passwords, to give the former example, that would be a problem in the system that I'm responsible for overseeing. I don't want to ever have that situation exist. I know that other companies do set out to have access to that information, so I don't see it making the situation worse.

DR RENWICK: Sure. Looking at this from an internationally-comparative point of view, the previous speaker made some powerful points about that. Mozilla is a worldwide - operates worldwide, can you point me to any other similar laws around the world?

MR THOMSON: The ones that I'm aware of are the ones that you're likely aware of. I think the *Investigatory Powers Act* in the UK is probably the most similar to this one. You're asking me for information that I'm not an expert on.

DR RENWICK: That's all right.

MR THOMSON: The Indian government has recently passed the intermediary Bill, and there are a number of things that exist, none of them quite like this one. Everywhere is different.

DR RENWICK: Yes, indeed. Anything else? Well that's given us a lot of food for thought. Just one question - and you may not want to answer this, but I raised with the last group the definitions contained in the current Bill, and I'll just read it out:

> *Implementing or building a systemic weakness or vulnerability includes anything that would or may create material risk that otherwise secure information would or may in the future be accessed, used and so on.*

And you may remember my express concern is, is that a wholly unrealistic standard because couldn't that apply to anything? In other words, couldn't you put the words 'will' rather than 'would' or 'may' create a material risk if you wanted a standard which isn't failed every time?

MR THOMSON: This is one of those areas where it's very difficult to know the totality of the effects of any change.

DR RENWICK: Right.

MR THOMSON: And so this is why I talked previously about having wide review of things, involvement from academia and other parts of industry in these decisions, because you make an assessment based on the information that you have at hand, and a lot of the things that we're attempting to do in the industry right now are subject to - effectively they're open research topics, we don't know the effects of them, we don't know how to deal with them, we have for instance cryptographers out there trying to work out how to build systems that are stronger in the face of quantum computers coming along, those sorts of situations are very fluid, and at any point in time you can only really make an assessment based on the knowledge that you have and the experience that you have, and it's a risk assessment more than anything else. I think Keith Besgrove mentioned that probably the best

previously.

And I read that as saying - although it may not be very clearly worded, as saying that in the assessment of those making a decision - this is where the (indistinct) of those involved matter, the risk now and the risk in the future of this change is acceptable. And so we're making a prediction at that point, but we're making a prediction based on what we know and what we understand to be the case, and how we expect the system to operate.

That's not what it says in the words that it says, but that's how I think the intent should be expressed. Unfortunately I can't give you a better answer than that, because they're (indistinct).

DR RENWICK: No, no. But thank you, that's most helpful. I mean, it's one of the reasons why the best I can come up with in terms of a system which is independent and which keeps up to date technically is to have some examples in TOLA which say what is and what isn't acceptable, and secondly to have the independent judge-type person, whether they are serving or not, assisted by an expert or experts who have experience both in government and in industry - and I appreciate there aren't a huge number of them. But in the UK, there are some - I met some of the incredibly impressive technical advisors who were available part-time to assist the judicial commissioners, and then it just seems to me at least then the lawyer in the middle - as in our system we do end up with lawyers in the middle, is at least technically well-informed about what it all means, because the thing I find hardest in this whole inquiry is - you know, a lot of the debate is up here as a matter of theory - and then you get down to, "Well, is there an adequate alternative way of doing it?" and I just gave you an example just as a layperson who thought, "Well maybe this is another way of doing it," maybe there's good reasons why you couldn't do that.

So that's why I'm thinking the independent lawyer with the technical advisors, and with the benefit of hearing in the system we're familiar with, with the government on one side and the DCPs on the other, and to take the point made by the last speaker, maybe there should be a public interest advocate who speaks on behalf of the customer.

MR THOMSON: We'd like that.

DR RENWICK: So they also have a seat at the table, metaphorically at least, if not actually. I just can't think of anything better than that at the minute, assuming you are to retain the TCNs, and I know your starting point is just get rid of them.

MR THOMSON: So the starting point may be just get rid of them, but I

can think of something better than that, and this has come up in our submissions as well.

DR RENWICK: Yes.

MR THOMSON: We recognise that when it comes to TANs and TARs, the operational details that are involved are often highly-sensitive, and so secrecy is almost a crucial component of those things, and I think others have talked about the time limits on secrecy, and we sort of agree with those comments as well. At some point in the future, it would be very nice if there was some accountability to the public for those things.

But laying that aside, the TCNs, there can never be any operational urgency involved in delivering a TCN. The review periods along mean that investigations will likely have moved on by the time that the process even starts. Periods of notice and negotiation and review and all those sorts of things.

DR RENWICK: Well let me give you - I can assure you, hypothetical example. But let's assume that an intelligence agency has a long-term interest in a particular terrorist group. It might be a slight overstatement to say you know, you're never going to be able to use things. I mean, if you've got a 10-year interest in Al-Qaeda for example, well okay, it may be great if we have it today, but it may still be useful if you have it next year.

MR THOMSON: And I the question, I guess then, comes down to whether the public has any interest in knowing that that capability exists, and whether the agency in question can be more strategic in the way that they develop those capabilities, such that their interests aren't exposed, or their particular avenues of investigation are not exposed.

