COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

Telecommunications Legislation Amendment (International Production Orders) Bill 2020

WEDNESDAY, 13 MAY 2020

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

To search the parliamentary database, go to:

http://parlinfo.aph.gov.au

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

Wednesday, 13 May 2020

Members in attendance: Senators Abetz, Fawcett, Stoker and Mr Byrne, Mr Dreyfus, Mr Hastie, Mr Leeser, Mr Tim Wilson.

Terms of Reference for the Inquiry:

To inquire into and report on:

Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

WITNESSES

BARBOSA, Mr Norman, Assistant General Counsel, Law Enforcement and National Security, Microsoft Australia

MASTERS, Mr David, Corporate Affairs Director, Microsoft Australia

Evidence was taken via teleconference—

Committee met at 09:39

CHAIR (Mr Hastie): I declare open this public hearing of the Parliamentary Joint Committee on Intelligence and Security for its review into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020. These are public proceedings, although the committee may agree to a request to have evidence heard in camera or may determine that certain evidence should be heard in camera. In acknowledgement of the current COVID-19 situation, certain measures have been implemented. Throughout the hearing, appropriate distancing will be maintained for those in physical attendance, and teleconferencing facilities have been arranged to allow most witnesses to appear remotely. In this way, witnesses can engage with the committee, and the committee can continue to undertake essential work.

I remind all witnesses that in giving evidence to the committee they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee, and such action may be treated by the Senate as a contempt. It is also a contempt to give false or misleading evidence to a committee. In accordance with the committee's resolutions of 4 July 2019, this hearing will be broadcast on the parliament's website, and the proof and official transcripts of proceedings will be published on the parliament's website.

I welcome representatives from Microsoft Australia. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now invite you to make an opening statement before we move to discussion.

Mr Barbosa: I appreciate the invitation to speak to your committee. I manage Microsoft's global lawful access compliance and public policy efforts. My team handles approximately 60,000 requests per year from law enforcement authorities around the world. I'm also responsible for Microsoft's public policy position on issues including encryption, cross-border access to data and CLOUD Act agreements. My team is part of a broader organisation within Microsoft known as our customer security and trust organisation. That includes our digital crimes unit, our digital security unit and the digital safety team.

Together these teams are responsible for much of the work Microsoft does to combat criminal and nation-state cyberattacks and prevent the abuse of our services for child exploitation and other serious crimes. This provides us with unique insight into the borderless nature of crimes on the internet and is one of the reasons we recognise that governments and the private sector must work together to prevent and detect crime in the digital age. Microsoft has recognised for many years that these traditional mutual legal assistance treaty processes, or inlet processes, are ineffective and incapable of addressing the complexities that arise when governments need access to electronic evidence that may be held in foreign jurisdictions.

I also have personal experience with the challenges of pursuing electronic evidence in cross-border investigations. Before joining Microsoft I was a US federal prosecutor responsible for supervising cybercrime and national security investigations. In my prior role as a federal prosecutor I often found myself frustrated by the delays inherent in the MLAT process. It could take months or years to pursue each lead in an investigation. This is obviously unsustainable when pursuing electronic evidence that can be ephemeral and disappear while you are waiting on a response.

Recognising these shortcomings in the MLAT process, Microsoft is a supporter of the CLOUD Act, which modernised how cross-border data can be accessed appropriately by law enforcement. The CLOUD Act came about as a result of Microsoft's efforts over the course of several years to highlight these issues and help find solutions. As many of you know, the CLOUD Act resolved a case that Microsoft brought in 2013 and ended at the US Supreme Court—the Microsoft Ireland case—in which we challenged a US government warrant for data held in our Irish data centre. We didn't bring our case out of a desire to frustrate law enforcement; we brought that case to derive the systemic changes necessary to advance public safety and security while at the same time ensuring adequate protections for privacy, human rights and digital sovereignty. Our goal was to create new processes that would enhance transparency and reduce the legal uncertainty that risked flowing the digital transformation of customers around the world, including government agencies and businesses in Australia. This is why we welcome

the passage of the CLOUD Act and have been working to help facilitate agreements with the UK, Australia and the European Union since it was enacted in 2018.

But while the CLOUD Act establishes an important framework for agreements we also believe that the domestic laws that enable these agreements should meet certain baseline requirements to protect privacy and human rights and provide the transparency necessary to maintain trust in technology. Shortly after the act was passed we outlined several principles that we think are important to meeting these goals. They relate to notice, transparency, mechanisms to address conflicts of law, and enterprise data or business-to-business services. As we outlined in our written submission to the committee, there are a few areas where we believe that the bill could be improved to address these principles without frustrating the goals of law enforcement or damaging public safety. I'll briefly touch on a couple of our points now before moving on to your questions.

First, we would like to see some provisions that protect customers' rights to be notified of surveillance demand and greater transparency in general relating to how the IPO bill is used in practice. While we recognise that there is often a need for secrecy at some stages of investigation, and that some particularly sensitive investigations may require greater secrecy, notice and transparency are important to maintaining trust in government and technology. As I stated just yesterday, transparency is likely to create better public trust and allow law enforcement to do their job better.

Second, as we noted in our comments, we also believe that the bill should contain express provisions for addressing potential conflicts of law. This goes to the heart of the issues the CLOUD Act seeks to address. It is important that as governments create new mechanisms to advance public safety and security the laws designed to facilitate those agreements resolve conflicts of law rather than create new ones. We have also recommended incorporating existing law enforcement best practices relating to enterprise data. Companies that use business-to-business enterprise communication services are rarely the subject of law enforcement warrants; and, absent extraordinary circumstances, we have found that law enforcement can almost always approach businesses directly when investigating activity related to the business. We believe that enterprise data should be excluded from the provisions of the IPO or that there should be a requirement that law enforcement make a separate showing that seeking enterprise data from a service provider is reasonable and proportionate based on specific risks to an investigation. Thank you, and I look forward to answering your questions.

CHAIR: Thank you. Could you outline how Microsoft Australia currently manages requests received through the provisions of the Telecommunications (Interception and Access) Act 1979?

Mr Barbosa: Microsoft responds to demands for non-content data globally from a number of countries, including Australia. We have local personnel who receive requests for non-content subscriber records and IP addresses who forward those on to our corporate team to process them and we respond to a number of requests from Australian law enforcement officials around your country.

CHAIR: You're talking in very general terms here. Could you talk a bit about how Microsoft Australia manages requests received through the Mutual Assistance in Criminal Matters Act 1987?

Mr Barbosa: Mutual assistance requests from Australia would typically be transmitted to the US Department of Justice who would then domesticate any request on behalf of the Australian government through US court procedures. We often receive warrants from the United States government that are in furtherance of MLAT requests, and we process those in the normal course of business. We may or may not see whether or not that is in furtherance of an MLAT request and very well may not see what country it is coming from—and sometimes we do. We process those based on US law and our ability to respond to US warrants for content.

Mr BYRNE: On both of the chair's questions about the Telecommunications (Interception and Access) Act and the Mutual Assistance in Criminal Matters Act, how many requests would you have under those two acts from Australia?

Mr Barbosa: I don't have specific data on requests pertaining to those individual acts. We do keep transparency reporting on the number of requests we receive in total from Australian authorities, but we don't break them down based on the specific act that they're requested under.

Mr BYRNE: Is it possible that you could take that on notice, please?

Mr Barbosa: Absolutely.

Mr BYRNE: You said, 'total number of requests'. If you're able to divulge this publicly, how many total requests would you have from Australia?

Mr Barbosa: Fortunately, I can look this up pretty quickly as I'm at my computer right now. For example, we have a publicly available transparency site where we report the number of requests we receive from each

government around the world. Looking at our most recent reporting that covered July to December 2019, we received a total of 898 requests from Australian government authorities.

Mr BYRNE: That's useful. Thank you.

Mr TIM WILSON: I've just got a quick question. You said before that you want a process of notification for people who are under investigation. Could you elaborate on what the threshold, or level, would be where there would be notification? How do you envisage that working?

Mr Barbosa: Absolutely. We believe it is a fundamental right of customers and citizens around the world to receive notice, at some point, if they have been the subject of surveillance. How we envision that working is similar to how it works in many countries around the world, including the US, in that, after a request has been executed, both the government and the service provider take part in that notice. The government should have an obligation at some point to notify the target of surveillance that they have been the subject of a request. And service providers should be allowed to communicate freely with their customers about them. Again, that is all the recognition that they're—

Mr TIM WILSON: Just for clarity, what you're saying is that you think the notification should come from you not from law enforcement agencies.

Mr Barbosa: We think it should come primarily from law enforcement, but the service provider should also be free to speak to their customers about the nature of surveillance that is required, but subject to limitations, obviously, when there is a risk to an investigation. We recognise that there are many cases where secrecy may be necessary for some portion of the investigation, or possibly longer, depending on the nature of the case.

Mr BYRNE: For example, if we want to access people's information content, that should be in relation to an investigation into something that is quite serious, like a potential terrorist event, and we're looking at that. What we're grappling with is that it would seem to be counterproductive if an agency is requesting this information and you are notifying that person. As a prosecutor, you would know that they'd become aware of the fact that there was potentially an investigation into their activities, and that could compromise the investigation. I listened to what you said at the end. Are you proposing that you would tell these people after the investigation had been completed? What are your potential time lines based on the sensitivity of the matters that are being investigated and looked at by the agencies in Australia?

