COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015

THURSDAY, 29 JANUARY 2015

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

Thursday, 29 January 2015

Members in attendance: Senators Bushby, Fawcett and Mr Byrne, Mr Clare, Mr Dreyfus, Mr Nikolic, Mr Ruddock, Mr Tehan.

Terms of Reference for the Inquiry:
To inquire into and report on:
Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015.
WITNESSES

AYNSLEY, Ms Brenda, President, Australian Computer Society ................................................................. 83
BLIGHT, Mr Jake, Assistant Inspector-General of Intelligence and Security, Office of the Inspector-General of Intelligence and Security ................................................................. 37
BURGESS, Mr Michael Paul, Chief Information Security Officer, Telstra ......................................................... 7
BYRNEs, Ms Bronwyn, Lawyer, Australian Human Rights Commission ..................................................... 70
CAMPBELL, Ms Suzanne, Chief Executive Officer, Australian Information Industry Association ............. 30
CHALMERS, Mr Athol, Manager, Federal and State Government Relations, Australian Computer Society ..................................................................................................................... 83
CLARK, Ms Narelle, Deputy Chief Executive Officer, Australian Communications Consumer Action Network .................................................................................................................. 80
FALK, Ms Angelene, Assistant Commissioner, Regulation and Strategy Branch, Office of the Australian Information Commissioner ............................................................................................................... 46
FLYNN, Ms Julie, Chief Executive Officer, Free TV Australia ...................................................................................... 91
FONG, Mr George, President, Internet Society of Australia ..................................................................................... 85
GLENN, Mr Richard, Deputy Ombudsman, Office of the Commonwealth Ombudsman .......................... 42
GRIFFIN, Mr Michael, AM, Integrity Commissioner, Australian Commission for Law Enforcement Integrity ........................................................................................................................................ 34
HOLLANDS, Mr Mark, Chief Executive, The Newspaper Works ................................................................................. 91
HUGHES, Mrs Kate, Chief Risk Officer, Telstra ........................................................................................................... 7
KRUGER, Ms Sarah, Senior Lawyer, Special Broadcasting Service ................................................................. 91
LAWRENCE, Mr Jon, Executive Officer, Electronic Frontiers Australia .............................................................. 21
LOBB, Mr Matthew Randell, General Manager, Industry Strategy and Public Policy, Vodafone ........ 59
LUsty, Mr David, Special Counsel, Australian Securities and Investments Commission .......................... 1
MARSHALL, Ms Sarah, Executive Director, Operations, Australian Commission for Law Enforcement Integrity ........................................................................................................................................ 34
MckAY, Ms Penny, Principal Lawyer, Australian Commission for Law Enforcement Integrity ................. 34
NEAVE, Mr Colin, Commonwealth Ombudsman, Office of the Commonwealth Ombudsman............. 42
PATTON, Mr Laurie, Chief Executive Officer, Internet Society of Australia ..................................................... 85
PAVLIDIS, Ms Katerina, Grants and Research Officer, Australian Communications Consumer Action Network .................................................................................................................. 80
PIlGRIM, Mr Timothy, Australian Privacy Commissioner, Office of the Australian Information Commissioner ............................................................................................................................... 46
RAICHE, Ms Holly, Chair, Policy Committee, Internet Society of Australia ......................................................... 85
ROCHE, Ms Suzanne, General Manager, Policy and Advocacy, Australian Information Industry Association ........................................................................................................................................ 30
Savundra, Mr Chris, Senior Executive Leader, Markets Enforcement, Australian Securities and Investments Commission .................................................................................................................. 1
SCHUBERT, Ms Georgia-Kate, Head, Policy and Government Affairs, News Corp. Australia ..................... 91
SELLARS, Mr Nicholas, Executive Director, Secretariat, Australian Commission for Law Enforcement Integrity

SHAW, Mr James, Director Government Relations, Telstra

TANZER, Mr Greg, Commissioner, Australian Securities and Investments Commission

THOM, Dr Vivienne, Inspector-General of Intelligence and Security, Office of the Inspector-General of Intelligence and Security

TRIGGS, Professor Gillian, President, Australian Human Rights Commission

VAN BEELEN, Mrs Jane, Executive Director, Telstra

WELTON, Ms Erica, Director, Inspections and Law Enforcement, Office of the Commonwealth Ombudsman
LUSTY, Mr David, Special Counsel, Australian Securities and Investments Commission

SAVUNDRA, Mr Chris, Senior Executive Leader, Markets Enforcement, Australian Securities and Investments Commission

TANZER, Mr Greg, Commissioner, Australian Securities and Investments Commission

Committee met at 08:32

CHAIR (Mr Tehan): I declare open this public hearing of the Parliamentary Joint Committee on Intelligence and Security. This is the second of the committee's public hearings for its inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

These are public proceedings, and the committee prefers that all evidence be given in public, but witnesses have the right to request to be heard in private session. The committee may also determine that certain evidence should be heard in private session. If a witness objects to answering a question, they should state the ground for that objection, and the committee will consider the matter.

Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Tanzer: Thank you. I have a brief opening statement. We welcome the chance to testify before the committee and we appreciate the opportunity given your very busy agenda. In opening our evidence there are just four points that I would like to make.

Firstly, under the current law ASIC can access telecommunications data and, via warrant, stored communications in order to investigate white-collar crime. ASIC has responsibly exercised these powers for many years. This type of evidence is vital for ASIC's investigation of white-collar crime such as insider trading just as it is for the types of investigations conducted by the criminal law enforcement agencies which are given access to this information under the bill which we are examining. The bill on its face proposes to take away ASIC's powers when to our knowledge there is no suggestion that ASIC has misused or abused these powers or even does not need them.

Secondly, the white-collar crimes that ASIC pursues pose significant threats to Australia's economic security as a whole and in particular to Australians' financial wellbeing. Australia's growing superannuation pool, now standing at $1.87 trillion, has been targeted by criminal elements in the past, and the physical harm and the mental anguish that is suffered by victims of fraud and white-collar crime is vast and ongoing, as demonstrated by the collapse of the Trio superannuation funds. ASIC has important criminal law enforcement functions which it can only perform if it has the right tools, and we have great concerns that the bill in its current form could compromise ASIC's investigation powers and increase the threat to Australians of financial crime.

Thirdly, as outlined in our submission, ASIC is subject to significant safeguards and oversight to protect the privacy of any telecommunications data that it obtains.

Finally, if the bill is passed in its current form, it is possible that the minister may make a declaration which allows ASIC to access telecommunications data or apply for stored communications warrants under certain conditions. ASIC considers this a suboptimal outcome as it would create risks and uncertainty into the future. In light of the importance of access to this data to the investigation of white-collar crime and in light of the safeguards and oversight in place to protect the privacy of the information, ASIC submits that the committee consider recommending that ASIC is included in the definition of agencies entitled to access to the data within the bill.

We would be very happy to answer the committee's questions or expand on these points.

CHAIR: Thanks. David.

Senator FAWCETT: Thank you very much for appearing and for your evidence. You talk in your submission about the numbers of people you have secured criminal convictions against. There are some 129 people for indictable offences, including proscribed offences as described in the TIA Act, and through your own prosecutions there are criminal convictions against another 2½ thousand people—I think you said an average of 481 per year.

Mr Tanzer: Yes.

Senator FAWCETT: How many of those cases involve the use of metadata?
Mr Tanzer: The submission also goes to the number of occasions on which we have used metadata. In particular with regard to insider trading matters, we identify that we use metadata telecommunications data in 81.4 per cent of the cases that we prosecuted over the last couple of years. The specific number of investigations when we have used it is 1,771 occasions or the purposes of criminal investigations in 2013-14.

Senator FAWCETT: We have discussed previously the fact that the minister is able to declare organisations as being eligible to access metadata. Why does ASIC have a concern about that process, and what would you prefer to see the bill amended to for ASIC's benefit?

Mr Tanzer: I guess our submission is that we would prefer to see the bill amended so that ASIC is included within the list of criminal law enforcement agencies which are entitled to access the telecommunications data and apply for warrants for stored communications, as is the case under the current law. The law would be different in the sense that the law as proposed in the bill has a list of agencies rather than a broad-ranging definition. Consistent with that, we think that the approach would be to include ASIC within that list.

In terms of the ministerial declaration process our issues is not so much with that process as a whole. Our issue is that we need to deal with what is in front of us at present. As I mentioned, if the bill is passed in its current form, it is possible that ASIC could apply for a ministerial declaration, but the outcome of that at this stage is uncertain. That is perfectly proper; there is no reasonable basis for ASIC to suggest that the Attorney can give any sort of guarantee or assurance that we would get a declaration at this stage. That would not be proper. Therefore, we have to deal with the here and now. But, in terms of a ministerial declaration more generally, we are concerned that the form of the ministerial declaration might be subject to legal challenge. It might be subject to particular conditions that restrict the use of the agency's power to particular types of cases, which might also invite challenge to the use of that power on a particular occasion. Also, our concern is that, as a legislative instrument, it is likely that that type of declaration would be subject to a sunset; whereas the legislation is not subject to a sunset and would apply until the parliament decided to amend it.

Senator FAWCETT: What impact do you think that uncertainty would have on ASIC's ability to carry out its statutory roles?

Mr Tanzer: Our concern is that—and we have seen this in other cases—it would leave us open to legal challenge in the investigation of a particular matter, particularly by a well-resourced defendant, and we have seen this on other occasions, effectively to frustrate the investigation or prolong the investigation beyond a reasonable period of time. White-collar crime is notoriously difficult to investigate and bring quickly to trial. We have seen many cases—cold-calling cases, investment fraud cases, superannuation fraud cases—where the damage and the mental anguish inflicted on victims of those crimes is prolonged by the fact that the investigation or ultimate prosecution takes a considerable period of time. So we are concerned both about the potential for an investigation to be frustrated, perhaps because we make a mistake in terms of the scope of that power if it were limited by particular conditions, or just by delay occasioned by legal challenge to the exercise of the power in a particular case.

Senator FAWCETT: Underlying your submission, if I can try and frame it, is that you see yourself as a contemporary crime commission in that you are dealing with criminals—you have a statutory obligation to do that—and you feel as though this is an omission and you should be included in the list. Does that summarise your submission?

Mr Tanzer: That is largely a good summary of our submission. We feel that, as we look at the purpose of the bill, which is to cover those agencies that investigate and prosecute serious criminal offences, and as we look at the other agencies that are included within that bill and the nature of the crimes that they investigate, the crimes that we investigate have a very significant impact on Australia's economic security as a whole, the integrity of our financial markets as a whole, but particularly on Australians' financial wellbeing. Without a well-functioning regulator and enforcer to enforce those laws, particularly in circumstances where we rely so heavily on our superannuation for our retirement incomes for the future wellbeing of Australians, we feel that that is very important to safeguard.

Senator FAWCETT: Under your current system there have been no complaints about your handling of data and no concerns raised about the processes or oversight or review of ASIC's access, handling, storage and use of data from a privacy perspective?

Mr Tanzer: That is correct. As far as I am aware, as the submission points out, we have been subject also to the independent oversight of Commonwealth Ombudsman, who has conducted a yearly audit over I think the last five years now, and there has never been an issue that has been raised in that respect.
Mr BYRNE: Mr Tanzer, you said in evidence a moment ago that you were worried that the ministerial declaration would be subjected to legal challenge. Can you tell me who told you that?

Mr Tanzer: What I am relying on is my understanding of the law, and it is that, while the exercise of powers under the T(IA) Act is not subject to the Administrative Decisions (Judicial Review) Act, it is still subject to the Constitution. So, whether or not the power was exercised for a proper purpose or whatever could be potentially subject to challenge.