DR RENWICK: So that's particularly focusing on what the public is being told about what's happened. So to be precise, what's your concern in that instance?

MR THOMSON: The concern here is that the capabilities are developed in secret without any knowledge of the public, and so given the nature of the systems that we have and the extent of the powers that are involved, we don't know now what the government is capable of doing, and there are no checks on the power of the government to ask these things. Independent review goes a long way to ensuring that sort of thing, but it doesn't mean that the government is then accountable for those decisions.

DR RENWICK: Well, can I just unpick that? I mean, you know the four corners of what's permissible, because the Act tells you what is and isn't

allowed.

MR THOMSON: In theory of course, yes.

DR RENWICK: No, no, no, I understand. But you've got the IGIS and the Ombudsman who actually audit it and so on. But going back to your earlier premise about, "We don't know what the government can do", couldn't that easily also be said about Joe Public, including myself, I haven't got a clue what most of the app manufacturers on my phone do with my personal information? I mean, you'd agree with that, wouldn't you?

MR THOMSON: I'd certainly agree with that, and I personally - and I think Mozilla is extremely concerned about the extent to which private enterprise and other corporations have accessed private information and what they use it for. Some of these uses are quite abusive in fact.

DR RENWICK: But that in a sense is a given for my inquiry, that the world wide web is always going to have a lot of DCPs who do stuff, one hopes, covered by the terms and conditions of carriage, to which we all click I agree without reading, but I accept possibly beyond those - that that's the world in which we live, we have all of that happening all of the time in a way which in truth is unknowable by the member of the public. Isn't that right?

MR THOMSON: But would you not hold the government to a higher standard than an arbitrary - - -

DR RENWICK: No, no, I understand. I was just focusing on your earlier - if what you were earlier suggesting is that it's only the government we don't know what they're doing, I mean my point is that in the world of the world wide web, the truth is Joe Public has got no idea what is done with my personal information, and probably no real way of finding out. And that's part of the fabric, isn't it?

MR THOMSON: That is the context in which we exist, but if we don't hold the government to a higher standard in this regard, I think we're completely unable to hold private enterprise to those standards. And we need to be holding private enterprise to a higher standard as well.

DR RENWICK: But I suppose - and particularly - just to finish on this, it particularly comes up in this way. If there's all that existing knowledge, existing analysis to which I hopefully have agreed, but not in an informed way because it's impossible for me to give informed consent, there's already a vast amount of information which can be got under a TAR or a TAN, isn't there?

MR THOMSON: Currently yes, yes. And if you're suggesting then that the need for TCNs is diminished in this context, then that may be the case.

DR RENWICK: Well I found that incredibly interesting, thank you.

MR THOMSON: Thank you.

DR RENWICK: Anything further? Thank you for your patience with my non-technical questions. We will now break for a vast afternoon tea, and we will come back at 3.20, thank you.

ADJOURNED [1502]

RESUMED [1521]

#SESSION 4: Communications Alliance, Ai Group, AIIA, AMTA, DIGI and ITPA

DR RENWICK: Ladies and gentlemen, welcome back and we move to the final session today, and second last but certainly not least, we welcome the Communications Alliance and other distinguished people. Could I invite you all to each to identify yourselves and then I invite an opening statement?

MR HOANG: Yes, Charles Hoang, Digital Capability and Policy lead, Australian Industry Group.

MS GILLESPIE-JONES: Christiane Gillespie-Jones, Director of Program Management, Communications Alliance.

MR STANTON: John Stanton, CEO at Communications Alliance.

MR HERRMANN: Chris Herrmann, President ITPA.

MR McINERNEY: Paul McInerney, Vice President ITPA.

DR RENWICK: Thank you. Does anyone wish to make an opening statement? Mr Stanton?

MR STANTON: Dr Renwick, thank you very much for the opportunity to appear before you today, and could we commend you and all your

colleagues for the thoroughness, the rigour, the determination that you've brought to this very complex assignment.

Communications Alliance represents the telecommunications industry and our members absolutely share government's desire to protect national security, to fight terrorism and crime, enforce the law, and importantly to enable the relevant agencies to do so effectively in a digital environment. Our members do cooperate on a daily basis with law enforcement agencies. In fact collectively the carriage service providers of Australia receive more than 11,000 requests for communications data on average per business day, and we cooperate also with agencies in relation to areas such as the blocking of websites that contain illegal content.

It's fair to say we've never seen a perfect national security bill, and I suspect we never will, but on each occasion over the past decade that new national security laws have been proposed, we've taken the approach of working closely with the agencies and other relevant stakeholders to try to improve the draft of the legislation to make it more balanced, practicable, capable of being implemented. And with pieces of legislation such as this TSSR Bill and the data retention legislation, I think those efforts yielded some significant improvements to the bill. I would have to say that we can't claim really any similar success in relation to the TOLA Act to date.

One of our foremost concerns with the legislation is the lack of meaningful oversight built into it, and in that context we warmly welcomed your opening statement today, and particularly your thoughts around that issue and possible solutions for it going forward.