Mr Barbosa: We found that the time line can vary depending on the facts of a case. Obviously, I speak from US experience—in the context of different investigations, the time line can be anywhere from a few months to over a year, depending on the sensitivity of the case and the progress of the investigation. An ongoing investigation may need ongoing secrecy, but oftentimes, once a case has been solved and a suspect has been brought to justice, the government will be revealing its evidence against that suspect and there is generally no longer a need for secrecy.

Mr BYRNE: I understand that, but what are you concerned about? Do you believe that, out of those 898 requests, there would be a number that wouldn't be on the serious end of the scale, so you could tell those people? I'm a bit perplexed. I understand that you need to ensure that people know their data is kept safe and that you have privacy provisions. But it's that aspect where, in relation to some of the people being investigated—and it could be in relation to matters like terrorism, foreign interference or espionage—you'd be alerting the suspect, effectively, to a potential investigation, and that could compromise the investigation. That's the thing that some members of the committee are grappling with, when you say that.

Mr Barbosa: I absolutely understand. And you've raised some of the cases at the far end of the spectrum of seriousness when you refer to terrorism and espionage. In those cases, I've investigated and prosecuted cases like that as a federal prosecutor, and the need for secrecy can often be much longer lasting than it might be in a more routine, but still serious, investigation. For example, fraud investigations can be quite serious. Violent crime cases, which are often solved in a lesser amount of time than broader international terrorism or espionage cases, don't necessarily need permanent secrecy in our experience. We see this come up most frequently in the context of white collar-like investigations when businesses and citizens are concerned about the type of surveillance that may be conducted and they expect to be able to ask questions about this and to understand how government works. It's just one part of the transparency that we believe is important to maintaining trust in both government and technology.

Mr BYRNE: I agree with you. I was over there just after San Bernardino and met with representatives of the FBI who were very keen to get access to the phone in question that was used by the terrorists. Having dealt with the prosecutorial agencies and the investigatory agencies, I'm aware that there's that competitive tension between the agencies wanting to get access to the information and the companies that are providing these services to assure

their customers that their data is being protected and not just accessed easily by enforcement and other agencies. So I get that. In a sense, you could say you'd be triaging, to some extent, when you may be advising these people under this bill, if it is implemented. The gravity of the crime and the stage of the investigation would determine when you'd advise them whether or not their data had been accessed or they'd been the subject of a request from an Australian agency.

Mr Barbosa: To be clear, we don't think this should be a decision that is left to the discretion of service providers. We think that the length of a secrecy order should be up to the issuing authority—preferably a court or other independent authority—that is assessing, based on facts presented to them from law enforcement, 'What is the risk? How does that risk exist?' and giving us, as a service provider, a clear indication of when we may speak. For example, in the United States, when law enforcement obtains what is called a non-disclosure order—it prohibits us from telling our customer—the order tells us when that expires. So, if we receive a warrant, it will often be accompanied by an order that says, 'You may not speak about this for one year,' and, at the end of that year, we know that we can now inform our customer.

Mr BYRNE: So you would do that as a matter of course? This is just for my understanding about the United States system. After that, every access request that you would have from an agency or law enforcement body, subject to what you would just say—after that period of time has elapsed, then you advise the person that there has been a request?

Mr Barbosa: Yes.

Mr BYRNE: Okay. That's very useful to know. Seriously, that's very useful evidence. Thank you.

Mr Barbosa: Thank you.

Mr DREYFUS: Thank you, Mr Barbosa and Mr Masters, for appearing to give evidence. You've given us a principles based submission, and in both your introduction and in the questions so far you've been dealing with principle 1, which is about people's right to know when government accesses their data. I wanted to go to your other principles, starting with the 2nd principle, which is that all demands for content should be pre-approved by an independent judicial or equivalent authority. As I understand your submission, you share concerns that others, including the Law Council of Australia, have raised about the independence of, in particular, the Administrative Appeals Tribunal. What's the basis of your concern about the Administrative Appeals Tribunal?

Mr Barbosa: We have a strong preference for independent judicial review of any surveillance orders. At the same time, we recognise that every country has different mechanisms for addressing how that independent review will be conducted. We are most concerned with ensuring that there are robust mechanisms for that review and that the standards clearly require law enforcement to set forth a factual basis that shows that the request is reasonable and proportionate, that there is reason to believe that there is evidence of the crime that is under investigation that will be located in the data that is being sought, and that the reviewing officer is not subject to any undue influence from the government agency making the request.

Mr DREYFUS: Over the last seven years, the current government of Australia has appointed over 70 former members of its own party—former politicians, failed Liberal or National Party political candidates, Liberal or National Party staffers, Liberal or National Party donors—to the Administrative Appeals Tribunal. Does that concern you?

Senator ABETZ: Any Labor ones in that?

Mr DREYFUS: Ignore the injections, if you would, Mr Barbosa, from colleagues on this committee.

Senator ABETZ: Because it's an inconvenient truth.

Mr TIM WILSON: It's a follow-up question, which is, 'If they were concerned, were they concerned about Labor ones as well?'

Senator ABETZ: With such a bipartisan committee, we would want the witnesses to understand that.

Mr DREYFUS: I have some people running interference on this. Just to give you the numbers, Mr Barbosa, the previous Labor government, in six years, appointed an eminent former trial lawyer, with the approval of the opposition, to serve on the tribunal—

Senator ABETZ: Because we are gracious.

Mr TIM WILSON: That shows bipartisanship.

Mr DREYFUS: and one other former Labor Party member to serve on the tribunal, who was subsequently reappointed twice by the current government.

Mr TIM WILSON: Didn't we appoint McClelland to the Family Court?

Mr DREYFUS: Regrettably, the current government of Australia has seen fit to appoint over 70—that's more than a fifth of the total membership of the tribunal—from its own party, including former members of parliament from its own party, former failed candidates from its own party and former staffers from its own party.

Mr TIM WILSON: The shadow Attorney-General is saying it with a smug smile on his face.

Mr DREYFUS: It's a galling fact that seems to bother some of my colleagues on this committee. But I would ask you to proceed on the basis that over 70 of these political appointments to the Administrative Appeals Tribunal have been made in the last seven years. No such concern has arisen in respect of Australia's courts.

Mr TIM WILSON: That's because we appointed someone from the Labor Party.

Mr DREYFUS: If you could just calm down. Mr Barbosa, the question is: does this concern you?

Mr Barbosa: In our recommendation we recommended that, to add confidence in this process, we would suggest that the PJCIS seek confirmation that only members of the security division of AAT can authorise IPOs, and that the PJCIS recommend additional requirements for the membership of the security division that are empowered to authorise IPOs to ensure that members have the requisite legal, technical and privacy experience when considering these. I don't have a view on the political implications of the appointments, but we just want to be sure that those reviewing these are not subject to, as I said, undue influence that could impact a review.

Mr DREYFUS: I take it that the basis for that suggestion about the security division is, at least in part, on the basis that most of the members of the security division are, in fact, judges of the Federal Court of Australia.

Mr Barbosa: That would be helpful to the process and we think it would add a layer of independence that makes it a stronger provision.

Mr DREYFUS: Thank you. I'll move to your third principle, which is that there ought to be a specific and complete legal process and clear grounds for challenging use of these powers. Is the bill currently consistent with that third principle?

Mr Barbosa: I don't believe so. In our review of the bill we have seen that it has some limited areas for challenge, which seem to be limited only to the potential conflict with an international agreement. While other areas of Australian law may provide an avenue to raise concerns, we think it's important to include specific provisions in the bill itself. The reason we ask for this—and the reason we outlined this as one of our principles—is, to be frank, technology is complicated and law enforcement may not always know the full extent of what they're asking for when they first come to us. I experienced that frequently as a federal prosecutor. The back and forth between a service provider and law enforcement cannot always be resolved amicably, and it sometimes needs to be brought to a court for resolution if there is a concern that the request may be overbroad or abusive to the extent that it could seek data beyond what is truly necessary. Those are rare instances, but I think provisions that help resolve them are very important.

Mr DREYFUS: Thank you. The fourth principle that you've set out is that there ought to be mechanisms to resolve and raise conflicts with third-country law. Again, I'd ask: is the bill consistent with that fourth principle?

Mr Barbosa: I don't believe so. At this point it doesn't have specific provisions to raise conflicts with third-country law. We have seen that Australian law has a strong tradition of respect for comity, and there may be mechanisms to deal with this. But, again, we would like to see that expressly adopted as part of this act, especially because this bill is to facilitate an international agreement for cross-border access to data. The CLOUD Act and these agreements are inherently designed to try to reduce conflicts, so we don't want a situation where it creates additional conflicts.

Mr DREYFUS: Your sixth principle is one directed to transparency—that providers should have the right to be transparent about how often the government is accessing data. Again, is the bill consistent with that?

Mr Barbosa: The bill has some provisions for transparency and allowing providers to report the number of requests received. We would like to see greater ability to provide granular data—for example, differentiating between requests for content versus non-content—and a clear ability to report numbers related to the number of requests from different parts of the country, for instance. These aspects of transparency, which kind of go hand in hand with the notice issues that we discussed yesterday, are something that we find very important to build trust in government and technology. We receive questions routinely from customers around the world, including government agencies and businesses, who just want to understand how the law works in the day-to-day practice, as they are evaluating what they see as a potential risk in going to the cloud. More transparency helps explain these things to businesses and customers around the world and, as I just stated, it helps the overall system work better and helps all of us do a better job protecting public safety.