Mr BYRNE: But that would not be relevant to just your organisation. If that is an interpretation of your organisation, that the ministerial declaration could be subjected to not just your organisation but other organisations, does that not then create a potential flaw in the system that is being put forward, which is that you could have not just ASIC but other organisations that have applied to be considered by the minister, but they could also be ruled out at the same time. Is that a possibility?

Mr Tanzer: My submission is that this is so important. Obviously I am speaking from ASIC's perspective, so it is important for us. But, from the committee's perspective, I am trying to demonstrate that the role that we have with respect to white-collar crime is such that this should be put beyond any doubt and it should be the primacy of the parliament that sits behind the grant of ASIC's power rather than a ministerial declaration.

Mr BYRNE: What you are also saying, though, is that you have a belief, based on an interpretation of what you have seen, and the law, the EM et cetera, that organisations like yourselves might be subjected to some form of challenge if they are declared by the minister, and that is creating the concern that your organisation has. Is that not right?

Mr Tanzer: That is part of the concern. The other two parts of the concern are that any ministerial declaration would be likely to be subject to a sunset clause and would therefore be limited by time, but also the declaration-making power on its face countenances that there may be particular conditions that are put in place to restrict the scope or otherwise. I think that by its nature would also give rise to the potential for legal challenge.

Mr BYRNE: Sure. Could you take me through the consultation process briefly, Mr Tanzer? Were you consulted by the AGD? Could you explain, in terms of the lead-up to this piece of legislation, what consultation process occurred between ASIC and the AGD or the relevant parties that put this legislation before us?

Mr Tanzer: An amount of that, I think, will go into details around cabinet consideration close to the bill. We certainly were not involved in any consultation at the stage close to the presentation of the bill. We were involved in earlier consultations, including hearings of this committee, around these types of issues, but there was no specific consultation around the detail of the bill at the time that it was being prepared in this form.

Mr BYRNE: When did you find out that you were not on the list?

Mr Tanzer: On 30 October.

Mr BYRNE: When they published it?

Mr Tanzer: Yes.

Mr BYRNE: So you were not told that you would not be on the list until they published it, even though you have had that power?

Mr Tanzer: No.

Mr BYRNE: That is a pretty interesting consultation process.

Senator BUSHBY: As I understand it, the main thrust of your submission is that you want to have continued access to data that you currently use and have been using, historically, for your prosecutions. To me, that has two aspects. One is what we have just been discussing—that you are authorised to access the data—but the other side of it is something which you have also touched on in your submission, and that is data retention, which is the main purpose of the bill.

Mr Tanzer: Yes.

Senator BUSHBY: I note that on page 2 you say:

This reform does not involve conferring new powers on law enforcement agencies, but rather seeking to ensure that crucial existing powers retain their utility and are not eroded because of profit-driven changes in commercial practices.

Has ASIC, as an organisation, experienced a lessening of the data that is available for you when you are using the powers that you currently have? When you are accessing data, are you finding that, increasingly, these commercial practices are leading to an increased difficulty in finding data?

Mr Tanzer: Yes, we have seen this. If the committee would like, it would be possible for us to get some more information. We would prefer to give it on a confidential basis, about particular cases. It tends to be less the case...
with traditional telecommunications providers, where we have longstanding arrangements and we have a good understanding of the periods of time within which they retain data, and more the case with the more recent internet service providers or those that are dealing with the internet as opposed to more traditional forms of telecommunications.

**Senator BUSHBY:** Certainly, if you could make that available to the committee, that would be useful. In terms of profit-driven changes in commercial practices—that is a term you use—what do you mean by that?

**Mr Tanzer:** What we are really referring to there is that the commercial environment is very fast-moving and there is a range of different disruptors who disrupt traditional players. That has always been the case. Sometimes they take advantage of cost structures that take advantage of existing infrastructure or sometimes they take advantage of new forms of infrastructure which they develop, which is entirely legitimate. But the point here is that if for a commercial purpose it is not necessary to retain that data in the same way, then there is a real commercial imperative to remove that data, because it is removing unnecessary cost from that entity.

**Senator BUSHBY:** Which makes commercial sense from their perspective—

**Mr Tanzer:** Absolutely.

**Senator BUSHBY:** But has a consequence in terms of the ability of organisations such as yourself to investigate and prosecute serious crime.

**Mr Tanzer:** Absolutely.

**Senator BUSHBY:** Just as a final question, how far back do you generally go? You mentioned cold cases earlier. Over what period do the authorisations that you seek to access this data generally extend? And, at the extreme, how far back have you gone?

**Mr Tanzer:** Maybe Chris will be able to help me with any particular example. In the general case, we seek to move as quickly as we possibly can. But there are definitely cases that come to us, particularly in this area of cold calling and particularly in cases of superannuation fraud, quite some time after the event, and that is because the victims themselves may not appreciate that they have been victims of fraud until some time later. Quite frequently the perpetrators of these crimes dummy up statements and dummy up websites to give the impression that all is well with your investment. And quite frequently that comes to us two, three or four years after the event. We quite understand that in the circumstances of this bill there is a balance to be struck, and we certainly have no issue with the two-year balance that is struck in the bill.

**Senator BUSHBY:** So, theoretically you would like to go back further at times, but you acknowledge the reality that the balance does need to be struck—

**Mr Tanzer:** The reality also is that, as a criminal law enforcement agency, the further back one has to go the more likely it is that the recollections and the cogency of evidence that people might have of the events that took place will become more problematic.

**Senator BUSHBY:** But, similarly, if the data exists and you can access it, it is hard data, and that can actually corroborate recollections that might be a bit fuzzy.

**Mr Tanzer:** Exactly, and we have given examples in the submission where that is absolutely critical, from our perspective, because it corroborates events that we have been told by witnesses. It may establish the location of an offender. There is one case that we talk about here where an offender was moving around between different states and it was important for us to be able to establish which state he was in at the time he made the particular communication in order to charge the right offence.

**Senator BUSHBY:** For jurisdictional purposes?

**Mr Tanzer:** Yes.

**Senator BUSHBY:** Thank you very much.

**Mr RUDDOCK:** I thank David for the questions he asked, because they were really the substantial questions I intended to ask. But perhaps I could just ask you about privacy generally. We are being told that privacy is in fact so important that I imagine there are some people who would say that insider traders have a right to privacy and should be free from investigation.

**Mr Tanzer:** Yes. I do not agree. And there is—

**Mr RUDDOCK:** It is not like terrorism, after all.

**Mr Tanzer:** It is not like terrorism, and I do not make a case that it is exactly the same as terrorism. That would be churlish and, frankly, stupid. But insider trading is an especially pernicious activity. If insider trading is permitted to continue, retail investors and institutional investors will lose confidence in the Australian market.
Australia is a net importer of capital—a very major net importer of capital—and if foreign investors in particular, let alone Australian investors, lose confidence in our market, we lose this whole engine and multiplier effect that we have through our capital markets for efficient capital raising. And it all sounds a little bit remote from the issues of ordinary Australians, except if you remember two things. One is that the market drives fundraising by ordinary companies, particularly large companies, and those companies employ a very large number of Australians. The second is that we are all dependent for our future financial wellbeing, particularly in retirement, on our superannuation savings, and a very large proportion of those savings are, rightly, invested in the Australian market, because Australians can have confidence. We have seen, on many occasions, people lose their superannuation savings. I am not equating this to a terrorist act, but I am equating this somewhat to other crimes which cause physical harm to people. It is very difficult for a person who has lost their life savings to recover, particularly if you are at that part of your life, as I am, where you do not have a lot of time to recover a deadweight loss.

Firstly, it completely knocks your confidence about. It causes unreasonable financial stress. In particular, we have seen cases where the harm causes victims to take drastic actions and that is a terrible thing to see. So the impact on ordinary Australians, particularly superannuants, when they lose out of this, is very, very profound.

Mr RUDDOCK: I think you have almost got me!

Mr Tanzer: Almost!

Mr Byrne: It is an easy catch; don't worry.

Mr Dreyfus: Thank you very much for coming. As I understand it, the position is that ASIC and its statutory predecessors have had access to telecommunications data, certainly since the Telecommunications (Interception and Access) Act 1979 was enacted.

Mr Tanzer: Yes.

Mr Dreyfus: I was taken aback to hear that the first you heard that ASIC was no longer to have access to telecommunications data was when you read the bill on its introduction to parliament, on 30 October.

Mr Tanzer: That is the case.

Mr Dreyfus: So there was no consultation by the government of your agency before this bill was introduced to parliament?

Mr Tanzer: Not before the detail of the bill was introduced. We were engaged in earlier processes leading up to the—

Mr Dreyfus: Sure, such as the inquiry by this committee in 2012-13, which led to its report in May 2013.

Mr Tanzer: That is right.

Mr Dreyfus: We do not have a lot of time, so I will have to cut this short. If I can summarise, your position is that ASIC should not only be one of the agencies with continuing access to telecommunications data but be listed in the legislation—in other words, the agencies should be listed in the legislation itself.

Mr Tanzer: We are quite happy to leave that to the parliamentary drafters, who are people much more expert in this, because I can quite understand that, as agencies might change their name or something of that nature, there might be reasons why it might be done in a slightly different way. Our point is that we believe that we should be put on the same footing, that our power should be included in the bill itself or in the act going forward, as it currently is. But we quite accept that the express intention of this committee and the express intention of the government is that the definition in the existing telecommunications interception act is too broad. We have no issue with that, but we believe that our case that we should be included within the bill itself is quite compelling.

Mr Dreyfus: So you are saying that, by all means, restrict the agencies as long as we are not excluded?

Mr Tanzer: I am not expert on what other agencies do. I really cannot speak—

Mr Dreyfus: I get that; you are speaking for your own agency?

Mr Tanzer: I have to.

Mr Dreyfus: Again, we really do not have time—

Chair: Mark, you have another five minutes, so feel free to ask the questions you want to ask.

Mr Dreyfus: I read through your submission and it is helpful to have the examples that you have given of enforcement action by ASIC that has relied, at least in part, on telecommunications data. Are you able to briefly describe the primary forms of data that you use? Reading the examples that you have given, it seems to have been
primarily call data, but I do not want to misstate that. So I am inviting you to explain to the committee in a
summary form what are the main forms of telecommunications data that ASIC would access?

**Mr Tanzer:** In essence, you are correct. The greater preponderance is that we get involved. At the early stage
when we are looking for telecommunications data, we are primarily looking for call data and that is primarily to
identify associations between particular people, particularly for the purposes of insider trading and market
manipulation but also investment fraud and those types of things.

It may also be the case—and we have given some examples here—that it is also email communication that we
are looking for and at, and particularly in the cases of investment fraud which involve the setting up of bogus
websites, which is often the case with these cold-calling investment frauds. That may well involve
communications with the internet service provider to find out what information we can get about the owner of the
website.

**Mr DREYFUS:** Has ASIC experienced difficulties in recent years with the use of various technologies like
Tor, VPN or encryption that are making telecommunications data more difficult to use or more difficult to use as
an investigation technique?

**Mr Savundra:** I think the answer is yes. It is getting more difficult, particularly with the use of online chat,
which does not go through call charge records—so messages through WhatsApp, Snapchat and measures like
that. In relation to the use of Tor, whilst we do not have direct evidence that Tor is being used, in trying to locate
the ISP it does not seem to marry, which suggests that methods such as Tor are being used.

**Mr DREYFUS:** Does ASIC have any strategies in mind for that future that we are looking at, which is one in
which there might be increasing use of methods that make the data that we are presently keeping less useful?