The starting point in our submission to you was that we called for a warrant-based system with judicial consent to be required for the approval of all TANs and TCNs. In light of your comments and perhaps stepping up a little bit from that position, if we look at the outcomes that we would seek for an oversight framework, they would include the fact that notices issued under the legislation ought to be reasonable, ought to be proportionate, technically feasible and ought not of themselves to create additional cyber security risks.

So that to us suggests the need for an oversight mechanism that's independent, that has a judicial approval component, and that could be a sitting judge, but equally I think as you observed it could be a retired judge of appropriately senior stature, and crucially, such a framework needs to have access to technical expertise, to somebody who can decipher the detail of what's been requested and look at the risks it may or may not create and all the issues that on most occasions would be impenetrable to a non-technical person.

So the IPCO and AAT models that you talked about in your statement, we think, are both worthy of further exploration, in particular the IPCO model seems to satisfy most of the requirements that I've just listed there, or the objectives. It also perhaps has the advantage of being in place today and apparently beginning to prove its mettle in the UK market. We suspect also it may prove to be a slightly more agile model than an AAT-based framework of oversight. Certainly we would be ready to continue any work and make any contribution we can to developing such a framework in Australia.

The second item that I wanted to mention was one that's been talked about a lot today, and that is the definitions of systemic weaknesses and systemic vulnerabilities. We agree with others who've commented that the existing definitions are too narrow, they provide ample opportunity for agencies to be creative, if an agency was to require a DCP to install a vulnerability on every iPhone 10 sold in the State of Victoria, for example. That could pass muster as not being a systemic weakness, when I think from any reasonable assessment it certainly looks like it would be exactly that.

So we have recommended deleting the existing definitions in the Act and focusing, as others have spoken of, on articulating the things that would be a prohibited effect of a TCN or a TAN. We think that the legislation currently in the Senate goes some way in that direction, I think you've pointed out some potential weaknesses to definitions in it as well. But we would be ready to join a cooperative working group to try to drill down and get those prohibited effects more clearly articulated.

The third item we wanted to highlight goes to scope and threshold, and these powers were required in Australia, we've all been told to combat the most serious crimes, things such as child sexual abuse and terrorism. The threshold however in the legislation, that of a three year potential prison sentence, we think does not satisfy that requirement. Under the Crimes Act a prank or a menacing phone call could meet that three year criterion. And we note that within the existing TIA Act there is a definition of serious crime under section 5(d), which would carry with it a period of at least seven years of imprisonment. We would like to see the two pieces of legislation aligned and we think that seven years is a much more appropriate threshold to put in place.

Next comes consultation around TANs and TCNs, and we have been dismayed from the outset that section 317PA provides ample opportunity for the Director of Security or the head of an agency to circumvent any consultation requirement around a TCN or a TAN, simply by declaring the notice to be urgent, and in my experience I don't think I've yet heard an

enforcement agency describe a request a non-urgent. So I think that provides a very easy way out that ought to be tightened up somewhat.

We've also pointed in our submission to what we see as a couple of loopholes that actually allows the legislation to bypass existing data retention and interception legislations; we've made some recommendations for deletion of some clauses to give effect to that.

We heard earlier today from Atlassian about the risk to the reputation of their company and the tech sector in general in Australia, the erosion of international trust, the difficulties that this legislation may pose to Australian companies competing internationally, and we think that risk is very real.

We recently engaged with InnovationAus in some research to try to put some context around that risk, and we surveyed 70 companies in the tech sector, more than 60 per cent of the respondents said that their international domestic customers have expressed concern about the legislation. Forty per cent said they'd already lost sales or opportunities at home or abroad as a direct consequence of the Act, and almost 60 per cent said they were less likely to perform development operations in Australia given the corrosive nature of the way that the Act sees Australian-developed products viewed these days. So we think these are serious implications that need to be considered by Government and in any reframing of the legislation.

I'll pause there if I may, some of my colleagues may wish to make a couple of comments as well.

MR HERRMANN: I would also like to extend my thanks for the opportunity to come here and for the work you've done. So we represent over 15,000 IT professionals, we are, by and large, the people who will be tasked with implementing TANs and TCNs as they come up, and we'd like the opportunity today to voice some of the concerns that our members have raised with us, because we are the people who will be potentially affected in a very real way day to day.

So previously we've provided feedback on the feasibility of providing selectively breakable encryption, which I think Mozilla have covered off very well today, so I won't cover that ground again right now. Rather, I'd like to talk about some of the things that some of the members have raised directly, for example we have a large amount of our member base who write software or produce devices that are sold overseas into markets like the US, Canada and Europe, and their feedback was that their customers are asking them, "Well, what's your position? How are you approaching this and how are you complying with our local laws?", given that they appear to be in

conflict with their own jurisdictions, and that's for both devices, so telemetry devices, like for public infrastructure, as well as software.

In health care, we have people who work as health care providers, and their comment was that real privacy is necessary to gain trust between a patient and a doctor, and you can't provide good health care if you don't – you're not able to establish that trust, and this becomes an issue if there's a lack of trust, which is what's happened right now.

Another comment from another member was that it seems somewhat ironic that while these current problems with doing business in Australia appear related to implementing encryption back doors for compliance with their own local legislation, and it would be a shame if the same were to occur for Australian businesses overseas. So at that point, I'll hand over to Charles.