Mr DREYFUS: Thanks very much.

Senator STOKER: Thank you for your evidence today. I want to ask you something about your submission in relation to the need for mechanisms to resolve and raise conflicts with third-country laws. What experience do you have of that being a problem to date in other jurisdictions?

Mr Barbosa: Our Microsoft Ireland case is a great example of that, where we saw potential conflicts with European law—which is one of the concerns that motivated us to seek solutions in this area. It's why we filed that case, it's why we highlighted these problems, and it is why we champion the CLOUD Act—because it does provide a path to address these issues.

Senator STOKER: Can you point us to what you say are the models we should be looking to from other jurisdictions as an example of a good way to provide for the resolution of those sorts of conflicts?

Mr Barbosa: Absolutely. The CLOUD Act itself is one example, It provides express mechanisms within the act that address comity and actually strengthen your government's ability to protect its sovereignty, and it strengthens a service provider's right to challenge a US government demand that might conflict with Australian law, for instance. We also see similar provisions in UK law, which are important to us as the UK is about to finalise or has finalised its agreement, and its agreement will come into effect over the course of the next several months. Provisions in the IPO bill that specifically address the potential conflicts with third-country laws would further the overall goals of this whole system.

Senator STOKER: Just to make sure that I understand it correctly: you wouldn't need that in relation to, for instance, the US but you would need it for circumstances in which we're dealing with Australia's interaction with another country? Could you tell me the circumstances in which a provision like that in the IPO bill would be useful to you?

Mr Barbosa: Absolutely. One thing to keep in mind is that, while these are bilateral agreements, we don't live in a bilateral world. Global service providers are doing business all over the world. Take, for instance, the UK and their agreement. It's important that they have provisions to address conflicts of law because, for instance, if the UK were to request data from a global service provider that might conflict with Australian law, that wouldn't be addressed by US law or the bilateral agreement; it has to be addressed in the UK domestic law. Similarly, if Australia entered into an agreement with the United States and then requested data that pertained to a UK person and potentially conflicted with UK law, we would want the ability to address that in Australian courts and raise that potential conflict of law.

Senator STOKER: If we were to provide something a bit like what the CLOUD Act has in the IPO bill, would that create complexities for circumstances in which you were trying to resolve a conflict arising with the US legislation, or do you think it would be sufficiently routine that that would not cause you problems?

Mr Barbosa: The instances in which these conflicts come up are relatively infrequent, so I don't think it would create significant complexities for law enforcement or create significant barriers to protection of public safety or the security of Australia. But when those issues come up it's important that there is a mechanism to address them.

Another aspect—this is something I hadn't commented on before but which we mentioned in our submission—is related to notice. Another aspect of notice that the UK and the US addressed in their agreement was a requirement that the UK notify a third country if one of their demands to a US service provider might impact that third country's citizens. That is another method of addressing those conflicts.

Senator STOKER: I have one final question before I hand over to colleagues. In your submission where you talk about grounds to challenge you've said:

The Bill should explicitly provide a basis to challenge IPOs that are overbroad, abusive, violate the terms of an international agreement or are otherwise unlawful.

What do you have in mind in relation to your concern about each of the categories of overbroad or abusive?

Mr Barbosa: To give an example of a potentially overbroad demand: if law enforcement were to come to us with an identifier that they believed pertained to only one person and were seeking the data for that one person, but it turned out that that identifier was an email address or a domain name that pertained to many individuals—hundreds or more—that is an instance where the request may be overbroad and not reasonable and proportionate to the investigative demand. Those are rare instances, but there needs to be a method to resolve them if they come up. As I said earlier, law enforcement doesn't always know the nature of what is behind an account on the internet. The internet has a great deal of anonymity, so sometimes these issues only come to the surface once law enforcement comes to a service provider.

Senator STOKER: Thank you very much.

CHAIR: Thank you very much, Mr Barbosa and Mr Masters. We've got no further questions for you. We appreciate you appearing before the committee. We'll make sure that you get a transcript of the evidence so you can make any corrections. Once again, I thank you on behalf of the committee.

Proceedings suspended from 10:20 to 10:26

FLETCHER, Mr Brian, Director of Policy, APAC, BSA The Software Alliance

Evidence was taken via teleconference—

CHAIR: I now welcome a representative of BSA The Software Alliance to give evidence. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now invite you to make an opening statement. Thank you for appearing. I do recall, I think, two years ago in Washington DC having an extensive meeting with BSA and the rest of the committee, so we look forward to your evidence.

Mr Fletcher: Thank you, Chair. Good morning, honourable members of the committee. BSA The Software Alliance appreciates the opportunity to speak with the joint committee in connection with its inquiry. BSA is an industry association headquartered in DC, with offices in Latin America, Europe and Asia. Our members include Adobe, Amazon Web Services, Atlassian, Cisco, IBM, Microsoft, Salesforce, Splunk and Twilio, to name a few. They are at the forefront of data driven innovations, including cutting-edge advancements in AI, machine learning, cloud based analytics and the Internet of Things. These innovations are helping to make our devices smarter, our business more competitive and the delivery of government services more efficient.

In close consultation with our members, BSA works with policymakers, stakeholders and legislators globally to ensure our member companies can access global markets in a matter that fits their business models and strategies. Our policy agenda focuses on issues that have the greatest impact on members' ability to innovate and commercialise software products and services globally. So I want to emphasise that BSA and our members fully support the Australian government's desire to have more powerful tools to aid the fight against criminal and terrorist activities. Broadly, we support the bill.

Our members are the recipients of regular lawful requests for information from law enforcement agencies around the world, and they are committed to complying and cooperating with lawful requests for information where possible from a technical and legal perspective in a way that honours the obligation they have to their customers and to the laws to which they're subject. Accessing digital evidence can present tremendous challenges to the privacy and security of technology users unless law enforcement investigations are guided by carefully crafted laws, policies and procedures.

BSA looks at access to digital evidence through a set of five principles. The first is safeguarding fundamental rights. By that, we mean judicial review ensuring due process. There is narrowly targeting requests—specificity of requests and defining content versus noncontent. There is cooperating across borders, ensuring good, strong international treaties, but also considering conflicts of law. There is collaborating with technology providers, ensuring the rights of technology providers. There is verifying the validity and accuracy of requests—technology conflicts and that kind of thing—and ensuring transparency. That is the notification of data subjects and public reporting of requests.

This bill meets a lot of those things. But, on the basis of those five principles, BSA and our members have made seven recommendations to the committee on how the current bill could be strengthened, very much looking at the process around how an IPO would be issued and serviced by a technology provider. Again, I want to thank you for inviting me to participate in the hearing and I look forward to any questions you may have.

CHAIR: Thank you very much, Mr Fletcher.

Mr DREYFUS: Thank you very much for attending, Mr Fletcher. In your submission, you've said this about the need for independent judicial oversight of the issuing of international production orders:

We are concerned that the AAT may not be seen as sufficiently independent in the IPO issuance process to ensure public and overseas government trust.

Are you able to elaborate on that?

Mr Fletcher: Thank you for the question, Mr Dreyfus. On the issuing of this type of legal instrument to access digital evidence, our strong preference is for judicial oversight. That said, we recognise—and certainly the US CLOUD Act, which, again, we support, requires—that orders issued by a foreign government be subject to review oversight by a court, judge, magistrate or other independent authority. The actual independence of the AAT is not something that I want to comment on. We're concerned about the perception and trust that are so important in maintaining the digital economy, and that is trust from the consumers of the digital product around the world, from the individual citizens and the businesses that use these products and from international governments that may enter into treaties with Australia in order to exchange information in a trusted way. The fact that we can have these conversations about the AAT does give us concern that people may not see them as

independent. We don't necessarily have to have these conversations generally when we're talking about judicial oversight.

Mr DREYFUS: As I understand your submission, and you've just elaborated on it, you're not so much going to the actual members of the AAT but to the constitutional position of the AAT, which is that it is part of the executive of the Australian government.

Mr Fletcher: There certainly could be a perception by both the citizens of Australia and people around the world that, in being a member of the executive branch, this—approving its own requests—could be seen as the Australian government marking its own homework. Again, I want to emphasise that I'm not suggesting that that is what is happening. We're concerned about trust in the technology and building the digital economy.

Mr DREYFUS: I want to go to a more practical matter. Does the software alliance have a view on the efficacy of the current mutual legal assistance provisions which this scheme intends to replace?

Mr Fletcher: I may have to take that one on notice; my apologies.

Mr DREYFUS: That's alright. At a more general level, can the software alliance provide examples of why consultation with providers on telecommunications matters is important?

Mr Fletcher: Thank you again for the question, Mr Dreyfus. When requests come forward to technology providers, there are many things that need to be considered from a technology perspective—and rarely will the requesting agency understand them. These include how the internal systems are architected, how data is accessed and indexed, where the data is located and any potential conflicts of law that may introduce. What we're interested in ensuring is that, once an IPO or similar instrument around the world is issued, it's able to be serviced quickly and efficiently by the provider. Preconsultation with the provider will allow them to say: 'These are the types of information that we need in order to get your record.' For example, an IP address is often considered to be a strong indicator of somebody at the other end somewhere around the world. That actually may not be particularly useful when it comes to seeking information out of providers' systems. There might be some other piece of information, which, again, may actually already be in possession of the law enforcement agency that they could provide to speed up that process and ensure that there's an efficient and quick recall of the information requested.