**Mr Tanzer:** It is probably a very big topic and perhaps it is one that I would not like to explore too much in a
public forum.

**Mr DREYFUS:** Does ASIC have any comment in relation to what should be in the dataset that
telecommunications companies are required to keep?

**Mr Tanzer:** At this stage we are content with the range of matters which are set out within the bill as would
give rise to the dataset, which is still coming through the Attorney-General's Department. We are satisfied that
that would cover the range of factors that we would need to see at this stage.

**Mr DREYFUS:** Have you been consulted about what the dataset should contain?

**Mr Lusty:** No, we were not.

**Mr RUDDOCK:** Have you got any view on the question of exempting wi-fi services in cafes?

**Mr Tanzer:** No, I do not.

**Mr RUDDOCK:** You do not think insider traders might think that wi-fi cafes may be an appropriate place to
do their work?

**Mr Tanzer:** There are a range of things that insider traders do. That is always possible. That is a much
broader issue. I think it is not so specific to insider traders or others. It is a particular issue for ASIC.

**CHAIR:** Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your
evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please
forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will
write to you. We look forward to the follow-up to Senator Bushby's request for additional material. Thank you.

**Mr Tanzer:** Thank you.

**Proceedings suspended from 09:04 to 09:15**
BURGESS, Mr Michael Paul, Chief Information Security Officer, Telstra
HUGHES, Mrs Kate, Chief Risk Officer, Telstra
SHAW, Mr James, Director Government Relations, Telstra
VAN BEELEN, Mrs Jane, Executive Director, Telstra

Evidence from Mrs van Beelen was taken via teleconference—

CHAIR: I now welcome representatives of Telstra. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Shaw: Yes, please. Thank you for the opportunity to appear before the committee today. As you are probably aware, Telstra is Australia's leading telecommunications company. We currently provide more than 32 million voice, internet and email services in Australia across our mobile and fixed networks and our BigPond email platform. We also have a long and credible record of working with law enforcement agencies in this area. Telstra has had a longstanding approach to the issues before this committee. The approach seeks to strike an appropriate balance between helping protect public safety, meeting our customers' expectations around privacy and minimising the regulatory burden imposed on industry.

Protecting its citizens is one of the state's most fundamental roles. The use of telecommunications data is critical to modern policing and national security. It helps save the lives of Australians and solve serious crimes. Telstra is cognisant of the importance of providing assistance to protecting public safety and the challenges posed for the agencies by changes in technology, and we stand ready to support this important area of work where we can. One of the obligations that come with being a telecommunications carrier and internet service provider in Australia is the requirement to provide lawful assistance to the agencies.

At the same time, we understand the importance that we all place on the privacy and security of our personal information and data. Privacy is and will remain the key customer concern and hence a concern for Telstra. For this reason, we will continue to invest in the necessary systems to protect customer data and to meet our obligations to only provide access to data for the reasons specified by law. In terms of minimising the impact of the scheme on industry and our customers, we welcome the limits that the government has established for the scheme, such as focusing on metadata rather than the content of communications and limiting the agencies that can access the data. We believe these limits will help give the community a greater degree of comfort about the access to telecommunications data by the agencies.

The legislation will impose a new regulatory burden on our business, creating both capital costs and operational costs. The impact on our business comes not just from new data we must collect but from the requirement to extract, index, store and retrieve upon request from the dataset, as well as security measures needed to protect the data. Given this impact on our business, we welcome the government's statement that it will contribute to industry costs and the fact that the government has been actively consulting with industry on what is practical and operationally feasible. We look forward to this engagement continuing to ensure that we achieve long-term certainty on the detail of the scheme, including the dataset, and a level playing field for all industry participants. We look forward to discussing these and other points with the committee.

Mr Byrne: Just in terms of the costing, how much will it cost?

Mr Shaw: Our submission indicates that it is a significant cost. The actual figure itself has been provided to PricewaterhouseCoopers, and we would regard that as a commercial-in-confidence figure that we would not like to put out in the public domain.

Mr Byrne: In terms of your submission, are you comfortable that the dataset that has been provided to you, if it were enacted in legislation properly, provides you with enough certainty in terms of what you would then need to do to ensure that you could keep that data?

Mr Shaw: We could build a data retention scheme based on the information that we have around the dataset at the moment.

Mr Byrne: At present, as we are talking about the security of the information—and you might need to take this on notice—how many times have you been hacked in the past 12 months?

Mr Shaw: Hacked is a fairly—
Mr BYRNE: Or someone has tried to penetrate your operations.

Mr Shaw: That is an ongoing battle for our network people. Mr Burgess and his team confront that situation on a daily basis, and he could elaborate, but that is an issue that any telecommunications provider of any size faces on a daily basis.

Mr BYRNE: But you also have said in previous evidence, as others have, that you are creating an advertised honey pot of information, which then provides an incentive for people to try and access that information. Is that an area of concern that you have? What additional measures would you need to take to ensure that, should you create that body of information, that body of information would be secure?

Mr Shaw: We would need to take further steps in the security layers that we provide in the network. Mr Burgess could provide a little more detail around that, but you are quite right to say that the existence of a large dataset with a lot of personal and other information contained within it could be an attraction for people for a variety of reasons.

Mr Burgess: Recognising that the data is of interest to law enforcement and security agencies, it would also be of interest to other people. The internet is a very busy place for those who choose to do harm—malicious activity. The key factor here, though, is that we would be providing a system that actually allows Telstra to collect, process and make available that data to the agencies upon lawful request, and hackers would take advantage of that. If I was after that information, I would go to the system that could provide that easily. They are just like everyone else: they will go for the least effort to extract that data. Because of that, we would have to put extra measures in place around that point of aggregation to make sure that that data was safe from those who should not have access to it.

Mr BYRNE: At present, what information do you store and for how long do you store it?

Mr Shaw: It breaks down into four categories, really. We have the data that is collected already for two years or more, and an example of that is the billing information that we have to collect under the Telecommunications Consumer Protections Code, which includes names, addresses, telephone numbers and data usage. We keep that for six years, which is a code requirement. Then we have data that is currently collected but for which the records may not be complete, and an example of that is the IMEI number that identifies an individual handset. We have that for handsets that we have sold but not for handsets that people might bring into our network—the bring-your-own-device type situation.

We have data that is collected but for less than two years, and it is not necessarily held against customer accounts, so it is generated by the network. That might be some of the IP information—the addresses on the fixed ADSL network. That is kept for varying periods of time. Then we have some data that is in the proposed dataset at the moment that currently either we do not access or we do not have at all, and some examples of that are missed calls, originating IP addresses for our mobile network, time stamps on Big Pond emails and information about missed calls.

Mr BYRNE: So you have provided information to PricewaterhouseCoopers—and I presume that at some stage we will get the information. Gosh, I hope we will; we are supposed to be making recommendations on it. We will get the costs so we can look at that, but you are saying that this will be a mechanism or system that you will have to set up that will have some significant cost to your organisation—is that correct?

Mr Shaw: It is. We are going to have to build a centralised platform that will extract, store, retrieve and process this data.

Mr BYRNE: How does that happen now, then? Say, for example, you have enforcement agencies that want to access that data and are doing that. Is this going to be a different system to what is currently in place? The argument put forward at the moment is that this is a continuation of the existing system, but you are saying that, actually, no, you will have to create a separate system in order to keep the data that the government would require.

Mr Shaw: That is correct. In the current circumstances, if a lawful request is made and the information is available and accessible, we make it available to the agency. Under the proposed scheme, there is a requirement to collect and retain this information, so it is that process of collecting, retaining, indexing and storing for that period of time, which is the differential between just the standard—

Mr BYRNE: So there is some information that you currently are not collecting that you would start to collect under the new regime. Is that correct?

Mr Shaw: That is correct.
Mr NIKOLIC: I have a follow-up question. On page 2 of your submission you talk about 85,000 direct requests for metadata each year, of which some 2,700 will warrant requests for access to content.

Mr Shaw: Correct.

Mr NIKOLIC: So if I understand it there is an existing process, mechanism or infrastructure within which you satisfy those requests. Could you expand a little bit more on that. Do I take from Mr Burgess's comments that the current infrastructure is sub-optimal and that, as a result of this legislation, you have to do more to make the information secure? Is it not secure now?

Mr Shaw: The information is secure at the moment on our network, and the infrastructure is there, and configured, to support our current regulatory obligations, which are to make information available if it is reasonably accessible. We do that on a daily basis, as you can see with the large number of requests that we already satisfy. With the requirement to keep and retain this data and have it ready and available should an agency seek to examine it, comes a new set of obligations and a requirement to build new systems to support that obligation.

Mrs Hughes: Perhaps I can interrupt. At the moment agencies might ask us for information, but we do not have it and so we therefore cannot give it to them. That is why they would like us to retain it. It is so that in the future if they did ask for it we would have it and we would have to give it to them.

Mr NIKOLIC: But in terms of the comments, as I heard them—and I might have misheard them—about additional security and additional threats, that additional threat does not arise from this legislation. They are existing, adaptive threats that are already providing challenges to you and other telecommunications providers.

Mr Shaw: There is a whole variety of different threats that exist and will continue to exist. With the creation of a new centralised platform to bring this information together, we consider there is a potential new vector for attack, which we need to secure for.

Mr Burgess: I am happy to explain that. You are absolutely right: we do secure the data we have today. So we do have that problem today. The issue here is that now we are advertising that for a customer of Telstra there is a whole range of data, depending on what services they have, that for two years we can make available upon lawful request. If I were that way inclined as a hacker, you would go for that system, because it would give you the pot of gold as opposed to working your way through our multitude of systems today to try to extract some data. But your fundamental point is that, yes, we face this risk today—absolutely.

Mr DREYFUS: This is quite a significant point. As I understand what Telstra is saying here, at the moment you faithfully answer approximately 85,000 direct requests from law-enforcement agencies—that was in the last financial year—and it has been a rising number over the last several years. Is that right?

Mr Shaw: There has been a gradual increase over time. Rising gradual

Mr DREYFUS: Not deeply increasing, but certainly an increase in number over the last few years. But the request comes to Telstra and the agencies take you as they find you?

Mr Shaw: That is correct.

Mr DREYFUS: In other words they are saying, 'Give us what you have got', and sometimes you will not have what they are asking for?

Mr Shaw: That is correct.

Mr DREYFUS: And in the answers to question you have acknowledged that there is of course a risk. Any telecommunications company faces the risk now of hacking, of data breaches and a whole range of threats that are out there. But you are putting—I am trying to re-state this, Mr Shaw—that there is an additional threat or risk that is being created by this legislation, because it will require the creation, in a standardised form, of a database that keeps a range of data that presently Telstra does not keep at all, which therefore creates an attractive target?

Mr Shaw: Yes, it is an enhanced target.

Mr DREYFUS: Which is a risk of a like nature to the risk that Telstra presently faces, but not in itself a risk that Telstra presently faces, because that database called into existence by this proposed legislation does not presently exist?

Mr Shaw: Correct.

Mr DREYFUS: Could I confirm that the proposal Telstra is faced with by this legislation would in fact require Telstra to keep a range of data that Telstra does not now keep?

Mr Shaw: That is correct.
Mr DREYFUS: And it will also require Telstra, and every other telecommunications provider, to keep the data in a standardised form?

Mr Shaw: The way in which the data is retained—'business as usual' is the response we get when we talk to government about how it is to be retained and made available. The legislation does not go to that standard about its presentation or the like; it goes to what needs to be retained in the period.