MR HOANG: Thanks for that. So I'm here as part of this collective in this joint submission, and I just want to give you some context of why Ai Group is here, because we cover some similar members but also a wider range of members as well. First of all, I would also like to endorse the remarks made by the Comms Alliance and ITPA, as well as future opportunity to collaborate with government further around developments around this Act and some of the ideas that's been posed today.

As I said, our membership covers a wide range of sectors, it includes those who are highly aware and concerned about this legislation, and then it extends down to those who you would expect to be more concerned if they actually stood the extent and scope and impact of the Act that could have on their particular businesses.

Just to provide you with an example, the other day I spoke with a large innovative manufacturer. They're aware of the TOLA Act, but they're not across the detail to know the extent or the impact that this would have on their business. And I suggested to them, is it because the Act is complex, it amends the Telecoms Act, for example, and this company's not traditionally subject to the Telecoms Act. So they have to rely on organisations such as ours and others who are more informed to provide them with that sort of insight, and it's likely representative of a range of other businesses who may not have been as engaged as one would have liked in this whole process.

Now, if I can also share some other examples. I spoke to another company, they're a multinational – they're based in the US, but multinational company, and they flagged there's a grey area for example around US export controls. So the hypothetical example of if government gains access to their source code, as a product of say the TCN, it could be in breach of

those laws. Now, I understand there's protections in place to try and mitigate that, but there could be a grey area.

Another example I received was from an Australian SME manufacturer. In their opinion they didn't think maybe it was necessarily applicable to them, but then the DCP, as it's defined under 317C – if that's the right provision – covers a range of businesses which could hypothetically capture them, because they're heavily engaged in what's known as industry 4.0, or smart manufacturing, everything is becoming more digitalised and hence, connected, and they do a lot of innovative stuff. So they could possibly be captured, either as an end user of those technologies, or as an implementer of those technologies too.

So those are just some of the examples of these sorts of companies that could be captured. Unintended consequences perhaps of a product of reliance on the infrastructure that requires a secure network, requires a secure system. There's all sorts of I guess different possibilities that we found, and I don't want to dwell on the process around the Bill, but there was a lot of views at the time we raised, as I'm sure others did, that they didn't necessarily appreciate the breadth of industries that could be captured.

Because I had noticed for example one of the provisions talks about the telecommunications industry, and the DCP I don't think is narrowed down to just the telecommunications industry. But sorry, I've gone off on a bit of a tangent, so – but yes.

DR RENWICK: Thank you. Were you going to say anything, Ms Gillespie-Jones? All right, thank you very much. Could I ask you to look at your submission to me of 13 September, which attaches a table, because I have some particular questions. So to deal with your concern, Mr Stanton, about shortness of time, I think that can be easily enough solved if the AAT is the decision maker, because they're the ones who will determine how much time is needed. And like any Court or Tribunal process, there's the capacity to speed it up or slow it down, as the occasion may require, so I think that's a practical way of getting around these things.

The risk to reputation, I suppose I would make a general remark that I'm hoping that this process and also the fact that I've been able to review or will review all the Schedule 1 and indeed Schedule 2 power exercises, and I'll say what I can about them in my final report.

I'm hoping that will sort of, you know, dampen concerns to some extent. As I mentioned earlier, we know from – publicly from the TI annual report that at the time that was issued there had only been, from a police point of

view, five AFP TARs, two New South Wales Police TARs, no TANs and no TCNs. And if that were to be a consistent trend, namely, mainly TARs, not TANs, TCNs, that might just put things in perspective perhaps.

I take your point about systemic weakness and vulnerability and we can talk further about that. So if I can then ask you to turn to the schedule at page 9 item 3, which is the definition of systemic vulnerability, weakness and so on. I take your point about the lack of definition of class of technology, I just wonder though if you turn to 317GA, I think that's the section I mean - 317ZG(a), sorry – the limits on notices, so ZG(4A), and I know – it would be great if we renumbered it from the beginning, that would just be super. That's probably beyond my capacity to recommend.

So you say:

> *Consider the case where ASIO instructs screen capture technology be introduced into all smart phones produced by large android manufacturer but not all android smart phones.*

Arguably this means not the whole class of technology is affected, but I just wonder whether 4A would prohibit that, because that says:

> *In a case where a weakness is selectively introduced to one or more target technologies connected with a particular purpose, the reference in paragraph (1)(a) –*

which is a prohibition –

> *includes a reference to any act or thing that will jeopardise the security of any information held by another person.*

You might want to take that on notice, but it just seemed to me that that might be one answer. The whole idea of class of technology is problematic. I mean, at the minute it's I suppose, given its ordinary English meaning, it doesn't have a set technical meaning, I wouldn't have thought. But it's pretty unclear what it means, and I certainly agree with that. But it just occurred to me that that might be one answer to that.

If you then turn to page 12, I think I can put your minds at rest on that, where you say, "The list of matters the Minister" – which is item 11 on page 12:

> *The list of matters the Minister must have regard to when considering a TCN is less extensive –*

I think in fact it's the same, and arguably because the Communications Minister has to also buy in. So I think that might - - -

MS GILLESPIE-JONES: I think we can leave that one alone.