Mr DREYFUS: Thanks very much.

Senator FAWCETT: My question was very similar to Mr Dreyfus's last one about formats and whether things were technically possible. In your presentation you talked about whether things were actually technically possible. Do you have any examples of where requests from agencies in the past have not been technically possible for companies?

Mr Fletcher: I can't give you specific examples, but certainly, theoretically, their request for an IP address is sometimes not particularly useful for a whole heap of technical reasons about how the internet works and how providers record information inside their systems. There's also a potential concern that an IPO could be issued for data that doesn't exist. I can give you a potential example of a request for data that is over 30 days old that may have been purged from a provider's system under the requirements of privacy laws from other jurisdictions. That would no longer be able to be accessed, and not being able to comply with an IPO could put a provider in a concerning situation.

Mr BYRNE: I want to go further and drill down with a more granular level of specificity. Can you give a practical example of that? That's good theoretically, but is there something that you could talk about that is a tangible example of that? What data are you talking about? What's being held that might be purged after 30 days?

Mr Fletcher: Again, I might take that on notice, if you don't mind, Senator. But certainly I call attention to something like Europe's general data protection regulations, which basically require that data is managed in an overall lifecycle manner—specifically when it comes to personal data.

Mr BYRNE: You might need to take that on notice. I'm sorry for cutting across you, Senator Fawcett, but we spoke to the intelligence agencies about metadata and about data that they could access and what they do, and we know very specifically what information they're after. I'm keen to know exactly what you're talking about with a specific example so I can help inform my decision-making process. That's why I'm asking you. I'm sorry for cutting across Senator Fawcett—and thank you for calling me Senator; I've been called many things, but not that!

Mr Fletcher: I beg your pardon, Sir.

Mr BYRNE: I'm a member of the House of Representative. But thanks.

Senator FAWCETT: He aspires to be reborn into a higher place!

Mr BYRNE: I've been elected by my constituents. It's a designated constituency.

Senator FAWCETT: Do you believe that the proposed legislation has adequate safeguards or recourses? If a provider was in the situation where a piece of data was asked for that another jurisdiction—for example, due to privacy legislation—had required to be purged, do you believe that a provider is adequately covered or do you think they would be exposed to action under this legislation?

Mr Fletcher: I beg your pardon, but who is speaking?

Senator FAWCETT: It is Senator Fawcett—the one senator in the room.

Mr Fletcher: To directly answer your question, no, we don't think there is adequate redress in the current bill. As we understand the bill as drafted, the only reason that a provider could challenge an IPO that had been issued to them would be in writing to the Australian designated authority on the basis that the IPO does not meet the designated international agreement. We would like to see the ability for technology providers to challenge on a wide range of considerations, including that the data that no longer exists.

Senator FAWCETT: There are two issues there. One is upon what grounds you could challenge the release of data that one holds but the nil return, where data has been required to be destroyed by another regulatory agency, would seem to be quite a separate distinct case from a provider who didn't believe they should be providing data. Would you see it as adequate if there was a carve-out for something that was required under the legislation or regulations of another nation state that was an automatic defence as opposed to a broad ability to challenge, which would appear to bog down and perhaps undermine the efficacy of the program if we are looking for a timely response to assist law enforcement?

Mr Fletcher: I understand what you are saying and, certainly, speed of response is extremely important when it comes to law enforcement support. It's still our preference that vendors are able to challenge on a wide range of issues very much in that it allows trust in the system to build and allows foreign governments and the citizens that use these products to trust that, when their data is accessed, that is done under a very rigorous and decisive process. In terms of a carve-out, we would certainly support that in a case where we couldn't get a full review, but our strong preference would be for a right of full appeal.

CHAIR: Thank you very much, Mr Fletcher. I don't think we have any more questions for you. I thank you again for appearing and I also thank BSA for the work that they contribute to inquiries. Thank you for your evidence. We will give you the opportunity to make corrections to your evidence in due course.

FRANKLIN, Ms Sharon Bradford, International Civil Liberties and Technology Coalition

KRAHULCOVA, Ms Lucie, International Civil Liberties and Technology Coalition

Evidence was taken via teleconference—

[10:46]

CHAIR: I now welcome representatives from the International Civil Liberties and Technology Coalition to give evidence. Do you have any comments to make on the capacity in which you appear before the committee?

Ms Franklin: I am the policy director for New America's Open Technology Institute and I am appearing on behalf of our International Civil Liberties and Technology Coalition of 32 members, comprised of civil society organisations and tech companies.

Ms Krahulcova: I work as a policy analyst at Access Now and I'm a board member at Digital Rights Watch as well. Like Sharon, I'm appearing here today on behalf of the International Civil Liberties and Technology Coalition under which we filed the comments.

CHAIR: Thank you very much for appearing at your time of night. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now invite you to make a brief opening statement before we proceed to discussion.

Ms Franklin: Thank you for the opportunity to testify before you today. I'm an attorney in the United States and I serve as policy director for New America's Open Technology Institute, which is a digital rights organisation. I'm appearing on behalf of our International Civil Liberties and Technology Coalition of 32 members that submitted comments regarding this committee's review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020. I will address two of the four issues that we covered in our comments and my colleague Lucie Krahulcova will address the other two points.

Before doing so, I would like to provide a brief background about the US CLOUD Act, which contains two parts. The first part of the CLOUD Act resolves a lawsuit called United States versus Microsoft, or Microsoft Ireland, in which the US government sought, under the US Stored Communications Act, to obtain electronic communications held by Microsoft on a server in Ireland. The first part of the CLOUD Act now clarifies that US government requests under the Stored Communications Act of companies that are under US jurisdiction apply, regardless of whether the data is located within or outside of the United States. The second part of the US CLOUD Act is directly relevant to the international production orders bill. It sets up a process through which countries like Australia can enter into a bilateral agreement with the United States that will enable each country to bypass the time-consuming traditional mutual legal assistance treaty, or MLAT, process for gaining access to electronic communications information. This will allow law enforcement officials in each country to make direct requests to providers in the other country in order to obtain communications information like emails.

Under the CLOUD Act process, first the US Attorney-General and Secretary of State must certify that the other country meets a series of factors demonstrating robust protections for privacy and civil liberties and respect for human rights. Then the two countries negotiate a bilateral executive agreement, and the CLOUD Act sets out minimum criteria for these agreements. Once negotiated, the agreement must be submitted to the US Congress, which has 180 days to disapprove of the agreement before it goes into effect. The CLOUD Act requirements for the bilateral agreements should be considered the floor, and not the ceiling, for the safeguards that are necessary.

As you know, the international production orders bill is designed to qualify Australia to enter into a CLOUD Act agreement with the United States. Our coalition has raised four concerns regarding why this draft legislation is not adequate to provide the robust level of safeguards needed. I will address two of these. First, the bill fails to ensure prior judicial review under a robust legal standard. CLOUD Act bilateral agreements are designed to replace the judicial review that, under the current MLAT system, is conducted by the home country. Individualised review by an independent authority is a fundamental protection under international human rights law. The international production orders bill does contain mechanisms for prior review, but these include review by the Administrative Appeals Tribunal, which is a part of the executive branch.

In addition, the CLOUD Act requires a robust standard of review for data requests, specifically that they shall be based on 'requirements for reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation'. However, the international production orders bill does not require any showing at all that the person being investigated has committed any wrongdoing or is tied to

any wrongdoing. Instead, it simply requires that there are 'reasonable grounds for suspecting' that the communications provider offers services and that a targeted person is using the services, and then that they are likely to obtain information that would assist in their investigation. Then the bill lists a series of matters to be considered, including how much privacy will be interfered with and the gravity of the conduct. Here, too, there is no rule defining how authorities should weigh these various factors. Rather, it appears to provide the deciding officials with broad discretion in conducting the review.

Second, the bill fails to provide a clear and robust mechanism for providers to challenge inappropriate and overbroad requests. This is another key principle for a rights protective system for cross-border access to data. Providers receiving direct requests from foreign countries must have an opportunity to challenge overbroad or otherwise unlawful demands prior to disclosing their customers' sensitive data. Specifically, there should be a procedure that protects the rights of providers to seek clarification from requesting countries about data requests and the system should establish a clear procedure for an independent authority to hear and adjudicate providers' challenges to data requests. The international production orders bill fails to provide a sufficient procedure for challenges and only notes that challenges can be filed.

I will now turn this over to my colleague, who will address the remaining two concerns in our coalition's comments, and I will then be happy to answer your questions. Thank you.

CHAIR: Thank you very much.