Mrs van Beelen: Perhaps I could clarify. Mr Shaw is correct that the legislation is not prescribing a standard, but what the bill would require us to do is to have that data in a location or a system where it can be accessed and where, for some of that data, for the first time, it would be associated with a particular customer as opposed to just data that is transient in the network. So really 'centralisation' is the appropriate word rather than 'standardisation', that we say is the issue here.

Mr Byrne: We went down to your global operations centre some time ago. This is the first iteration of it. Currently my understanding is that you have a lot of information that goes through your system that is bundled. Is the government proposing through this dataset that you will have to unbundle the information that comes through and then keep separate elements of it as well, or not?

Mr Shaw: Sorry, Mr Byrne, I am a little bit lost by your use of the word 'bundled'. We have got information flying across our network in various forms, and this legislation would require us to keep a prescribed dataset in a form that can be made available to the agencies. I am not quite sure how this fits with the concept of bundling. There are various pieces of network information that are generated by their various network elements that either go into a system and be retained or just fall off or the like. So there will be an obligation to collect that and retain it for that period, but I am not sure how we relate—

Mr Byrne: I might have a separate conversation with you to provide some further clarity subsequent to that.

Mr Shaw: Absolutely. I am happy to do that.

Mr Byrne: Do you currently store content?

Mr Shaw: Some content, yes.

Mr Ruddock: My questions were in precisely the same area. In relation to this new data that you are going to collect, I have not been persuaded why a hacker would see that as being more valuable than the information that you have generally on your system. Can you persuade me why collecting the information would be more attractive to hackers than just getting general access to your database?

Mr Burgess: Certainly. So it is not whether it is more attractive; it is the point of access. It is the systematic approach: give me a customer identifier and tell me where their mobile phone has been for the last two years. If they compromise this new system or the proposed system to meet this requirement, they have got that. Today they would have to get in, and across our mobile network we have some 13 core systems, and it would be very complicated for a hacker to actually move across our network and put the pieces together to track someone's phone in terms of where it has been, because we simply have that rolling through our system. We do not store that for any other purposes of where we need it immediately to make the call. So, because of that new functionality we are putting into the network, that is why it is of concern to me. And I know that because if I were in a foreign intelligence service wanting to hack Telstra's network, this new proposed system would be where I would go. You would tell the computer; you compromise the account of the user that has access to the system to provide the answer to law enforcement and you type in the subscriber information and, presto, there is your answer. The alternative is you probably have to be on the network for months, if not years, studying how it is set up, because that is not available to people from outside Telstra, and figuring out how to do that to then answer the question, should that be your question. As you know, there would be some hackers out there who would like to know who has been calling who and where a phone has been in a certain period of time.

Mr Ruddock: It might make it easier for counterintelligence to be able to identify foreign agencies when they are trying to get into your system.

Mr Burgess: That is exactly my point.

Mr Ruddock: It might be a good tool to being able to pursue counterterrorists.

Mr Burgess: I am sure government understand and the agencies understand the power of this capability.

Mr Ruddock: Anyway, it is as narrow as that. I hear that. The draft datasets on page 2 that you are speaking of are going to include internet browsing sessions from mobile services and call attempt records. To what extent do you get requests for that sort of information now?
Mrs Hughes: The agencies know we do not keep that now. So, as a consequence, they have learned not to ask for it. When they have asked for it in the past, on occasion we will have had it, but it is not certain information. That information gets overwritten. We do not store it.

Mr RUDDOCK: So you have no idea—

Mrs Hughes: No. They might want to ask for it, but we do not keep it and so they will not.

Mr RUDDOCK: Maybe I need to ask them. To what extent have you estimated that you are experiencing loss of business to competitors because others do not keep the same information as you?

Mr Shaw: We have not done that calculation.

Mr RUDDOCK: So you have no idea?

Mr Shaw: No.

Mr CLARE: Mr Shaw, can I ask Telstra's view on the proposed dataset?

Mr Shaw: We have sufficient clarity around the dataset to be able to implement a data retention scheme.

Mr CLARE: I understand from your submission that Telstra's preference in the interests of certainty of cost is for that dataset to be embedded in legislation rather than regulation. Is that right?

Mr Shaw: The question of how to prescribe it is one that we think is for government. Our concern is about that long-term certainty around the dataset, the form of the dataset and how it might be changed. If that outcome is achieved, that is our priority.

Mr CLARE: But, if I am correct, Telstra's concern is that the changes would or could occur to the dataset and that, if that were to occur, that would have the potential to impose significant new costs on industry. So presumably if it is embedded in legislation that would provide more certainty than if it is imposed in regulation.

Mr Shaw: I think it is true to say that the standard regulation-making process in which regulation is made and then comes into effect immediately, subject to a short disallowance period, does not provide the longer term certainty you might have, but there might be ways that you could make the regulation work so long as you have a sufficient implementation period and there is oversight of the regulation and discussion around it. That is there or there is the black letter law. I think our submission is silent on that precise point on whether it is to be in the act or in the regulation. Our overriding concern is around certainty and sufficient implementation time around any changes.

Mr CLARE: On that point, would you agree that industry would have greater certainty if the dataset was in legislation rather than regulation?

Mr Shaw: Generally that is the case with most legislative instruments, yes.

Mr CLARE: Can I ask for Telstra's advice on something. What can you tell the committee about the age of the data that is currently sought from you by law enforcement agencies?

Mr Shaw: Very little, unfortunately. We do not keep those sort of records. There is no requirement for us under the current arrangements to do so. It is not something built into our business system. We just process the request and, if we can reasonably access data, we provide it. We do not track the age of the requests or the data that is being requested.

Mr CLARE: If the committee were to ask Telstra to have a look at the age of the data that had been sought by agencies, perhaps over a short period of time—late last year, for example—would Telstra be able to do that work and advise the committee?

Mrs Hughes: Not without a significant burden. It would require us to pull every authorisation down. Information might not be contained on the face of it and so would require further research. It would be very time consuming, even for a short period of time. There are 85,000 requests annually, so even for a one- to two-month period—

Mr CLARE: Would it surprise you that other telcos are able to provide that information to this committee but Australia's largest telco is not?

Mr Shaw: No, it would not. We are a business that has been around for quite a while in various iterations with a lot of legacy systems that go back to the time of Federation and the Postmaster General's Department. There are new entrants into the industry that have single platforms. They are niche providers. They are set up in a different way. It is quite possible they can provide that data. Given the multitude of systems we have, with the different networks and platforms—there are hundreds of thousands of network elements—it is something that we just do not turn an eye to because there has never been a need to.
Mr CLARE: But given the seriousness of the legislation that is before the parliament and the importance of understanding the age of data that is generally sought by law enforcement agencies, would Telstra be willing to have a look at the age of the data sought by law enforcement agencies, even if it is over a very short period of time, to assist the committee in its deliberations?

Mr Shaw: Perhaps we could take that one away and have a look at it and talk internally to our people and see what we might be able to do.

Mr CLARE: Sure.

Mr Shaw: If we can assist the committee, we most certainly will. I am not really in a position to give an open-ended commitment at the moment without understanding fully what might be involved and talking to some of my colleagues and their people at the coalface.

Mr CLARE: Through you, Chair: I would personally welcome that. I think this is very important for the work we are doing. So, thank you.

Mr Shaw: We will make our best endeavours.

Mr CLARE: Perhaps I could turn to another area, and that is costs. A number of submissions have pointed to the impact of this scheme on small ISPs as opposed to large ISPs, and how you deal with that. The committee at present does not have the PWC report, which may or may not look at this—I do not know. Does Telstra have a view about how to deal with that matter?

Mr Shaw: On the issue of the costs of the scheme and how it might fall across the industry, we think it is a little bit simplistic to suggest that just because you are a small ISP it will fall disproportionately on you. We think the complexity of systems, numbers of systems and the like mean that on a per-subscriber basis you could find that it will vary according to factors other than just the size of the ISP or carrier. If you are providing only a simple broadband service but you have a large number of customers, as opposed to a carrier that has multiple systems—mobile platforms, fixed platforms, IP platforms, the old PSTN—then you have a multitude of products across them. That complexity adds significantly to the cost of extracting and indexing and collecting that information. So, we would not agree with the proposition that says that the cost of implementation is directly linked to the size. We think complexity is a very important factor.

Mr CLARE: Can you explain to the committee what consultation occurred between the government and Telstra prior to the announcement of this legislation?

Mr Shaw: This is an issue that has been around for years, as you would recognise. This is not my first appearance before this committee on this particular issue. The notion of a data retention scheme has been kicked around for at least a decade. I think some of our people internally can recall discussions with a number of governments before on this particular issue. We know that the agencies have always had an interest. So, it has come up from time to time. And we have been aware that since the last PJCIS report there was a series of recommendations and it has been looked at again within government. We talk to the government across a range of issues in the national security area on an ongoing basis. And even if there have not been formal proposals before government, agencies and others have talked to us about what might be possible, for instance. So, it is an ongoing discussion.

With the legislation being brought into existence, there has been the industry working group, of which we have been invited to be a member and in which we have participated. We have found it quite useful. In fact, it has suggested some amendments to the dataset. But really it is an issue that gets raised in other business if it is not a formal agenda item, and we have some interactions with government.

Mr CLARE: Did anyone from Telstra meet with the Prime Minister in the days before the announcement of this legislation?

Mr Shaw: I believe that there was a meeting. I believe it was before the legislation was introduced.

Mr CLARE: Who attended that meeting?

Mr Shaw: Our chief executive officer and Ms van Beelen.

Mr CLARE: Can you provide us with any details of that meeting?

Mr Shaw: I would prefer not to divulge the nature of the discussions between the Prime Minister and our chief executive officer.

CHAIR: Andrew had one follow-up question from one of the questions Jason asked.

Mr NIKOLIC: On the questioning regarding having metadata enshrined in legislation versus regulation: if I understand what you have said, the explosion in multi-user technology and the different ways that people have
used telecommunications over the years have been mirrored in changing requests from agencies to you about what they may require. I imagine that as more people have used different platforms, the nature of those security requests to you have adapted. Is that a fair comment?

Mr Shaw: Yes.

Mr NIKOLIC: I just wonder if I could better understand the concern around this being in legislation versus regulation. Legislation is obviously much harder to change and is a much longer process. If we truly believe in adapting to what counter-terrorists, adversaries, paedophile networks et cetera might be doing to get away from this stuff, could you articulate more clearly for me the concern about having something enshrined in legislation versus regulation, given that this is a constantly adapting situation and security agencies are constantly adapting to it?

Mr Shaw: We recognise that concern of the agencies and it is reflected in our opening remarks—the changing nature of technology—which is why our submission focuses on long-term certainty and the need to have time to implement new arrangements. We do not go to the point in our submission of regulation versus legislation. We focus on that issue of certainty for industry, around what our obligations are.

Mr NIKOLIC: Thank you.

CHAIR: Following up on that, if there were to be further change, you would want a long lead-in time, similar to what the government is giving you now, which is about 18 months. This is a serious question. That is the issue. You just want to make sure that you would have time to adapt and have a proper length of period to do it rather than your concern around legislation versus regulation?

Mr Shaw: That is one element.

Mrs van Beelen: Could I add to that, Mr Shaw? I agree that the lead time is important. The other thing, of course, is consultation, so that there is an understanding of what is possible, what is able to be done and what it would take to do it. Consultation, including on what it would cost, would be an important consideration before any additions or changes were made to the dataset, and then of course there is the time to implement.

CHAIR: Thanks.

Senator FAWCETT: In the first part of your submission, you give an overview statement saying you are seeking to contribute to striking an appropriate balance and you go on to list a number of bullet points. The last one says:

- Puts appropriate oversight mechanisms in place.