DR RENWICK: Leave that one alone?

MS GILLESPIE-JONES: It is in the end there through reference of a reference and through different clauses you get to the same result I think.

DR RENWICK: Okay, thank you. Can I ask you some questions on page 17 at item 21, where you recommend that TANs be removed? Can someone just talk me through – so see, my starting point is, unless I've misunderstood it, that TANs involving giving help where you can already do something, whereas TCNs are designed towards ensuring that the DCP is capable of giving listed help. So one's an existing capability and one's building a new capability. And they're quite different, and indeed, our last speaker seemed to have – and many speakers – had a much greater concern about TCNs rather than TANs.

So is that a point you still press or do you want to explain it a little bit further for me?

MR STANTON: Part of our concern was that the TANs don't have or they don't carry with them the right to an independent assessment.

DR RENWICK: I see.

MR STANTON: As faulty as that may be under the existing legislation or as weak as it may be, and we thought on the one hand it was a way to reduce the complexity of the Act, and also the edges, in practical terms, can blur between what a TCN asks for and what a TCN (sic) asks for. So we thought, well, let's ensure that everything has a right to assessment, let's simplify the Act and have a single class of notice, and were that the case and it was subject to an independent oversight, you still achieve safeguards around whether what's being asked is reasonable and proportionate. Do you want to add to that?

MS GILLESPIE-JONES: No, I think that captures it. We were of the opinion, and I probably are still of the opinion, that what you can request with a TAN is quite far-reaching, but is not subject to the same controls mechanisms, and we found the distinction quite blurred between the two, and the Act itself is difficult to understand and would probably benefit from a removal of the TAN. Having said that, we wouldn't be sure if that is

universally the opinion of the industry and it's probably not a point that we want to press.

DR RENWICK: Got it.

MR STANTON: And if everything is subject to independent oversight, then the urgency of the issue is diminished.

DR RENWICK: No, I understand. Going back to page 8 item 1, the definition of electronic protection in 317B. So it's not really a definition is it, it just says it includes authentication and encryption, and I think you say it's particularly problematic in view of 317ZG.

So what you seek, you delete the words "into a form of electronic protection". So are you only – just to be clear, do you only want that removed in 317ZG? Or do you also want the definition of electronic protection in 31ZB amended? I think it's the former isn't it, you just want it out of 317ZG?

MR STANTON: That's the alternative that was suggested, yes.

MS GILLESPIE-JONES: Overall I think it would be fair to say that we would be – we are supporting the amendments as put forward by the recent repair bill.

DR RENWICK: I see.

MS GILLESPIE-JONES: Which is the deletion of these various, I think they're four in total, definitions like cyber technology, whole class of technology, electronic protection, systemic weakness, and rather target the effects that a TCN should not have, and clearly articulate those.

DR RENWICK: All right. The point made by Access Now's representative before the break, or one of the points she made, was that the focus of the Act and the debate is very much on the DCP on the one hand and the government agency on the other, but the customer of the DCP tends to get forgotten, and they have, even if they may not have strict legal rights, they have certain expectations about the privacy and security of what they use as provided by the DCP.

Now, at the minute, when we talk about the underlying warrant given by obtained ex parte, there's no one there to advocate on behalf of the target, and that's something which is criticised occasionally when for example the target might be a journalist, but there's no specific protection for the target.

So the proposal, as I understand it, is if it was to go to the AAT, which would be both the warrant itself, the underlying warrant – so to be clear, to obtain the thing, under pre-existing TOLA law, and then to obtain the unlocking under TOLA, that would both be in the AAT, and the concept is that both the DCP and the government applicant would have a seat at the table in the AAT and could be heard.

You heard what I said to Atlassian earlier, that there may be good reasons why you don't want the other to hear your innermost secrets, and that's an advantage you can have in the AAT but you probably can't get in the courts.

The question I suppose, is whether there should be some person who at least is available to speak on behalf of the customer, because the interests of the DCP and the customer may diverge. Do you have a view about any of that?

MR HERRMANN: So in our case, most of the people we're representing are smaller than Atlassian, and they in turn might be representing an individual who is sick, or a person who has a complex housing issue they're trying to resolve, or it might be a business providing legal services. So in our case, they're the kinds of things that our members have come back to us saying, "Well, how do I protect them? How do I give these people assurances that they're not going to have their data inadvertently exposed, either through a technical flaw or through a flaw of process?"

DR RENWICK: So do I take it from that then, that you support some sort of seat at the table of a representative - not the individual - but a representative, who could speak on their behalf generically; is that what I get from that, or not?

MR STANTON: You go to the question that came to my mind, which is are you talking about someone who would protect their rights generically, would protect, you know, human rights and privacy, or someone who would be advocating, effectively, for an individual or an individual entity?

DR RENWICK: I think maybe I can answer my own question by saying it's probably the former, I think. Yes, more generalised, I think.

MR MOONEY: Okay, so it's just to represent those interests.

DR RENWICK: Yes.

MR STANTON: We wouldn't object to that. The mechanism would need to be figured out I guess, but conceptually, there may be merit to that.