Ms Krahulcova: Good morning and thank you for the opportunity to further explore some of the concerns that we raised in our coalition's comments. As you know, contrary to the documentation that was supplied with this bill, we have concluded in our analysis that the bill does not provide sufficient safeguards to protect human rights. Before I delve into the two points that Sharon mentioned, one of the big overarching concerns that we have is that the bill, as it stands, compounds some of the issues under TOLA as well as the data retention inquiry. To that extent, I think it's worth noting the 4 October 2019 letter from Jerrold Nadler, who is the chairman of the US House of Representatives Committee on the Judiciary. He raised the issue that some of the provisions under TOLA, as they infringe upon individuals' rights, would preclude Australia from successfully reaching a CLOUD agreement with the US. As you may be aware within this committee, we've been extensively involved throughout the review in assistance and access in TOLA. Some of the concerns that I'm about to go over have been part of those conversations as well. I've raised them both with this committee, as well as with the independent review that's being conducted by Dr James Renwick. I know that we will get to the ins and outs of some of the points in this legislation and what could be made better, but I would strongly urge this committee to table this bill, at least until the ongoing review of TOLA is completed and until the independent assessment of individual rights under TOLA is completed, before we introduce an extraterritorial dimension, essentially, to some of the powers that are enshrined in it.

There are the other two points that Sharon mentioned—and I'm mindful of time, so I won't go over them—notice and transparency, as well as the compulsory nature of IPOs. In our submission, we wrote that the current bill does not include a mechanism requirement for government officials to notify subjects of data requests. This is the same challenge under TOLA: that individuals have a right to be notified. This goes back to Sharon's point—an individual's right as well as a company's right to challenge requests. In the explanatory memorandum, they do provide that individuals can challenge in court, as part of a court criminal proceeding. However, it is my understanding that, under TOLA as well as under this bill, requests will often be made to inform an investigation or a request will be made under which criminal proceedings aren't undertaken. So, essentially, for anyone whose case doesn't escalate to the court, where they can deploy that mechanism, where they're notified of the [interruption] understand. This is what we brought up as well in the case of US law. There will be cases where you cannot proactively inform individuals that they are subject to warrants, but, once the investigation has concluded, there should be notification to individuals that their privacy was infringed upon. There should be notification, and individuals who were subject to the provision should have a right to understand, ask questions and challenge in court if they believe that it was arbitrary or unlawful.

The last thing I'll mention is, going back to what Sharon mentioned about the company having a right to stand up for an individual, under TOLA—you may know this from my comments under that legislation—that right is removed, because the company cannot be subject to individual action on the basis of a breach of privacy. I think that's a flaw that we're seeing here, further compounded by the nature of the IPOs being mandatory.

One of the things I want to flag is that I understand there is the introduction of the public monitors as a part of the bill. As we know, those only operate in Victorian and Queensland. So I think there are deficiencies in terms of individuals rights' and representation that need to be remedied. Again, I would urge this committee to defer this until the review of TOLA is completed and those deficiencies have been addressed.

CHAIR: Thank you very much again for appearing today. If we could go to page 3 of your submission, where you state in paragraph 4, 'In general, users have a universal right to notice.' Perhaps you could start off a discussion about the right to notice and balancing that against the risk of destruction of evidence. Could you go into a bit more detail, and perhaps also talk about the example you give of the destruction of physical property on page 4? Is that the same as the destruction of electronic material?

Ms Krahulcova: The Fourth Amendment details that we list on page 4—If individuals are to exercise their rights, there has to be a notification. We've had that conversation within the independent review of TOLA as well. I think an essential component of that is missing. Ultimately, the access to remedies and redress is subject to individuals being notified that they were implicated in such an investigation. That is a key component of individuals exercising their rights. That said, of course, as I mentioned and as the bill foresees, notice can be delayed for an investigation. However, it shouldn't be completely disregarded. I don't know if Sharon wants to add on that and on the US component.

Ms Franklin: Yes, the notice can certainly be delayed as appropriate to avoid interfering with an investigation, but we're talking about the gathering of evidence in connection with a prosecution. Certainly that notice does need to occur, even though delay can be appropriate.

CHAIR: Thank you. Accordingly to Microsoft's law enforcement requests report, approximately 23 per cent of legal requests for data were rejected in 2019. In the view of the coalition, are communication providers well placed to challenge orders that exceed the provisions of international agreements?

Ms Franklin: That's the point I was addressing about the importance of providing a mechanism for providers to file those challenges, particularly in light of what we were just discussing, where there may be a need to delay notice so the subject would not be aware of the request and would not be in a position to defend their own rights. The provider will have the ability to see requests and, if there are a number of these, particularly with the larger providers, and to be familiar with what the appropriate scope is and to question whether a request may be overbroad or otherwise inappropriate.

Ms Krahulcova: In practice we have to look at what happens here and the sort of interests that are at play—whether it's a law enforcement agency or an intelligence agency almost directly submitting an IPO, for instance for telecommunications data. The discretion doesn't have to be exercised. They can go direct. There's no intervention on behalf of the individual. There should be an interactive notification for individuals. But I think you have to look at the weighing mechanism, when a warrant like that is presented, of who is representing the individual. Often this ends up being companies just because they have the legal team and they are bound by consumer legislation in different jurisdictions to respect individuals' rights. As I flagged, my concern is that this sort of mechanism that the individual has over the company has been removed. I think that's a huge area of concern. I was part of the EU negotiations on very similar mechanisms for several years when I worked in Brussels. From my perspective, companies being in a position to reject requests is not a perfect system, but it is often the last frontier for individuals' rights, because there isn't a human rights body or an independent reviewer who is part of that mechanism. Again, I recognise that there are public interest monitors who would be engaged in several states as a part of that process. However, that sort of neutral or independent reviewer should be part of every evaluation that happens, because there is such a power discrepancy between an agency going directly or an agency with the Attorney-General's signing-off going directly to the company, where the company is not liable to the user. It presents a really tragic power paradigm.

Senator FAWCETT: Can I segue off that last point you made. On page 5 you talk about concerns about extra-territorial jurisdiction as a result of civil penalties for non-compliance. Most legislation, to be effective, has some penalties for non-compliance, either criminal or civil. If you don't support the existing form, how would you suggest that it is made effective such that non-compliance is discouraged?

Ms Krahulcova: I think that's a great question and it's something that any mechanism that tries to replace or supersede a mutual legal assistance treaty, which is kind of what this lays the ground for, will inevitably suffer from an extraterritoriality because you are exerting kind of power in another territory. I would say that this is not just a problem of this particular bill; it generally comes up with these types of mechanisms.

I think currently there is unfortunate public discourse around the use of Amazon servers for a contact-tracing app. I'll use this as an example—it's not a perfect one. But one of the things that the government has to start to do is to assure individuals that their data won't be shared by Amazon with US entities and that data won't leave. I'm not going to argue about whether that's a concern for this committee at the moment, but it's not something that Australia can guarantee. Amazon is still an entity. It's a US based entity, and when we get into a place where governments put provisions like this into legislation there is simply no way, unless there is a very expensive diplomatic undertaking and extreme carve-outs are sought, to guarantee that. Our concern, I guess, is about a

framework that's set up in the future and which countries have that discretion over others. I would urge this committee to consider the sorts of implications that creates for the international regime more broadly. I don't know if Sharon has anything to add to that.

Ms Franklin: The one thing I would add is that, as I noted, the structure under the CLOUD Act is designed to bypass the MLAT process, but when you ask about how you would ever enforce it, ultimately the MLAT process will still be in place as a backstop where needed.

Senator FAWCETT: Perhaps I could just go to the principle. We're moving away from here from data and to the principle of a sovereign state achieving an outcome that's deemed desirable. If we look at, for example, modern slavery legislation, there is some discussion even in the US at the moment—certainly in other places—that where you have an example of a multinational company who has in their supply chain forced labour or modern slavery conditions that they haven't taken action on whether there should be civil penalties applied to them in the country where they're selling their product as opposed to the country where the modern slavery conditions exist. That seems to have fairly broad support, but isn't that essentially applying a penalty in one country for an action that was taken in another country?

Ms Franklin: This is I think less about penalty than an attempt to exert jurisdiction over data that is held in a different country. Although, how far can one country reach into the other where the provider is located to demand the data? To date, that has been only through government-to-government requests under the mutual legal assistance treaty process. The CLOUD Act structure is designed to create a more streamlined process, recognising that in the MLAT process is rights-protective but cumbersome, so it's a question of how far one country can reach into the others. I think it's a jurisdictional question separate from how you can condition the rights of companies that try to do business within your borders.

Senator FAWCETT: I accept that; thanks.

Ms Krahulcova: If I can just supplement: I'm not superfamiliar with the example that you used of slavery, but there are different standards—and the bill goes back and forth on the different standards: this will be for a serious criminal offence, this will be for terrorism, this will be for enforcement. These standards vary greatly internationally, and one of the things we struggled with even at the European level was to arrive at an understanding of what could constitute something like this where that sort of infringement on people who are residing in another country would be proportionate and lawful under the jurisdiction of another country and even within the EU where there's key legislation and a lot of harmonisation. We were not simply able to arrive at a conclusion. I think some of our members voted in terms of if there's a minimum penalty of five years, three years or seven years and the reality is just that those frameworks differ.

There's a reason that MLAT is a higher part of a more diplomatic international framework rather than domestic legislation, and I know that creates a lot of frustration for folks in Home Affairs, not just here but elsewhere as well. But the reality is that that's there for a reason, and something like interfering with slavery and enforcing human rights, I think I could see that as being a noble reason to interfere and exert that sort of power. But here we have seen huge infringements, and I'm not convinced, as I outlined, because of the challenges that exist within Australian systems that have been really amplified by TOLA. I'm not convinced that Australia should be seeking to exert that power externally.