Do you have any specific concerns with either existing oversight mechanisms or what is proposed in the bill?

Mr Shaw: We do not have concerns with what is proposed, but, like any piece of legislation, having it ventilated in the way this bill is at the moment, there could be other proposals brought forward around oversight to allay some of the concerns that we know people have put forward. We do not have any specific proposals. We are just mindful that, if something is of the nature of a data retention scheme, oversight is important. We know that the ombudsman is getting increased powers under this bill, and that is a reasonable step to take. There might be other mechanisms that come through the committee process that would be reasonable to put in place as well. Those dot points are really a set of principles that we think should be enshrined in the scheme. The bill does some of those things. We are not suggesting that there are deficiencies there. It is the framework within which we should be working.

Senator FAWCETT: The same statement says that one of your purposes in trying to seek this balance is to minimise the regulatory burden on industry. Your top bullet point says that the data retention scheme should be 'proportionate to the threat level'. The two main concerns that seem to be raised are the period of retention and the scope of what is included in the dataset. Given that the threat levels that have been identified by agencies in the examples they have given range from child pornography and abuse through to terrorism and white-collar crime and things like solving Jill Meagher's murder—what they believe is the minimum dataset to enable them to continue to deal with those threats—if the scope of the data or the period of retention were changed, would it significantly alter the burden of regulation on the industry? If it was one month and two or three items of data versus what is there, what are you telling us is that you have to create this new system anyway to meet the new obligation. Would it significantly change the regulatory burden on industry if the period was two months, two years or five years?

Mr Shaw: The retention period is only one factor in determining the cost of the scheme. There is no doubt that, if you were to extend the retention period, you would get an increase in costs simply because you have a larger volume of information to collect and to manage and to index and to have available. So there would be an...
increase in capital costs; part of that is an increase in your operating costs in order to manage it all. But there could be significant cost increases if you suddenly changed the dataset and we had to go and find new elements of data in our network and bring them into that scheme, because to interrogate the network and collect and bring the data together could impose a requirement for new systems, and once you start to build new systems into our networks—IT does not come cheap.

So the answer to your question is: yes, if you change either the time period or the construction of the dataset, there will be cost impacts. The actual cost impact would depend on what you proposed to do. We are, unfortunately, dealing with a bit of a hypothetical there, so I cannot really go beyond that.

Senator FAWCETT: Sure. The point you are making, though, is that, if it is changed down the track, those costs accrue. At this point of defining the scheme for its implementation, the critics are saying two years is too long. What I am asking is: whether we say two years or one year, the actual regulatory burden for you is not going to significantly change if something is defined at the inception, as opposed to a change down the track, is it?

Mr Shaw: The costs will change if the prescribed period changes. We have costed to two years. If that were to change, then our costings would change. Will we get substantially different costs? Probably not, because a lot of that capital cost is setting up the systems to extract this data. But there would be additional costs just for keeping that volume of data for that period.

Senator FAWCETT: Sure. So, if they are not substantially from costs but we are addressing the same range of threats, then you feel two years is appropriate?

Mr Shaw: We do not have a view on the retention period. That is something, I think, for the government to determine, and we will cost accordingly and then implement a scheme that meets our obligations.

Senator FAWCETT: Okay. Thanks.

CHAIR: Just as a follow-up to that, some of your competitors are not keeping data for as long as you are; they have different platforms. The argument is that that can give them a commercial advantage over you. If this legislation were not before us and did not become law, do you think cost pressures would force you not to maintain as much data as you are now?

Mr Shaw: Our data collection and holdings at the moment are those that are necessary to run our business and provide services and to meet various regulatory obligations. We are mindful of our obligations under the Privacy Act to not retain information for any longer than is required for those sorts of purposes, so we retain and dispose accordingly. That is really what drives our current data retention practices.

CHAIR: Okay.

Mr RUDDOCK: But would you change it to try and meet your competitors—keep less information?

Mr Shaw: If we could run our systems by retaining less information and there was no business need to retain that information, then that is the way that we would design the system. To suddenly no longer collect large amounts of information would require changes within our network, and we do not make those changes lightly.

Mr RUDDOCK: But it is the organisations that are asking for the information. We have a fair degree of coverage because we still get Telstra and Optus—maybe we have 60 per cent, 70 per cent. If you change your model because of commercial practices, they may lose even that.

Mr Shaw: As I say, our perspective on all of this is—

Mr RUDDOCK: You are saying there is no need for you to change to meet the market?

Mr Shaw: As we change our business, as we introduce new products, or we might phase out an old system and introduce a new system—a new building platform or something, for instance—we would design that in order to meet business needs and whatever regulatory obligations there are. If that meant that we kept less data because we did not need to keep it, then that would be an artefact of that particular process. But I think there is a bit of tail wagging the dog in that sort of discussion of the data retention practice. It is not central to the way that we manage the business. The data retention is a consequence rather than the driver.

CHAIR: Every business has to keep its costs down. You are saying that this would put additional costs. Therefore, as you are going forward, if this legislation were not in place, you would be looking to minimise the amount of storage to keep your costs down. That has to be a logical flow-on.

Mr Shaw: We do that already. Some of the data that is being sought on a quiet day might be kept for a couple of weeks but on New Year's Eve is on the network for only a few hours. So we manage the network and dispose of data on a needs basis. To suddenly say we no longer want to collect this information and are going to dispose of it would require changes to the network which in fact cost more than the savings you might get from no longer
collecting the data. I mentioned the fact that we have a lot of legacy systems. Changing those legacy systems can be problematic, so sometimes it is best just to let sit. But it might be that in a few years time there is a project to overhaul our entire billing platform, and a consequence of that might be a change in our data retention practices. But to sit here today and say we are not going to keep that piece of data anymore, because it might save us a few thousand dollars compared to today—we look at this more holistically.

CHAIR: You are obviously with a legacy network going to have to modernise at some stage and continue to modernise, and cost is going to be an important factor in doing that. It might not be tomorrow, but down the track it would be a possibility.

Mr Shaw: It is a possibility, yes.

Mr BYRNE: So, on evidence, basically you are going to be required to create a new system where you will be able to store the data that the agencies and law enforcement bodies will want. You have indicated to this committee that you have said that would impose additional costs—by the sounds of it, substantial costs. In any of the conversations that you have had has the government offered to compensate you for any of those additional costs that you would incur in creating the system?

Mr Shaw: Yes. We have noted the comments of the minister when the bill was introduced about making a significant contribution to the costs. That has been an issue that has been discussed with the department.

Mr BYRNE: Have you been given a dollar figure for that?

Mr Shaw: At this stage we are still in the early stages of those discussions and PricewaterhouseCoopers is still undertaking its work.

Mr BYRNE: Without giving a dollar figure, would you be able to indicate a percentage of the impost that the government has offered to reimburse you?

Mr Shaw: We have not got that far in discussions yet.

Mr BYRNE: But you have a dollar figure, so you must have a percentage of the cost, you were just saying. So where are we at then? How much money do you think you will get back from the government?

Mr Shaw: We have not reached that stage of the discussions with the department yet.

Mr BYRNE: Right. When do you think you are going to reach that stage with the department?

Mr Shaw: Hopefully, sooner rather than later.

Mr BYRNE: For our committee purposes—because we are supposed to be writing a report on this—could you give us a rough indication?

Mr Shaw: I cannot. I think that might be a question you could put to the department tomorrow.

Mr BYRNE: I will be looking forward to talking to AGD.

In your mind, is this the final data set that you are going to be required to keep? On that point: have you been asked to make provisions for any further changes to the data set that you might be required to keep?

Mr Shaw: We do not rule out the possibility that this committee might make recommendations that could impact on the data sets, so we will respond to whatever comes out.

Mr BYRNE: What about discussions that you have had with AGD or within the technical working group? In any of those discussions has it been foreshadowed to you that there will be further changes?

Mr Shaw: Further specific changes?

Mr BYRNE: General changes or specific changes.

Mr Shaw: No, I am not aware of those sorts of discussions. I think the focus has been around interpreting the draft data set that has been put out.

Mr BYRNE: Is your organisations anticipating any further changes to the data set? Put aside the committee recommendations. Are you provisioning corporately for any further changes to the data set that you might be required to maintain at this point in time should it be passed into legislation?

Mr Shaw: We are not provisioning for anything at the moment. We are waiting for the outcome of the process. We do not rule out the possibility that there could be future changes to the data set, which is why we touched on certainty in our submission.

Mr BYRNE: Do you have a subsidiary in the United Kingdom?

Mr Shaw: We have operations in the United Kingdom, yes.
Mr BYRNE: The UK government has started to talk about changing the data set. My information provided by the United Kingdom is that they are looking at further enhancing the data set and are not entirely satisfied. Can you tell us or take on notice whether or not your UK operations are now starting to look at the data set that they were going to be keeping and might need to change?

Mr Shaw: We will take that on notice and get some advice from our UK counterparts.

Mr BYRNE: Thank you.

Senator FAWCETT: I take you back to the issue of costs. Paragraph 9 in your submission talks about court orders. You highlight there that, where there are civil litigation proceedings that do not otherwise involve Telstra, you sometimes receive a court order not only to produce data but to interpret it. You express a concern that the incidence of that may increase. Are those costs at all a factor in your discussions with the government, or is that something that at the moment you are anticipating you would continue to bear as a company?

Mr Shaw: Our submission goes on to recommend that industry should be given the ability to recover those costs of providing information to a court order. My colleague Ms Hughes, who manages that part of our business, could take you through a recent example that we received requesting information through the court processes, which we currently cannot recover the cost of and which runs to several pages and will take a significant amount of our resources to meet. We have been mindful that the existence of this data set could lead courts to seek to inquire from it, and if there is a court order then we have obligations in that regard. We think that is something the government should turn its mind to.

Mrs Hughes: Of the court orders we receive today, this one is eight pages long and in relation to a dozen or so services. It is about billing information, credit card information and so on and so forth. So it would take us four to five days to compile this information, and that is in relation to one subpoena. If we were to receive many more of these, it would be fairly onerous not just on our business but on every telco provider. I think you are right, James: the existence of the data set sometimes can act as inducement to issue us with further because it is an easy source of information within a court order. So I think we need to give consideration to that because it is not a simple request for very easily identifiable information.

Senator FAWCETT: So you preferred solution is that that is something you can recover from the legal system and that it becomes part of the court costs.

Mrs Hughes: I think it would be unfair for our consumers to be burdened with this cost. It should go back to the ultimate user of the information.

Senator FAWCETT: Thank you.

Mr DREYFUS: I want to explore that last topic of subpoenas. Telstra would receive subpoenas in both civil and criminal proceedings, and at the moment there is no means by which you can recover the costs from either the defendant or the prosecution in a criminal proceeding or from either party in a civil proceeding.

Mrs Hughes: That is correct.

Mr DREYFUS: And you would expect there to be an increase in the volume of subpoenas or court orders directed to Telstra.

Mrs Hughes: Yes.

Mr DREYFUS: And the suggestion in relation to this legislation is that there ought to be some cost recovery ability.

Mrs Hughes: Absolutely.

Mr DREYFUS: To contrast that: at the moment, there is some cost recovery available to Telstra in respect of authorisations or requests from law enforcement agencies under the Telecommunications (Interception and Access) Act.

Mrs Hughes: That is correct. It is a cost recovery model for all of the agencies.

Mr DREYFUS: Because Telstra probably is the company that receives or deals with more requests simply because of your size, I wonder if one of you is able to describe to the committee how the authorisation process
works. I would like it at a simple level because none of the submissions have really explained what actually happens. Let's say, for illustration, that it starts with an email from the Australian Federal Police.