DR RENWICK: That's all the questions I've got. It's very, very helpful. As I said to earlier groups, if there's anything you wish to put in soon by way of supplementary brief submission, I'd be grateful. But in particular, if the AAT model commends itself to you, any refinements you might have about that. I think I have the point that if that's to work, there's got to be able and independent technical advisers sitting with the lawyer, in making the decision. And presumably, there is a small number of people who are suitably qualified and suitably independent who could do that.

I should just note that, finally, in the UK, the strength of the system there when IPCO does both things, it grants or has the double-lock and does the IGIS-type function is, those technical experts can then get involved in the auditing. And in that way, you have sort of assurance that the conditions on the original warrant are maintained, and also, everyone's up to date about what's actually happening.

I mentioned in my opening - and I welcome any thoughts on this - that you could have those independent experts appointed as part-time senior members of the AAT; but they could also be consultants say, to the IGIS and the Ombudsman. They'd obviously have to avoid conflicts of interest in particular cases.

But that seems to me to be valuable knowledge because the thing I fear most in this area is that, candidly, me included, it is technically beyond a lot of lawyers unless they have some really savvy independent technical advisers.

MR STANTON: We can certainly undertake to talk to our members about the AAT model, and bring back some reflections from them on relevant issues. And I'm sure your Secretariat will talk to us about relevant lines for coming back.

DR RENWICK: Yes, sure. And I think you've got the point that I made at the beginning, which is that the other thing the AAT would allow you to do is either at the hearing, or through ADR before the hearing, if there is a discreet technical question, for example, Home Affairs says, "This is not a systemic weakness," Apple says, "Yes it is," there's an effective mechanism of resolving that in a cost-effective and quick manner.

MR STANTON: That would certainly be a big step forward.

DR RENWICK: All right. Well, look, thank you all very, very much for attending, and indeed, participating in such a valuable way in this whole review. And I'm sure we'll be speaking further.

MR STANTON: Thanks very much.

DR RENWICK: Thank you. And now Michelle.

#SESSION 4: AustCyber (Australian Cyber Security Growth Network)

DR RENWICK: I invite Ms Michelle Price to come forward. Ms Price, you're the CEO of AustCyber. I invite you to, for the record, just say something about AustCyber's role and any opening remarks you may have.

MR PRICE: Well, thank you. So AustCyber, the Australian Cyber Security Growth Network; we are an independent, non-profit organisation that is part of the Federal Government's Industry Growth Centres Initiative. So we are funded by government, but we are a private entity. And my job is, as part of the contract that we have with the Commonwealth, is to grow the Australian cyber security sector. So it's not just about industry; it's making sure that Australia has global competitiveness in the economic opportunity that is found in cyber security.

To make some opening remarks, I too - to link back to your remarks at the very top of the day, Dr Renwick - I acknowledge the traditional owners of the country throughout Australia, and recognise their continuing connection to land, waters, culture, and emerging in cyber space. We pay our respects to their elders, past, present and emerging. And I thank you too, as many others have today, for these hearings.

The hearings are really important, for a number of reasons. In part, because of the comparative immaturity of Australians around the complexity of cyber risk; that's been mentioned many times today. But also around the opportunity of having a secure and trust cyberspace, as well as the comparative economic immaturity of Australia's cyber security sector.

While the sector is rapidly maturing, there is still a way to go on matters of policy and constructive advocacy. I say this not as a criticism of the sector that I am tasked to try and build, or of the organisations that work so hard within that construct; but rather, an observation around the status of the culture of doing business in cyberspace, and that of cyber security, resilience and privacy.

Overall, as a sector, the cyber security sector was largely silent in the period leading up the passage of the Act, however, we seem to take a lot of the blame for the interesting debates, or not necessarily debate that took place around that time, and some of the analysis that has happened since, that in

fact, it was the cyber security industry that was trying to work behind the scenes with government to find a better way to resolve these issues.

And so public debate of course is exactly what we need on this topic, and the way that this topic relates to every part of human endeavour now in a cyber-physical world. So I appreciate and support your opening remarks, and in particular around the oversight mechanisms, the matters of definition, and the high degree of thorough investigation that clearly helped form your opening remarks.

The businesses developing cyber capabilities - and we must remember that those capabilities are both human as well as technological - are complex, they're both fast and glacial, they are transporter, they are cross-sector, they are multi-actor, and very importantly, they are highly contextual. To manage all of this, it is widely appreciated in industry that we need to move quickly into a world, into a business culture of developing things, including people, that are secure by design.

I contend that cyber security is now a required enabler for all things in today's cyber-physical world. Everyone and everything needs some form of cyber security to be able to live confidently and trust their world is what they think it is. I note and applaud the opening yesterday, officially, of Australia's space agency; another feather in Australia's cap of the multiple benefits that we can enjoy now, that we can take now, and for all generations that come after.

This, however, is a reminder of how quickly we need to adjust the left and right arcs around the application of legislation and regulation. Encryption-based technologies are a key feature in the security of the world's space industry, as it is, in many other industries, been created around new forms of technology like 5G, quantum computing, et cetera, et cetera, et cetera. And while we might think that quantum computing is very far away, quantum technologies have now been with us for over 20 years.