Mr DREYFUS: I've got a question for Ms Franklin. The Department of Home Affairs has told this committee that it consulted with the United States Department of Justice on the measures in this bill. That suggests that the Australian government is confident that this bill does in fact provide sufficiently robust protections for privacy and civil liberties as required by the CLOUD Act. Do you take any comfort from the fact that the department has consulted with the US Department of Justice?

Ms Franklin: I am glad to know that they are talking to each other, but I know that there is not a procedure for prior certification, to my knowledge. The Department of Justice has reached out to various civil society organisations in the US and elsewhere for consultation on what kinds of requirements should be in place. The one that I focused on that are contained in our comments that I talked about here today, including prior judicial review under a robust legal standard and an opportunity for companies to be able to object, are ones that we have continued to have a dialogue with the Department of Justice on. They don't necessarily always speak with one voice either.

I will also note that, although it is not a strong safeguard from our point of view, there is at the end of the day the ability for our congress to weigh in on the terms of the agreement as well. We have continued to urge that the bare minimum requirements in the CLOUD Act are just that, bare minimum and that the implementation should seek to be as rights protective as possible.

Mr DREYFUS: You've come now to the other part of the process. You've mentioned the congressional approval. When you were speaking in your introduction you mentioned the letter from Congressman Nadler to the Australian Minister for Home Affairs. Can you explain that approval process through the congress—in other words, what role will congress play in this process?

Ms Franklin: Unfortunately, from my perspective, to be perfectly candid, congressional approval is not required. The way it works is that once the agreement is finalised our justice department must submit it to both houses of Congress, and that starts a clock ticking for a 180-day period. The CLOUD Act contains some fairly detailed description of a procedure that congress can follow to disapprove of a CLOUD Act agreement, but if Congress does nothing during those 180 days then it will go into effect. The procedure is to enable congress to act more quickly than it normally would, so that is an important tool. In fairness, it is not a congressional approval requirement so it is not as robust a check as we would have hoped when the CLOUD Act was being enacted.

Mr DREYFUS: We're familiar with that process here. We also have a disapproval process by the parliament for regulations and treaties. But it's the case that, even if the US Department of Justice is satisfied with the measures in the bill, the United States Congress might form a different view and decline to endorse an executive agreement.

Ms Franklin: That is correct.

Mr DREYFUS: In the light of the letter that Congressman Nadler has sent to the Australian Minister for Home Affairs, do you think that, as drafted, this bill will satisfy the Department of Justice and the US Congress that Australia provides sufficient robust protections for privacy and civil liberties for the purposes of the CLOUD Act?

Ms Franklin: I hesitate to forecast anything that our congress will do. I think, as we have pointed out, that there are some real questions and that you would be well served to make those safeguards sufficiently robust so that there won't be those questions and concerns in play.

Mr DREYFUS: Thank you. Perhaps I could just go to a specific matter. You've noted in your submission that this committee has a current inquiry into TOLA, and we've also got another current inquiry into press freedom in Australia. This goes to the matter that you've both raised about human rights protections. The Australian Inspector-General of Intelligence and Security has drawn this committee's attention to the fact that, unlike the current domestic data access regime for access to telecommunications data, the international production orders bill does not include any specific protections for journalists. As I just said, we are conducting another inquiry into press freedom in Australia. I can't recall a single person telling this committee that existing protections for journalists in Australian law should be watered down. Not even the current government has said that. But, incredibly, this bill that is now before the committee appears to water down existing protections for journalists. Does this concern you?

Ms Krahulcova: Maybe I can jump in on that one. I think that's a fantastic question. Drawing that sort of parallel between the different pieces of legislation, I think, is really essential, so thank you for that. Yes, I would be concerned. At Access Now, we haven't focused extensively on freedom of expression, but Digital Rights Watch and other Australian digital rights groups have, and it is of high concern.

To go back to the extraterritoriality and the incoming orders and requests under part 13 of the schedule: it removes blocking provisions mutually, so not only is Australia able to go directly to the IPO but that is reciprocated in the bill. Through the way it's written, there's absolutely nothing that would give you the ability to stop the request to that extent, not just from the US but from anyone that Australia would seek to implement an agreement like that with, which seems from the explanatory memorandum to be any 'like-minded' country. So I'd be really concerned about the impact that's going to have on journalists and on the integrity of communications in general, even for lawyers, politicians and others.

Mr DREYFUS: So I take it you're suggesting that the bill should expressly require some minimum level of protection for journalists.

Ms Krahulcova: I wouldn't classify journalists as a specific category. I think they're a great example of where the real risks are, though. There are other extremely vulnerable people—political dissidents and other individuals—who would benefit from the same sort of protections that you're suggesting journalists have. But ultimately, yes, I think this does compromise freedom of expression and journalistic integrity.

Mr DREYFUS: Thank you. I will just tease out something that you've been reasonably clear on in the written submission. As I understand your position, the Australian Administrative Appeals Tribunal, from your point of view, simply does not satisfy the requirement for independent authorisation that would be adequate to protect the rights of individuals.

Ms Krahulcova: That is correct, yes.

Ms Franklin: Yes. From what we understand, the Administrative Appeals Tribunal is part of the executive branch. It is not equivalent to independent judicial officials, so it does not provide that level of independence. I would also just reiterate concerns about the standard of review not meeting the requirements of the CLOUD Act or the sufficiently robust standard. I quoted from the standard in my opening remarks.

Mr DREYFUS: You've correctly made the point that this is something that the Independent National Security Legislation Monitor, Dr Renwick, is looking at in his review of TOLA, and this committee will almost certainly be looking at it in our review of TOLA, which is upcoming.

Ms Krahulcova: Yes. This is something that we brought up with Dr James Renwick, and he has been extremely concerned. I think he draws a comparison with the UK Investigatory Powers Act and some of the other mechanisms in the UK, which enjoy something that's called the double-lock mechanism. I think that sort of objective independence is not guaranteed under the AAT structure, so I would look forward to what both the committee inquiry and his own review yield on that.

Mr DREYFUS: Thank you very much.

Ms Franklin: If I can just add to that, our coalition, or substantially overlapping members of the coalition, also submitted comments in connection with that review back in July of 2019, and specifically in connection with the request to address the interaction with foreign laws including the US CLOUD Act. Those comments addressed our concerns in that regard, particularly noting the issue of the lack of independent judicial review.

Mr DREYFUS: Thank you very much.

CHAIR: Thank you very much again for your evidence and for appearing before the committee today. If you have anything to add, could you get it to the secretariat by Thursday next week. We'll also give you a transcript of your evidence so you can make any corrections. Thank you again on behalf of us all.

Ms Krahulcova: Thank you so much for the opportunity.

BENSCH, Ms Nikki, Director Legal, Australian Commission for Law Enforcement Integrity

HINCHCLIFFE, Ms Jaala, Integrity Commissioner, Australian Commission for Law Enforcement Integrity

Evidence was taken via teleconference—

[11:33]

CHAIR: I now welcome representatives of the Australian Commission for Law Enforcement Integrity to give evidence. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now hand over to you to make a brief opening statement before we proceed to discussion.

Ms Hinchcliffe: Thank you very much, Chair. I do have a very brief opening statement to make. Thank you for the opportunity to give evidence and answer questions today. I'm taking the opportunity to provide an opening statement because it's the first time I've appeared before this committee in my new role as the Integrity Commissioner, although I've appeared before you on several occasions in my previous role as the Deputy Commonwealth Ombudsman.

ACLEI is a unique agency in the Commonwealth because we're both an oversight agency and a law enforcement agency. In my oversight role I oversee the corruption framework which is set out in my act, the Law Enforcement Integrity Commissioner Act, across the five Commonwealth law enforcement agencies that are subject to my jurisdiction. Those agencies are: the AFP; the ACIC; AUSTRAC; the Department of Home Affairs, including the ABF; and particular parts of the Department of Agriculture, Water and the Environment.

As well as being an oversight agency, ACLEI is also a law enforcement agency in our own right, albeit a very small one. In order to conduct serious and systemic corruption investigations that my act tells me to focus on, I need the powers of a law enforcement agency, along with several others, including hearing powers, that I have within my act. These law enforcement powers that I have include powers in relation to telecommunications intercepts, stored communications, communications data and surveillance devices.

I come to this hearing, and to hearings like this, over my term as Integrity Commissioner with both of those roles in mind. I will carefully consider submissions that I make for additional powers as a law enforcement agency, such as the submission that I've made here today in support for this bill as it relates to ACLEI. I will also carefully consider the proposed oversight mechanism or any additional powers as a control to ensure that the powers are being utilised as parliament intended and also as a potential corruption prevention mechanism as a control to ensure that the powers are not being utilised for corrupt purposes by law enforcement agencies or staff of those agencies. With that said, I will hand over for questions.

CHAIR: Thank you very much.

Mr LEESER: In your submission, on page 3, looking at the current Mutual Assistance in Criminal Matters Act, you have the following to say:

> Our experience using this mutual legal assistance regime for accessing this information from foreign communications providers is that it is time consuming and slow. Significant delays may occur in the execution of requests at multiple points; in the application, transmission and execution of a mutual assistance request. Such delays might ultimately slow down and hinder the investigation.

I wonder if you could give us some information or some more specifics about dealing with the mutual assistance law and how important getting information in a timely manner in these sorts of investigations can be.