Mrs Hughes: If only we were that electronic. Largely it is fax.

Mr DREYFUS: Fax is still electronic!

Mrs Hughes: Yes. We live in the dark ages, unfortunately.

Mr DREYFUS: So you get a fax?

Mrs Hughes: Often, yes.

CHAIR: Is that due to your legacy systems or theirs?

Mrs Hughes: Theirs. There is a list of agencies that are authorised. At the moment we believe there are about 70 that are authorised by the Attorney. They request, in a particular manner, information from us, and they can reach out and do a pre-authorisation check—so, if they know what they want to ask for and they are not quite sure how to ask for it, we can help them do that so that they do not give us something that we will not respond to or that is unlawful.

Mr DREYFUS: Just pausing there: you have got staff, who are dedicated staff—

Mrs Hughes: Very much so.

Mr DREYFUS: dedicated in both senses—

Mrs Hughes: Yes.

Mr DREYFUS: who are there to talk to law enforcement agencies to assist them in formulating the request?

Mrs Hughes: To assist them in understanding what we have and do not have. So: 'Don't put in a request, (1) because we will charge you for it, but (2) we may not have the information and you might be barking up the wrong tree.' So we might be able to say, 'No, we don't keep it; we can't help you with that,' or, 'The person doesn't have a service with us; you need to go and talk to another provider.' But if they proceed with an authorisation, we will receive that authorisation. It has to lay out the information very clearly as to what they are seeking. And then we have a team of people and systems to help deliver that information in the manner that they require it in. I think that there is often a lot of mystery around it. Very simply, it is often very simple metadata—the same sorts of information that you might be able to access from your bill: who you called; where you were when you made the call, by cell tower; a name and a billing address. I am sure people perceive that it is mysterious. It is actually, often—most times—very simple metadata.

Mr DREYFUS: So perhaps there is a pre-check, or perhaps not; the quickest pre-check is: 'Is this one of your subscribers?'

Mrs Hughes: Yes, that is right.

Mr DREYFUS: Then how long will it take? Perhaps that is an impossible question to answer; perhaps there is no average. But is there an average length of time or a common length of time that Telstra would take?

Mrs Hughes: We ask the agencies to tell us if the information is required urgently, and in peak times it could take a couple of days. If it is an urgent request, we may deal with it there and then on the spot, and we certainly ask the agencies to tell us if it is a priority request and the reasons for that. It might be that they have got something happening imminently in a court or whatever that they need the information for. We will make every endeavour to meet their time request. It is a 24/7 service, so we are always available to do that. But it also comes down to the complexity of the information they are asking for. So if it is very simple and urgent then we will respond immediately; if it is more complex but less urgent—so it can wait a couple of days—then we will take the time we need. We have very strict processes around how the information is confirmed and actually sent, and so we want to make sure we give ourselves the right amount of time to do that properly and securely.

Mr DREYFUS: Can you give us an illustration of what might be said to be an urgent case?

Mrs Hughes: An urgent case is a threat to somebody's life: a domestic violence situation; a child at risk—those sorts of things.

Mr DREYFUS: Just to take that last example: a child has gone missing; you might want to know—

Mrs Hughes: 'Can you tell us the last cell tower where that child's phone had some sort of activity?'

Mr DREYFUS: There are various terms for that tower information. It is sometimes referred to as VLR data.

Mrs Hughes: The technical terms do not matter to me.

Mr DREYFUS: Can anyone help me here?
Mr Burgess: It is VLR—visitor location register. That is if someone is roaming on our network. It would be a home location register if it were a Telstra phone. But that is kind of irrelevant to: 'Where was that phone last seen active?'

Mrs Hughes: And what sort of service—if the child has a mobile phone, then we are talking about a mobile service. 'Has there been activity on that phone?'

Mr DREYFUS: It has been suggested to us that Telstra does not keep visitor location register data for more than a momentary period—this being the phone not being actually used but sending its signal to nearby towers.

Mr Burgess: Could I just make sure I understand your question correctly so I can answer it?

Mr DREYFUS: I am trying to ask an open question to know what it is, in this particular area of tower data, Telstra keeps.

Mr Burgess: Today we will keep, and, for our purposes, we can tell you, that this phone call was initiated from this phone onto that tower. After that, if that phone moves around the city, we do not track what tower it goes to for the purposes of that billing event. That is why we capture the first thing—there is a phone call being made; there is a charge; we need to account for that for billing purposes. Separately in our system, as we are maintaining a call or allowing a phone to maintain data connectivity if it is talking to a weather app or doing some web browsing, we do know—the system knows; the humans do not know—where that phone is. So, in that case that Mrs Hughes gave, if we are looking at where a phone was last seen, we are able to interrogate our system and, depending on the load of the system, we may well be able to answer that question and say, 'At 2.45 yesterday, we saw that phone for the last time attached to that tower.'

Mr DREYFUS: Because the phone has sent a signal; that is how—not necessarily for the purposes of the call.

Mr Burgess: It could have just been a heartbeat to say, 'Phone here—connectivity ready for when the user needs it,' or it could have been that there was activity from that phone that needed connectivity.

Mr DREYFUS: How long does Telstra now keep that kind of data?

Mr Burgess: The answer, I am afraid, is, 'it depends.' It actually does depend, because, if there is a load in that particular area, it can roll off quickly or it could be there for one or two months.

Mrs Hughes: Similarly, if it is a phone call then we will keep that.

Mr DREYFUS: Of course.

Mrs Hughes: So if you made a call and it bounced then we will keep that for six years.

Mr DREYFUS: That is understood. I am trying to get it for non-phone-call, non-use data.

Mr Shaw: At a cell site on New Year's Eve, that data would be overwritten far more rapidly than at a cell site out in a regional area where there is minimal traffic. It really comes down to the load on the network. These things are kept for network management purposes, and if the network is managing properly then we do not need to keep it. That is the way the systems are set up at the moment.

Mr DREYFUS: On that, I appreciate there are quite a lot of differences. You have attempted, Mr Shaw, in the confines of the time we have here to describe that variability in Telstra's system. This is not a criticism; I am trying to get to a factual appreciation of how your system works. Telstra keeps a range of data at the moment for its own commercial purposes—that is, for the purposes of billing customers and running the system. Is that right?

Mr Shaw: Basically, yes.

Mr DREYFUS: And also—and there might be some overlap—it keeps data because it is required to for the consumer code—for example, for that purpose.

Mr Shaw: Correct.

Mr DREYFUS: You have said that billing data is your most kept category, and you keep it for six years.

Mr Shaw: That is right.

Mr DREYFUS: Then there are a whole range of other data categories which you keep for lesser periods.

Mr Shaw: That is right.

Mr DREYFUS: Is Telstra proposing any imminent reduction of the data that it keeps?

Mr Shaw: No.

Mr DREYFUS: I am not going to hold you to that either. It might be that in two, three or five years time some different means of organising the business becomes available which might carry with it less data being kept.
I am just trying to get to whether or not, at present, Telstra has any imminent plan to reduce the data that it is keeping.

Mr Shaw: We have no proposals to substantially reduce our data holdings at this point in time. What we have at the moment is sufficient to meet our regulatory obligations and to manage our network and provide services to customers.

Mrs Hughes: But I do think it is important that the committee be mindful that the Privacy Act requires us to delete information after we no longer require it.

Mr Dreyfus: Yes, and that is part of one of those basic privacy principles, which is that you are entitled to collect personal information for the purposes that you have publicly stated to customers but you are not to keep it for any longer than the purpose for which you have collected it remains. Once that is gone, your obligation is to destroy the data.

Mrs Hughes: That is correct.

Mr Dreyfus: I also want to follow up on something else. I know you have been asked a number of questions about cost already. The committee is in the position that it has not been provided with any cost estimates at all; there have been some wildly divergent cost estimates offered in public discussion. I will start with this: are you in a position to give us, not for Telstra as a particular corporation but for the industry as a whole, any estimate of the capital cost? The question is asked in the context of the government having said that this will be a substantial cost to taxpayers.

Mr Shaw: Unfortunately, I cannot speak on behalf of the rest of industry. We can only look at the Telstra situation and, as our submission says, we believe there would be a significant cost. We regard that number as being commercial-in-confidence, but it has been provided to PricewaterhouseCoopers on that basis.

Mr Dreyfus: At some point this is going to have to stop being commercial-in-confidence, because the taxpayer is going to pick up the bill, Mr Shaw.

Mr Shaw: I understand that and I think that is the delicate balance that the Attorney's department will have to strike in assessing what they get for PricewaterhouseCoopers and how they share that with the committee.

Mr Dreyfus: Is there any way that this committee and the public can get some feel for this? Are we talking hundreds of millions of dollars or tens of millions of dollars? That is an order of magnitude—

Mr Shaw: You are drawing me into an area where I am quite uncomfortable, given the commercial-in-confidence nature of that figure. I can say we have been willing to share that with the government and I presume they have some plan about how they will draw together the inputs from the various contributors from the industry in preparing the advice to government on the cost of the scheme.

Mr Byrne: So if we did this in camera you could tell us, could you?

Mr Shaw: If it was in camera, I would still ask that it be treated as commercial-in-confidence.

Mr Byrne: Yes.

Mr Dreyfus: I am not sure how much further I can take this, but perhaps let's go to the two types of cost. There is the capital cost, and that is created by the cost to the corporation of setting up a system which you do not presently have—

Mr Shaw: Yes.

Mr Dreyfus: which will do two things. It will store the data in a particular way for ease of access and capture and keep data that you are not presently keeping.

Mr Shaw: Yes—capture, index, retain, secure, make available and ultimately dispose of.

Mr Dreyfus: Yes, and then there is an operating expense. I think we can all grapple with the idea of the capital expense. What makes up the operating expenses associated with a data retention scheme?

Mr Shaw: The work of Kate's team in taking those requests, processing the requests and providing the data back to the agency—so going into the system, assessing the request to start with to determine that it is lawful, examining our systems to extract that record and then making it available to the agency.

Mrs van Beelen: Could I just add that there are also, of course, the operating expenses associated with running the system. So there is the capex to invest in the systems required. Then those systems need to be created and maintained. That is an operational expenditure. Then, as Mr Shaw has pointed out, there are the costs associated with answering specific requests, and it is largely Mrs Hughes's team who interact with the law enforcement agencies and respond to their requests.
Mr CLARE: Could I ask one final follow-up question from Mr Dreyfus's question about operational expenses. In evidence last year the Communications Alliance said that the opex costs of the data retention scheme, depending upon how long data must be retained for, were exponential rather than incremental. They said that the amount of time data is held is critical in understanding the real cost, not just capital but operational. Also, because of the likelihood of much more data being created and much more data needing to be held in the years ahead, any decision by the parliament about how long data must be retained by a company like Telstra would have a significant impact on the total cost of the scheme. Would you care to comment on the evidence given by Comms Alliance that the length of time data must be held would have a significant impact on opex costs?

Mr Shaw: I am not sure that we necessarily agree on the use of the word 'significant'. It certainly has an impact on cost, because the more data there is then the greater the task to continue to maintain that database, make it accessible and then to interrogate when required. With changes it becomes more complex. So there is a relationship between the retention period and the cost of the scheme. I am not sure that we would go as far as saying it is significant, but it is certainly a factor.

Mrs Hughes: And as new products and devices are offered up into the system they would need to be added and they would create more data. The data we are capturing today—it is not a year-on-year increment—is massively bigger than it was five years ago as more and more people have smart phones and use them more and more to do more things. With more devices, more products, out there, they will also need to fit into the scheme, and that data needs to be captured as well.