So I might leave my opening remarks there.

DR RENWICK: Thank you so much, Ms Price. So one of the things I wanted to discuss with you was how TOLA interacts with international cyber norms. And as you will recall, one of the requirements for decisions under TOLA about whether any Schedule 1 powers are reasonable or proportionate is to look at the legitimate expectations of the Australian community, relating to privacy and cyber security. So, would you care to comment on what that means to you, and how TOLA fits in with international cyber norms?

MS PRICE: Indeed. And I do actually have here, that I can leave with you, colleagues can go to, those watching on the inter-webs can go to DFAT's website and find the listing of cyber norms. So this is a piece of work that is going on actually quite out in the open, around how to develop norms of behaviour in cyberspace.

Australia's representative in the formal mechanisms around the development of cyber norms is the Department of Foreign Affairs and Trade, principally through our Ambassador for Cyber Affairs, Toby Feakin.

There are currently 11 norms that are recognised as being the foundations of behaviour in cyberspace. Now, norms of course, are not law; they're not requirements for us to adhere to. Like anything else, in terms of whether or not we walk on the left side of the street or on the right side of the street is our preference, those norms of course form the foundation of how we behave, and then develop policy, implement that policy through things like standards, guidance, regulation, legislation.

So the norms work at the international level is critically important. And those 11 norms go to things like the fact that we won't use cyber technologies that are not dual-use, they're multi-use technologies; we won't use them against ourselves; we'll accept that we are on the light side of the equation, and that we'll trust that all of us around us, as likeminded organisations and nations, will behave in a similar kind of predictable way, so that we can understand a language in order to do business in a cyber-physical world.

So when we are faced with I guess a complex world of legislation and regulation - and I would contend that the practice of developing legislation and supporting regulation now hasn't kept pace with the multifaceted, interconnected world that we live in - we still do see legislation and regulation, not just in this country but in other countries elsewhere, being developed in silos.

It doesn't take account of the contextual nature - that's a word that's very, very key to a lot of this - the contextual nature of how we actually do go about our daily lives, whether that be in a personal context, or it be in a business context. So those norms are very important for us to be able to guide the left and right of arc around those behaviours.

Norms of behaviour in cyberspace are very tricky because of the complexity, but also the pace and reach of how technologies and humans using those technologies, can transgress borders in ways that we can't physically, and the time involved in that. In a sophisticated way, it does still take time, but we're talking in orders of magnitude of hours now; and

in the simple, straightforward types of attacks, they're seconds, they're not the 24 hours that it might take us to catch a plane from Sydney to London, for example.

So this is what makes the norms in cyberspace very important: they don't happen in isolation of course, is what I'm getting at. So the development of those norms do take account of the legislative and regulatory environment that each of the countries bring to the table in their minds, on their shoulders, and in their talking points, when they're negotiating around those norms on our behalf.

Of course, in that sort of sense that we get in Hollywood whenever we see those movies about the negotiations that go in the sidelines of the United Nations, it's very, very similar to that: these are multilateral, multinational fora that act on our behalf to try and achieve what is good, what is the right thing to do for the world.

So when we have legislation that doesn't provide clarity, doesn't provide expectation management in ways that those norms are brought to the forefront, it creates doubt. And it creates uncertainty around how we can negotiate on those norms, and whether or not we're a trusted partner in likeminded negotiations, to try and shape and steer the conversation in ways that we would like to see happen, as opposed to those that are openly attacking us every day, and get their way around how the landscape should be shaped and influenced when it comes to those norms of behaviour that then inform international law and then domestic national law.

DR RENWICK: So if I can just take an example, which could pull in either direction, about expectations? If people discover, as they do periodically, that when they've clicked "I agree" to the terms and conditions of their ISP or whoever, in fact, they're looking at much more stuff, content and data, they're monetising it in ways they could never have imagined. I mean, I just wonder, does that raise the expectations we have in cyber security, or reduce them because we've become more cynical?

MS PRICE: I think it depends, again, on context. I think this is where we can get into the culture of where we sit at the time; we're influenced by where we're physically sitting and when we're clicking on the acceptance of those terms and conditions. So me accepting the terms and conditions for example, that Mozilla put out this morning with their latest update of their browser, I would be thinking differently, as an educated person, around those topics; I would be thinking differently in clicking on that here, versus somewhere like, for argument's sake, Ecuador or Estonia, or Spain, because every country has a slightly different regime.

So the point I think you're getting to is that if you're less educated around the context of these matters, you are blindly clicking. And the application of these things can't happen in a consistent way internationally yet, because those norms haven't been fully agreed, and therefore we are relying on other forms of international law to take account of the gaps between different jurisdictions. So that lack of clarity exists at that level as well.

And this is where we do have situations that have already played out with large technology providers using different forms of state law, national law, to try and I guess navigate the lack of clarity at the international norms and international law level. So it's actually not as straightforward as what people might think, in terms of clicking to accept terms and conditions for a provider that's domiciled somewhere else in the world.

But they still do have that expectation that that provider will be providing the kind of safety and security that your own country provides, in terms of where you clicked the acceptance from.