Ms Hinchcliffe: Of course. In our submission we provide an example of what we mean by that in relation to an operation called Operation Murray. In that case we made a request for data that was held in relation to an email account that was held offshore. We did that through the mutual assistance request process. To give an example of the types of time frames, in that matter there was a preservation request made in August 2013. There was then the mutual assistance request sent in October 2013. The investigation then progressed while we awaited the outcome of that, and it progressed quite quickly, for various other reasons. We eventually received the material in August 2014, and by that stage the investigation was in its final process and was about to be completed at the investigation stage and move on to the prosecution stage.

While those time frames may not necessarily seem large—12 to 18 months has been the kind of example given for mutual assistance requests. We only deal with these mutual assistance requests very rarely, so our experience is limited. When you're in the midst of an investigation, particularly in those early stages when you are looking

for this type of information to help to build an understanding of what has occurred and where to look for further evidence, it's imperative that you get that information in a timely manner. That helps the investigation to progress. We were fortunate that in this particular operation we were able to utilise other information. At the end, as we said in our submission, the information that came back from the mutual assistance request had limited utility. But that's the kind of time frame that we're referring to in that part of our submission.

Mr LEESER: You also said on page 4 of your submission that, if this bill is passed, you will pursue information of this kind with more regularity. Do you have any sense about how often you would seek IPOs?

Ms Hinchcliffe: Of course it's always difficult to say, because it will depend on the investigation, but I will caveat what I'm saying with this point: as I said in my opening, we are a very small agency, and so the number of investigations that we can conduct, compared to the other law enforcement agencies that you might speak to such as the AFP, are very small. I did have a look to give you a sense of the number of telecommunication intercepts and stored communications applications that we've done in the last two years. In 2018-19 we made 11 applications for telecommunication intercept warrants and no applications for stored communications. So far this year we've made no telecommunication warrant applications and we've made two applications for stored communication. So you can see that the numbers we make under the current regime are very small. I suspect that, if the bill passes and if an international agreement is made, which is required so that the bill has effect, we will then probably look to whether we seek an IPO when we are seeking, in particular, a stored communication or a telecommunications data application to make sure that we have full coverage of the communications that are occurring in relation to that particular investigation. But we will consider that on a case-by-case basis, and it will really depend on what intelligence and what evidence we have at that point about what communications means the person of interest is using.

Mr LEESER: Thanks, Ms Hinchcliffe.

Senator FAWCETT: I will come to two points. Previous witnesses have talked about the desirability of allowing communications providers to challenge orders that they believed exceeded the provisions of international agreements. In your experience, would providing such a pathway be effective, or would it allow people to challenge the interpretation of what international agreements provide for and thus introduce additional delays in accessing information that's required for a criminal investigation?

Ms Hinchcliffe: I think that that will be an issue where we will need to see how that process operates. I can foresee the ability of that to create delays. As I've said, at the point of the investigation when we're seeking these materials, it's often at a critical stage where time is of the essence. That's why we see merit in relation to this bill as opposed to the current methods that we have.

I'm also conscious of the fact that at this point of the investigation usually we are in a covert stage rather than in an overt stage, and so any mechanism that is available for the providers to challenge would need to ensure that the nature of the investigation at that covert stage is able to be maintained.

Senator FAWCETT: Other witnesses have also expressed concerns about the fact that the bill contains civil penalties for noncompliance and that it can create an extraterritorial jurisdiction. Do you have any concerns in that regard? Is that something that you have experience with in other areas of Australian law? Could you comment on the operation of any other areas that are comparable?

Ms Hinchcliffe: I think that that is actually outside of my jurisdiction to comment on. That may be a better question for the Attorney-General's Department or the Department of Home Affairs given that they have the policy for this bill. I'm not sure that I have anything in particular to say on that point. That really goes to issues of international law, which are outside of my specialty.

Senator FAWCETT: Sure. A final question: concerns have been expressed about the fact that a review might be conducted by the AAT as opposed to a judicial officer. In your experience in the Australian legal construct, do you have any concerns about review by the AAT?

Ms Hinchcliffe: Our experience under the current regime is that both AAT members and judicial officers can be issuing officers under several of these regimes. We note that under the proposed bill that would also be expanded across to telecommunications data as well. I have not had any concerns about the operation of those issuing officer provisions. It seems to me that issuing officers come to these decisions with seriousness and with a respect for the requirements of the law, which are set out in quite some detail in the Telecommunications (Interception and Access) Act, and they make those considerations carefully before they decide whether or not to issue the warrant that's being considered.

Senator FAWCETT: Thanks.

Senator ABETZ: I refer to page 3 of your submission, in which you tell us about the difficulties with the Mutual Assistance in Criminal Matters Act and you refer to a few of what I will refer to as 'speed humps'—namely, application, transmission and execution. You then give us the case study of Operation Murray. I understand it took us about 10 months from the time the request was initially made to when access was provided. Was that a one-off 10 months, or is that a normal, average delay?

Ms Hinchcliffe: As I was indicating before, because of the time frame that it takes, we have limited use of the mutual assistance act. Our experience—and Operation Murray bears this out—is that 10 months is not an outlier and that these processes can take between 12 and 18 months. I think that that's borne out in the submission by the CDPP to this inquiry.

Senator ABETZ: On the top of page 4 of your submission you say:

For these reasons, ACLEI has not sought information of this kind with regularity in the past.

Are you able to advise us or remind us of how often such requests have been made?

Ms Hinchcliffe: I don't have that information in front of me, but I'm happy to take that on notice.

Senator ABETZ: If you could, I'd be much obliged. Thank you.

CHAIR: Thank you very much for your evidence and also for appearing before the committee. We have no further questions, but, if you have anything further, could you get that to the secretariat by Thursday next week. Of course you will get a transcript of your evidence so you can make any corrections. I thank you again on behalf of the committee.

FITZGERALD, Mr Michael, Assistant Commissioner and Commander, Forensic Evidence and Technical Services Command, New South Wales Police Force

Evidence was taken via teleconference—

[11:54]

CHAIR: Welcome. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and therefore has the same standing as proceedings of the respective houses. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard and attracts parliamentary privilege. I now invite you to make a brief opening statement before we proceed to discussion.

Mr Fitzgerald: I appreciate the committee extending an invitation to the New South Wales Police Force to not only provide a submission but also provide evidence. As the committee will know, the New South Wales Police Force exercises powers under the Telecommunications (Interception and Access) Act more than any other state law enforcement agency in the country. Except for the need to obtain an international production order for metadata, the proposed new legislation has many working similarities to the Telecommunications (Interception and Access) Act. The bill, if passed, will provide the New South Wales Police Force and its partner agencies with unprecedented but necessary capacity to expedite investigations into serious crime beyond our territorial limits.

The New South Wales Police Force already has in place a well-established legal unit and a telecommunications interception unit that is capable of maintaining and facilitating international production orders on behalf of investigators. The international production orders will be provided to an Australian designated authority, who, in conjunction with the Commonwealth Ombudsman, will ensure the orders are compliant with the designated international agreement nominated in the international production order.

The New South Wales Police Force understand that, like the TIA Act, we are responsible for protecting the privacy of individuals, and we understand the importance surrounding the strict compliance rules around reporting, recordkeeping, the destruction of records and disclosure of protected information. I can assure the committee that those tasks are well resourced from a New South Wales Police Force perspective and will continue to be so resourced for this new regime to ensure its integrity. The mandate of the Commonwealth Ombudsman to vigorously review the activities of the New South Wales Police Force is supported, and we will continue to work closely with the Commonwealth in regard to safeguarding this legislation.

Evidence of conversation, stored communications and relevant data such as call charge records regularly links offenders to victims and crime scenes. This evidence also assists investigators to identify and exculpate innocent parties. Like the Telecommunications (Interception and Access) Act, the proposed legislation justifiably limits the types of offences that can be investigated. The issue of costs associated with inquiries done through international production orders may also ultimately determine prioritisation of requests by the New South Wales Police Force.

The current process used by police to obtain information is via the mutual legal assistance treaty process. On average, these requests take from six months to over two years, if they are even answered at all. An international production order regime will alleviate these time delays and frustrations to the administration of justice. The mutual legal assistance treaty process commences with the New South Wales Police Force drafting an affidavit and several other documents, which, in most cases, satisfy probable cause in the USA. The material is robustly vetted by the Commonwealth Attorney-General before that office makes a request to the government of the United States for relevant assistance. The FBI is then engaged to obtain a warrant, and they then call upon the local US police jurisdiction to execute the warrant to obtain the required information. The requested information then flows back through the same chain, and eventually the material is returned to New South Wales. As we say, this can take up to 12 months for the execution of a warrant on a service provider or carrier. I can provide examples of excessive time delays that have occurred in murder, child abuse and other serious criminal investigations through the mutual legal assistance process, if required. But the new international production order removes the double handling within the US and other signatory nations, while allowing the information to be sought directly from the service provider by the Australian designated authority. This is a great improvement to our current process and will solve crime and save lives.

My most respectful submission is that the proposed bill is appropriate for the current and future needs of law enforcement and partner agencies, the security of this nation and the safety of the community, a role in which the New South Wales Police Force is a willing participant. Thank you very much to the committee for giving me this opportunity to speak.

CHAIR: Thank you very much.