Mr DREYFUS: That was the first mention we have had—just in that last question—about 'the internet of things', which is what I take you to be talking about, Mrs Hughes.

Mrs Hughes: I was actually just talking about new handsets, new apps.

Mr DREYFUS: Some of the submissions we have received talk about the very greatly expanding number of devices on the internet—not merely handsets but all manner of other devices that are henceforth going to use the internet. So we will have not only a steeply rising number of devices but also a steeply rising amount of data. Will this data set in its present draft form—the only data set we have been provided to look at—hypothetically at least capture all of those new devices and increasing data that is likely to come onto the internet?

Mr Burgess: It depends on the device but generally yes. Remember that, with 'the internet of things', we are talking about internet connected devices. So this data set is asking us to keep the IP address associated with that device tied to a customer. As that grows, that requirement will grow.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward it to the secretariat as soon as possible—and there was that one request. If the committee has any further questions, the secretariat will write to you.
CHAIR: Welcome. Would you like to comment on the capacity in which you appear before the committee?

Mr Lawrence: I appear before you as a representative of Electronic Frontiers Australia but I am also a non-executive director of the Internet Society of Australia, from whom you will be hearing evidence this afternoon.

CHAIR: Although the committee does not require you to give evidence under oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given to day will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Lawrence: I do. EFA has been advocating for the promotion and protection of civil liberties in the digital context since January 1994. In fact, last week we quietly celebrated our 21st birthday. We are an independent, member based national association.

EFA believes that an indiscriminate, society-wide mandatory data retention scheme such as is proposed in this legislation is an unnecessary and disproportionate invasion of the privacy of all Australians, including of course everyone here today in this room. I invite committee members to reflect on this point: are you comfortable with a record of every phone call you make and receive being stored for two years and potentially being leaked onto the web? Such a scheme also subverts the principle of the presumption of innocence by collecting information about every single Australian’s online and telephonic communications, regardless of whether they are a suspect.

Further, as I believe we have heard from the previous testimony, it adds significant costs to a range of businesses, has the potential to reduce competition particularly within the ISP sector and will drive up internet costs for all Australians. This legislation will also create the potential for serious harm to Australians should the enormous databases of personal information that will be created be misused or compromised. EFA believes that, should this legislation proceed, it will not be a question of whether some of this information is compromised or misused but rather when and by whom.

If there are any illusions as to the likelihood of such compromising occurring, I invite committee members to reflect on the recent hack of Sony Pictures and, to give another example, on the alleged compromising of the personal details of hundreds of thousands of Australians who are customers of Aussietravelcover, a breach which, incidentally, that company decided not to disclose to their customers.

The reality is that the only truly secure data is data that does not exist. The Prime Minister, the Attorney-General and other advocates of this bill have asserted that the collection and retention of communications data is less intrusive than access to the content of communications. EFA totally rejects this assertion. Bulk collection of communications data is, arguably, more invasive for a number of reasons. As the European Union's Court of Justice said in its April 2014 judgement that ruled that the European Union's data retention directive was invalid, bulk collection of communications data — and I quote:

… may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments …

This court's ruling of invalidity was based primarily on the directive's indiscriminate nature. It is clear that mandatory data retention has been tried and tested in many countries within the European Union, has failed the test of effectiveness and also the tests of legality and proportionality. Despite this clear statement from a major supranational court, the Attorney-General's Department continues to rely on this now discredited data retention directive as the basis for this legislation. EFA of course understands that Australians lack the constitutional protections for their civil liberties that our friends in the European Union and the United States enjoy.

This committee therefore has a critical role to play in ensuring that the civil liberties that are what we believe makes Australia what Australia is are not discarded in the name of some generic terrorist threat or in order to protect us from the tiny percentage of men who prey on children. EFA urges this committee to take this responsibility very seriously.

EFA is, along with 400 other civil society organisations from around the world, a signatory to the International Principles on the Application of Human Rights to Communications Surveillance which, as I have told this committee previously, can be found at necessaryandproportionate.org. EFA believes this legislation falls well
short of these principles and should therefore be withdrawn. EFA is not however opposed to targeted surveillance with appropriate safeguards and oversight. We support the important and necessary work that our law enforcement and intelligence agencies perform on a daily basis. However, we believe that the existing powers available are sufficient for them to perform this work.

EFA would particularly like to point to the data preservation notice scheme, which came into force on 1 March 2013, when Australia acceded to the Council of Europe Convention on Cybercrime. EFA believes these data preservation notices provide a more appropriate, targeted mechanism for access to communications data on persons of interest. However, we understand that this relatively new power has, to date, been rarely used. These notices provide for mandatory retention of both communications data and content on suspects and persons of interest, while leaving the tens of millions of innocent Australians well alone. EFA believes that this existing power should be used and tested for efficacy. If it is insufficient, then clearly it must be repealed.

EFA is also unconvinced about the efficacy of mandatory data retention regimes. In January 2014, the United States's Privacy and Civil Liberties Oversight Board found that there is little evidence that the US's metadata program has made the US any safer. In 2011, the German parliament's legal service found that their mandatory data retention regime had increased crime clearance rates by only 0.006 per cent.

There is one element in this legislation which EFA does support, which is the restriction on the number of agencies that are given warrantless access to communications data. This is a necessary and urgent reform which, during the last parliament, this committee itself recommended. EFA is, however, somewhat concerned that despite this restriction the legislation provides the minister with the power to add other agencies to that list without reference to parliament. EFA fully supports any legislative safeguards that prevent the expansion of authorised agencies.

Most gravely, EFA is concerned that the legislation does not even define in detail the dataset that is sought for retention. EFA believes that defining the dataset by regulation, as is currently proposed, represents a serious undermining of the role of parliament and will enable the scope of the dataset to expand without proper scrutiny. History shows us only too clearly that schemes such as this almost inevitably expand in scope over time. EFA is also entirely unconvinced by the proposed two-year retention duration and is unaware of any evidence that suggests that this time frame is in any way justified.

Finally, in closing, I would like to point to some recent research which shows that this scheme is actually deeply unpopular within the community. Essential Research surveyed 1,842 people in the week of 18 February 2014 and found that 80 per cent of respondents 'disapprove of the Australian government being able to access their phone and internet records without a warrant'. In the week of 12 August 2014, Essential Research surveyed 1,845 Australians and found that 49 per cent of respondents felt governments are 'increasingly using the argument about terrorism to collect and store personal data and information, and this is a dangerous direction for society'. In that same survey they also found 68 per cent of respondents had little or no trust in the government, telcos and ISPs to 'store retained personal data safely and in a way that would prevent abuse'.

Mr NIKOLIC: Mr Lawrence, you totally dismiss the utility and effectiveness of metadata. I wonder whether you have had—

Mr Lawrence: I do not do that at all.

Mr NIKOLIC: Can I finish my question before you respond?

Mr Lawrence: Sure.

Mr NIKOLIC: You said 'metadata has failed the test of effectiveness'. Those were your words. Have you had an opportunity to view or read the evidence to this committee from the Australian Federal Police and a variety of agencies that say that metadata is central to virtually every counter-terrorism, counter organised crime, counterespionage and cyber-security investigation, that it is used in almost every serious criminal investigation, including for murder, rape, kidnapping and child exploitation, and that the critical role of telecommunications data in law enforcement and security agencies can be seen through its impact on a higher range of high-priority investigations? Have you had a chance to either hear or read the evidence of those people?

Mr Lawrence: I have, and I certainly do not dispute the fact that communications data is a very, very valuable and important tool for both law enforcement and intelligence activities. What I am saying is that indiscriminate, society-wide mandatory data retention regimes have been proven to be ineffective. We are not in any way opposed to appropriately targeted surveillance. As I said, we believe that there are sufficient powers on the books already, particularly with relation to the data preservation notices that came in in 2013, to provide the ability for law enforcement and intelligence agencies to ensure that they are able to access this data.
Mr NIKOLIC: But these agencies do not agree with you. They are saying that it is insufficient at the moment. In your argument that what they have at the moment suits their needs, what is the experience of your organisation or you in counter-terrorism, counter crime or counter paedophilia operations to be able to make the judgement that what those agencies have at the moment is sufficient for their needs despite their absolute clear and unequivocal advice to this committee that that is not the case?

Mr Lawrence: I think it is entirely self-evident that I have no experience in counter-terrorism, counterintelligence or counter paedophilia. What I do have is access to research that has been performed in the European Union and the United States—

Mr NIKOLIC: No, I am not talking about research in Europe; I am talking about advice to this committee from agencies like the AFP that what they have at the moment is entirely insufficient, given the adaptive nature of the threat that we have seen—the resurgent threat of terrorism and paedophilia networks, which are becoming increasingly adaptive. Your evidence to this committee just a moment ago was that what they have is sufficient for their needs. So, I am searching, frankly, for how you would justify that. It must be on the basis of some more superior knowledge than that of the people who are actually conducting these operations.

Mr Lawrence: I am going to repeat my previous answer, Sir. We have looked at the experience of the European Union and the United States, where there has been extensive research done on these schemes, and they have been found, as we believe, to be unnecessary and disproportionate. That does not mean that we do not think that information should be kept on persons of interest. There are already very broad powers available to law enforcement and intelligence agencies to access that information right now. As you would be aware, in the year to June last year, I believe, there were something like 600,000 authorisations for communications data processed in this country. There is no shortage of information available to law enforcement and intelligence at this point.

Mr NIKOLIC: So, you would prioritise research, undefined at this stage, over the clear evidence of agencies involved in the conduct of these operations and keeping our society safe that what they have at the moment is insufficient. I understand your point.

Mr RUDDOCK: My understanding is that metadata is not used primarily in relation to proving offences against people of interest; it is in fact used to discover who might be of interest to undertake further inquiries. And when you eliminate that as a tool, there will not be anybody of interest.

Mr Lawrence: Okay. Was that a question, sorry?

Mr RUDDOCK: Well, it is a statement, with which I thought you may want to perhaps disagree. But I am simply asserting that metadata is used to discover who might be of interest.

Mr Lawrence: I am going to repeat my previous answer, Sir. We have looked at the experience of the European Union and the United States, where there has been extensive research done on these schemes, and they have been found, as we believe, to be unnecessary and disproportionate. That does not mean that we do not think that information should be kept on persons of interest. There are already very broad powers available to law enforcement and intelligence agencies to access that information right now. As you would be aware, in the year to June last year, I believe, there were something like 600,000 authorisations for communications data processed in this country. There is no shortage of information available to law enforcement and intelligence at this point.

Mr NIKOLIC: So, you would prioritise research, undefined at this stage, over the clear evidence of agencies involved in the conduct of these operations and keeping our society safe that what they have at the moment is insufficient. I understand your point.

Mr RUDDOCK: My understanding is that metadata is not used primarily in relation to proving offences against people of interest; it is in fact used to discover who might be of interest to undertake further inquiries. And when you eliminate that as a tool, there will not be anybody of interest.

Mr Lawrence: Certainl

Mr RUDDOCK: If you take it away, who do they inquire into? They have nobody of interest.

Mr Lawrence: I think the problem with that approach is that if you take that to its logical extension it means that we retain everything about everyone, forever. And there has to be a limit. We are a free society. Australia, as I mentioned in my opening statement—not necessarily by design, because we do not have a lot of the civil liberties written into our Constitution that many of our friends in the US and the EU enjoy—is a very free, open, diverse, wonderful society. And I think we need to retain those elements.

Mr RUDDOCK: I understand.