DR RENWICK: When we talk about Australia's reputation, we obviously can't turn the block back and imagine we had a year to look at the TOLA Bill; we didn't. That's what happened. Part of my role is to, in a sort of low key way, just explain what use there has been of the powers. As I said this morning, there's no question of mass surveillance or anything like that, and in fact, it seems the Schedule 1 powers have enabled things to be done in a more targeted fashion.

I'm just wondering what else, apart from doing my report and faithfully recording what I'm told, one can do in relation to reputation.

MS PRICE: We've heard a lot today about the impact to reputation, and I think there's action that needs to be taken on both sides. And I do like the way that you've put forward that kind of dichotomy of having industry on one side of the table and government on the other; it continues to set up this separation between the two, when in fact, of course, we need to be collaborating more than ever, against the common issue in all of this, which is to catch out those who wish to do us harm.

And so I think that there does need to be - we know that there needs to be - some mending of trust in this entire equation. And in terms of when it comes to reputation, reputation obviously is all about trust. It's quite straightforward - not necessarily easy - but straightforward, to have; it's very easy to break or breach, and it's very difficult to rebuild. It will take time and it's not going to be straightforward or easy to do so.

Meaningful engagement, both domestically and internationally, is needed to provide some kind of, I guess, break in the cycle. I give you the example where as recently as two weeks ago, we were provided with some examples out of the UK, because we do hear a lot about the examples coming out of the US; and Atlassian, of course, has provided some of those from their own experiences today.

But we've had companies, both very large and very small, talk to us out of the UK - these are both British companies as well as Australian companies operating in that environment - talk to us about how their expectation over the past 12 months with TOLA being enacted, was that Brexit would be the area that they would have to focus their energies on, to convince people that, "It's okay, you can still buy from me. Brexit is not going to impact us."

In fact, Brexit has rarely come up in conversation; it's been TOLA that has come up still, repeatedly, in conversation, and is still causing a lot of unrest in those commercial discussions. And without there being anything to point to, your premise around providing some examples is often what people speak to; if we had examples of what this could look like in operation in terms of how it could be applied. Even though it's not been applied outside of the telco environment, as far as we are aware and have been made aware, through those disclosures, the Act does allow for it to be applied in many, many other circumstances, and that that is the ambiguity that's causing the uncertainty and the unrest.

So while there's not as much noise anymore being created around this, and I think that's a good thing, the open debate about these matters is still so critical. And so that reputational damage that actually has been done needs to go as far as joint representation between industry and government, to other countries, to provide reassurance around how this is going to operate and how it affects them, how does it affect that jurisdiction, relative to multi-party commercial deals that are being done every day?

DR RENWICK: Thank you. Mark, anything further?

MR MOONEY: No, I think we've covered it, James.

DR RENWICK: I think we've covered everything. Is there anything more you wanted to add, Ms Price?

MS PRICE: I think the only thing I'd like to add, in addition to what has already been said, is that from the point of view of a model that can be evolved from what we are living with today on the oversight framework, the trust piece I think in terms of both the relationship between government

and industry here, as well as abroad, also in the context of how that applies to reputation, would be enhanced by making sure that there are mechanisms within that framework that provide for transparency around the appointment of the technical advisers.

So we need to learn the lessons, in my view, around how got to seven years' worth of negotiation between government and industry on TSSR, and a shorter but still rather lengthy negotiation between industry and government on metadata and data retention. Let's learn those lessons and appreciate that if industry has a voice and can have a constructive say - and industry needs to step up to this too, appreciate that - but can have a constructive input into the appointment of who occupies those roles of the technical advisers, I think that is another really, really, key piece of making sure that we can get the trust piece back on track.

DR RENWICK: So you could have - and I think I alluded to this earlier in the day - a provision in the AAT Act which says when you have one of these applications, say a TAN, for consideration, "The tribunal shall be constituted by a senior lawyer in the middle, a person who has technical experience who's worked in government, a person who has technical experience who's worked in industry." And for the latter, you might say, "And before such a person is appointed, it shall be necessary to consult with industry."

MS PRICE: Indeed.

DR RENWICK: Something like that.

MS PRICE: Something like that. and I think it's worth noting as well that increasingly, the reality of the skills shortage in cyber security is such that we estimate - we're going to do some work on this later this year, to have the actual data - but we estimate that around a third of the people working in the cyber security industry are former government employers, so they do understand the legal left and right of arc of what government is working within.

DR RENWICK: Yes. And just as a practical matter, one should be able to find say, half a dozen people who would be able to still be in touch with the technical matters, wouldn't you?

MS PRICE: I'm very confident of that, yes.

DR RENWICK: Yes. Well, Ms Price, thank you so much.

MS PRICE: Thank you.

DR RENWICK: I'm conscious of the time. Being 4.17, we will finish for today. And tomorrow, just for those who are coming, we'll again start at about quarter to 9. First, we have the Law Council; then we have the Allens Hub for Technology; then we have the South Australian ICAC; then we have the Software Alliance from Singapore, I think; then we have the AFP; and last but not least, we have the Department of Home Affairs, who administer the legislation.

So thank you all, and until tomorrow.

ADJOURNED AT 4.16 PM TO FRIDAY 21 FEBRUARY 2020