Mr BYRNE: Assistant Commissioner, I'm just looking for a point of clarification in order for the committee to fully understand the impact of this legislation. I don't know if you heard the response to a question from Mr Leeser to the Australian Commission for Law Enforcement and Integrity—I think it was the Integrity Commissioner who responded—and there's also something that's been brought to my attention by Senator Abetz. It relates to the new power, as I see it, that doesn't exist at the moment that could be given to law enforcement agencies by the legislation—the international production orders. I'll just refer to the submission—and Senator Abetz drew my attention to this—from the Western Australia Police Force. In relation to the use of live intercepted data, it says:

The WA Police Force require more information and guidance as to what services are able to be intercepted from overseas carriers … If the restrictions imposed by encrypted services (such as, WhatsApp, Viber, Facebook Messenger) may be overcome to enable live interceptions, we expect that the IPO framework under the Bill will provide law enforcement officers with a highly valuable investigative tool.

I have a question, following this long preamble—and the secretariat has just drawn my attention to the explanatory memorandum for the bill, where it says 'intercept is defined to mean record or live stream to a single destination'. Is it your understanding that this bill gives law enforcement the powers to conduct live interceptions of communications in a place like the United States?

Mr Fitzgerald: Whilst I don't agree with everything in the Western Australian submission, because I don't believe this bill relates to fighting encryption—

Mr BYRNE: No, I agree.

Mr Fitzgerald: what I do believe is that, in the right circumstances, if it's a non-American citizen utilising a telephone in regard to crime occurring in Australia—for the importation of drugs or the like—then we could seek a live-stream interception of a telephone but under very strict requirements.

Mr BYRNE: And this is not intended to be a criticism. Please don't interpret my question is a criticism. This is something that the committee has just uncovered today in terms of the bill itself. This is not meant to be a criticism; this is us trying to understand the full reach of the bill. Please take the question in that way—so that we have a grasp of what this law might entail. That's the only basis on which I ask that question.

Mr Fitzgerald: I'm not trying to be defensive. What I'm saying is that, from a police force perspective, we are very, very excited by this bill and we do believe that it is capable of intercepting a phone under a very strict guideline of a person overseas, in the US or another signatory nation, who is using that phone for crime, whether it's terrorist activity or drug activity—as long as that person is not a US citizen—or using a messaging application or the like that we could intercept, if they were communicating with a person in Australia. We are excited by it.

Mr BYRNE: No, I understand. It's something that we weren't aware of. We were under the misapprehension that it was about stored data, so this has been very useful evidence for us to understand the additional powers this might give law enforcement. Again, thank you for that. Now that we as a committee are aware of this, we need to digest and process that. So I thank you very much for your evidence.

Mr LEESER: Commissioner Fitzgerald, I wanted to go through a couple of things in your submission. You said that the current TIA Act has led to the arrest of 1,218 persons from interception and 383 derived from stored communications. Is that right?

Mr Fitzgerald: That's correct.

Mr LEESER: That's just in the period 2018-19. Then you go on to raise some issues with the mutual legal assistance treaty, saying that requests can take months or even years before they're answered, and that has led to prosecutions being dropped. Without prejudicing any ongoing matters, would you be able to give us the flavour of some of those prosecutions that have been dropped, and people you've not been able to apprehend as result?

Mr Fitzgerald: With the MLAT, investigators generally use it for evidence gathering post arrest. We don't generally use it as an investigative tool, because it takes so long. But I can go through some examples, which is what we hope the IPO powers will rectify. I've got a number of examples in front of me. One of them is that between 2012 and 2015, when an accused was involved in threats to kill through multiple Facebook accounts created by the accused of the victim's deceased family members, the defendant had edited photographs of those family members. We commenced the MLAT process in 2014-15 to identify accounts created by the accused, and Facebook complied with that request in 2019. That's four years. I've got examples of aggravated sexual assaults of 14-year-old girls in 2018, where provider has told us it will take up to two years to get stored comms data. We have murder investigations where we've had offenders charged and we've had to wait up to a year to two years to get information from those providers. So we use the MLAT as a source to build up the brief of evidence. It's generally not used as an investigative tool, because of the time delay.

Mr LEESER: In your submission, you talk about prosecutions being dropped. Are the examples you've just given us examples where the prosecution of the relevant people have been dropped because of the delay?

Mr Fitzgerald: In that first example, as a result of a long delay in obtaining evidence, 16 of the serious stalking related offences had to be withdrawn. I can provide information at a later date to corroborate and confirm the information in my statement.

Mr LEESER: I think we'd be obliged to you if you could, because it helps the public understand why you and other agencies need the IPOs.

Mr Fitzgerald: Anecdotally, as I say, investigators drop a number of these MLATs due to the time delays.

Mr LEESER: This is the only other question I have. In your submission you talk about a range of matters that will 'benefit from the international access regime', and you list terrorism; drug importation; cybercrime, including child pornography; and homicide investigations. They are perhaps all reasonably straightforward. You also mention domestic violence. Can you explain how domestic violence investigations would benefit from international access?

Mr Fitzgerald: Unfortunately, many cowards who harass their partners use fake Facebook accounts to stalk and intimidate them. This process will allow us to not have to wait a year for the information. We'll actually, hopefully, be able to get that information quickly to identify the actual subscriber or person who has created these false accounts. That's just one example that I could use, and I could provide other examples later. But a lot of people use these services to try and remain anonymous while they stalk their ex-partners.

Mr LEESER: Thank you, Commissioner.

Mr DREYFUS: Commissioner, can you provide some detail on how you expect to use this legislation? Specifically, what do you think you're going to use it for?

Mr Fitzgerald: We've been considering how many applications we would be seeking with regard to this. To be honest, we think stored comms is one of the main areas we'll look at. Whether it's a terrorist or a person involved in child exploitation, they upload the majority of those photos to a cloud based solution. So we would be seeking to obtain photographs or data from those stored comms. That would be the main line of inquiry, which we see as being one of the great benefits of this legislation, going forward.

Mr DREYFUS: Assuming that the Australian government does manage to successfully negotiate an agreement with the United States and this IPO framework becomes available to you, are you able to estimate how many IPO requests you might make or that you're likely to make? And how would that compare with the number of warrant applications that you currently make in respect of domestic information? I'm just trying to get an idea of volume.

Mr Fitzgerald: I have been asking the same question of my people who work for me. We think there could be up to a thousand IPO applications by New South Wales police per year.

Mr DREYFUS: Right! So substantial use is what you have in mind?

Mr Fitzgerald: Yes.

Mr DREYFUS: That is heartening.

Mr Fitzgerald: That's right.

Mr DREYFUS: How many times a year does the New South Wales police make use of the existing mutual assistance framework to access—

Mr Fitzgerald: I have that data—just bear with me for one moment.

Mr DREYFUS: I know it's very slow; nevertheless, you do use it, even though it's slow?

Mr Fitzgerald: We do. I've been told by the section which manages it, which is the Police Prosecutions Command, that they process about eight applications per week.

Mr DREYFUS: What sorts of matters do they relate to, just to give a bit of concreteness to this?

Mr Fitzgerald: As I said, generally they're in regard to seeking information from telecommunication providers from overseas—once again, in regard to information that has been stored. Sometimes we put a request in to hold information. We would then seek to say, 'Can we see that data that has been sent from one person to another?' It's in relation to building up briefs of evidence—that's generally what we've used the MLAT for at this stage.

Mr DREYFUS: Yes. To go to another matter: the Inspector-General of Intelligence and Security has drawn the committee's attention to the fact that, unlike the current domestic data access regime for access to

telecommunications data, this IPO scheme does not include any specific protections for journalists. The committee is currently conducting an inquiry into press freedom, and I can't recall a single person telling this committee that the existing protections for journalists in Australian law should be watered down. Not even the current government has said that. But, incredibly, this bill appears to water down existing protections for journalists by making it easier to obtain an international production order for a journalist's telecommunications data if that data is held overseas. Does the New South Wales police support that aspect of the bill?

Mr Fitzgerald: What we do support is the current regime under the telecommunications interception act. It's a fairly strict regime and, if we ever did attempt to seek information in regard to a journalist, it would have to go before a public interest monitor. I would assume that it would be the same process that we'd find. I would certainly believe that if we ever did seek this information then it would come across my desk, and then I would seek fairly high-level legal advice and corporate advice in regard to proceeding.

Mr DREYFUS: So you support the current regime domestically, which is for a journalist's information warrant, and—certainly at a practical level—you would anticipate undertaking at least the same level of care in seeking an IPO?

Mr Fitzgerald: Yes.

Mr DREYFUS: Thanks very much.

CHAIR: Are there any further questions? No? Thank you very much for your time this morning, Assistant Commissioner.

Mr BYRNE: Thank you for your evidence.

CHAIR: Yes, we all appreciate it. We'll get your transcript to you in due course and you can make any corrections to that. Once again, thank you very much for your time.

Mr Fitzgerald: Thank you. With your permission, I heard a number of other witnesses indicate their concerns in regard to the scrutiny process. I would like to place on the record how strict our criteria are in regard to ensuring compliance and support of the Commonwealth legislation in regard to these new proposed bills.

CHAIR: Sure—we'll make sure that's noted on the *Hansard*. Also, if you would like to make any supplementary submission on that point, please do so, but please do so by Thursday of next week. That would be appreciated.

Mr Fitzgerald: Yes.

CHAIR: Thank you. I now declare this public hearing closed.

Committee adjourned at 12:14