Mr Lawrence: And particularly when you start to wrap it into issues such as section 35P, the anti-whistleblowing element of legislation that has already passed this parliament, I think there are genuinely dangerous threats to freedom of expression and privacy in this country.

Mr RUDDOCK: Well, there may be, but you argue this in terms of human rights.

Mr Lawrence: I do.

Mr RUDDOCK: I would put it to you that the right to life, which is a human right, is of fundamentally greater importance than the right to privacy.

Mr Lawrence: Absolutely, and you said so last time I appeared before this committee.

Mr RUDDOCK: So, in terms of counter-terrorism investigations, which are likely to protect people's lives, I would not want to lightly give it away.

Mr Lawrence: Of course the right to life is greater than the right to privacy. You said this to me the last time I appeared before this committee. And the reality is that, as I have said, there is an enormous amount of data already available to law enforcement and intelligence agencies. There are already very broad powers, as you would yourself be well aware, available to law enforcement and intelligence agencies. There are the data
preservation notices, which allow them to order a telco or an ISP to retain both content and communications data on any person of interest for a three-month period—

Mr RUDDOCK: In relation to a person of interest.

Mr Lawrence: Our point is not that this information is not valuable; our point is that an indiscriminate, society-wide mandatory data retention scheme is a step too far.

Mr RUDDOCK: The inquiry that the agencies are interested in is how they identify those about whom they should make inquiries. It is level of connectivity that is often the key to identifying who may be appropriate to further investigate.

Mr Lawrence: I do not dispute that for a second.

Mr RUDDOCK: Can I just go to the two points in your submission where I could not find evidence to support what you were saying. Firstly, what would be a more efficient and inexpensive solution to achieving what the agencies need—that is, to identify people of interest—that you are suggesting is available?

Mr Lawrence: As I have said a number of times, there is already a great deal of information available to agencies. They already have power such as the data preservation notices to ensure that data is retained. The reality is that what we can loosely term as 'signals intelligence' will never be as powerful as the human intelligence that our intelligence agencies are really good at.

Mr RUDDOCK: I was also looking for objective evidence that you might be providing of the real possibility of data retention being misused.

Mr Lawrence: How long have you got?

Mr RUDDOCK: I read the submission.

Mr Lawrence: That is a fair question, sir.

Mr RUDDOCK: I am looking for the objective evidence of the data that is now retained being misused.

Mr Lawrence: Data is misused every day all over the world. We know from Edward Snowden that analysts within the National Security Agency in the United States routinely used this sort of information to stalk potential and current lovers. They even had a term for it. They called it 'LOVEINT'. They only know that by their own admission because people told them that they did it. There is no other mechanism for this to be detected. We know there is an example from, I believe, Ireland where a member of the Garda, their federal police agency, had done the same thing. They had used this sort of information to stalk a former lover. There is some evidence that Victoria Police has been at least some point in the past infiltrated by bikie gangs. That sort of information being available to those sorts of organised crime figures is a very real and very serious threat to the security of all Australians.

Senator BUSHBY: Mr Lawrence, you have made the point that you accept that there is value in the use of metadata by law enforcement security agencies but that you think they have sufficient abilities now to deal with it. As I understand it, what we are talking about here is that this bill does not increase the powers of law enforcement and security agencies to access data—in fact, it actually tightens that up a little bit by, as you acknowledged earlier, refining which agencies can access the information. Do you acknowledge that it does not increase the powers to access; it just provides a more consistent dataset for a longer time than what might otherwise be available? Secondly, all of the data that will be required to be held under this bill by organisations is currently held, albeit in some cases only instantaneously, by those organisations at the moment? You don't acknowledge that?

Mr Lawrence: No. That point has been made a number of times, particularly by Steve Dulby from iiNet.

Senator BUSHBY: How is an organisation supposed to retain data if it doesn’t have it at any time?

Mr Lawrence: I think it is very clear. Let's of course remember that we do not have a finalised dataset, despite the fact that the Attorney-General's Department has been working on this issue for about a decade. We still do not have a defined dataset. I believe Telstra in their evidence just before me acknowledged that there is certain data that they do not retain for any particular period of time.

Senator BUSHBY: But it passes through. There must be data that passes through that they have in their possession, albeit instantaneously?

Mr Lawrence: Yes.

Senator BUSHBY: There is no data that will be required to be held that those organisations do not have access to at some point, even if they do not currently capture and hold it?

Mr Lawrence: Yes, I believe that is a true statement, but I am not sure how relevant that is.
Senator BUSHBY: I am just trying to establish a few things that are knowledge. So everything that goes through is something which those organisations could hold.

Mr Lawrence: They cannot just manufacture data.

Senator BUSHBY: No, exactly, or have to go out and find it somewhere else.

Mr Lawrence: No, that is fair enough, sure.

Senator BUSHBY: Currently, law enforcement and security agencies already have the power to access all of this data if it is available. Do you also acknowledge that there are business practices and new business models, particularly with the newer providers, which are built on models that do not require them to capture the same information that some of the more traditional providers are holding? Are you aware of the evidence from law enforcement and security agencies around their current abilities to access data which they have used in a number of cases we have had evidence of that have been key to resolving security and criminal activities? Their main concern is that that data, because of these changing business models, will not be available to them and in the future, when they go seeking this information and metadata that they do use usefully, it will not be there. As a result, there will be consequences in their ability to deal with security threats and to resolve criminal activities. Do you acknowledge all of that?

Mr Lawrence: I certainly do, yes.

Senator BUSHBY: So what is the answer if that data that is currently available or has in the past been available to and accessible by our law enforcement and security agencies is no longer available? Is there an alternative? You have mentioned some things, which we can get into in a minute, as to why that probably would not work, but is there an alternative to enable the law enforcement and security agencies to have access to the information they need to put together who might be persons of interest so that then they can go on to the more intrusive warrants to phone tap to look into content and all those sorts of things, to help them identify who to apply those more intrusive elements to? How do they actually get to that point without their metadata if those business models continue to the point where that data just does not exist for them to access?

Mr Lawrence: There are two points. I agree with everything you have said there. As the Attorney-General's Department itself points out in its submission, there is a long-term trend towards less and less of this data being collected by telcos and ISPs.

Senator BUSHBY: If I may, that, as I understand it, is the main motivation behind the law enforcement and security agencies requesting the retention of the data—because they are concerned that the data will not be there when they need it.

Mr Lawrence: Yes, that is understood. There are a couple of points I would make. One is that, as you point out, this is a long-term trend. There is nothing particularly urgent about this legislation that we are aware of. The other point is that I think we are in danger here of re-engineering the way we manage our society in order to increase the convenience of law enforcement and intelligence, and I am not entirely sure that that is the right approach. I think it has been very evident that access to communications data under the current regime has massively expanded in scope over time, particularly in terms of the range of organisations that are accessing it. We are all aware of the Victorian Taxi Directorate and Wyndham City Council and all those sorts of things. I think there is a definite trend here that this information is being accessed because it is easily available. To me, that is not necessarily a justification for why it should be. As I have said, we are not in any way opposed to appropriately targeted surveillance.

Senator BUSHBY: You mentioned that before. With appropriately targeted surveillance, the reality is that, if you actually have a person of interest of sufficient concern, there are more intrusive methods, and that is usually when they are utilised. You have identified somebody you have believe there is an issue with and then you can go off and use the normal traditional methods to get search warrants or whatever—phone tap warrants and so on. It is the stage before that that the evidence to us suggests is so vital. It is the stage at which you know there is a problem with somebody and then you might use contacts that they have with other phones to piece together a network of persons of interest so that you can then go to the next stage.

It is the data that is available, which has previously and historically been retained, that has made that possible and which the law enforcement and security agencies are concerned might not exist in the future and therefore they will not be able to work out who is in that network of persons of interest to go to the next, more intrusive level. Being able to say that we can look at the data of persons of interest when they are persons of interest, as Mr Ruddock pointed out, is sort of putting the cart before the horse in a way because you do not know who they are. It is the ability to go back and piece together that puzzle that is so vital for law enforcement and security agencies in order to access it.
You also made the comment that this is changing society. That comes back to my earlier question. The data is all there, and we are only asking the old organisations to hold that data. It is not like it is going in and being trawled through and accessed; there are very strict protocols—and I think they are being tightened up under this bill as well—in terms of when you can access and what you can do with that information. In the absence of a law enforcement and security agency accessing that information under those very tight circumstances, it is just held by the provider for a longer period and a clearer more consistent set of data than they might otherwise have done. That is really the only change that is occurring. So I do not see how that changes society. You might care to explain to me how this is a fundamental societal change.

Mr Lawrence: It all comes back to the fact that this is an indiscriminate scheme. It mandates the collection and retention of information about every person in this country. That is our primary objection. As I have said, we are in no way opposed to appropriate targeted surveillance. At the core of the European Union's Court of Justice judgement against the European Union data retention directive was that it was invalid and incompatible with the European Charter on Human Rights, because of its indiscriminate nature.

Senator BUSHBY: Mr Lawrence, I hear what you are saying, but on the other side we have to weigh up the importance of this data in being able to address security issues and solve serious crimes. If the data is retained, what would make you more comfortable in terms of the security of that data? Is there some way that we can go forward to satisfy you and satisfy the security and law enforcement agencies?

Mr Lawrence: As I said, I believe that those powers already exist under the data preservation notice scheme.

Senator BUSHBY: Thank you.

Mr CLARE: Mr Lawrence, I appreciate that the view of EFA is that it does not support the proposed scheme. What I am keen to seek your views on is some of the reoccurring themes that come through all of the submissions that the committee has received to date. It seems to my mind that there are about half a dozen issues constantly raised in the submissions from industry and the general public. One relates to whether the definition of metadata should be in the bill or in regulation. Another deals with cost. Another deals with how long the data should be retained—two years or more or less. Another deals with security. That is a constantly reoccurring theme. Oversight is also raised, as are definitions of serious crime and law enforcement agencies and also the exploitation of this data via court order—and there may be one or two others.

They appear to me to be some of the reoccurring themes that we are seeing coming out of submissions. I am keen to seek your views and your organisation's views on those issues. You have mentioned some of them in your introductory statement. I will step through some of them. What is the EFA's view on the issue of the definition of metadata or the dataset and whether it should be in legislation or regulation?

Mr Lawrence: As I said, we firmly believe that, if this legislation proceeds, the dataset must be defined in the legislation. We believe that to do otherwise is to seriously undermine both the role of this committee and the role of the parliament generally.

Mr CLARE: On the issue of the amount of time that data should be retained, you made the point in your introductory comments that you thought two years was too long. Would you care to expand on that or express a view on an alternative for the committee to consider?

Mr Lawrence: In short, I would not, because I am not proposing this legislation. The reality is that those agencies and individuals that are advocating this legislation have completely failed to make any case for why two years is an appropriate length of time.

Mr CLARE: On the issue of security of data that is retained, in 2013 this committee made a recommendation that, if data were to be mandatorily retained, it should be mandatory that organisations encrypt that data. My understanding is the legislation is silent on that issue. Do you or does EFA have a view on what further steps should be taken to make this data more secure? I recognise your point that no data is secure once it is created. But do you have a view that you would like to express to the committee about what steps should be taken that have not been taken to date in relation to this legislation?

Mr Lawrence: Clearly, the encryption of data is an absolutely basic requirement. However, this legislation will result in the creation of what will be massive databases of very, very valuable personal information that will be honey pots to organised crime and to any sort of person that can potentially access it. Now, the scope of risk, for example, for systems administrators who must look after this data to be compromised in some way is very high. As Steve Dalby from iiNet said in a room not far from here last year, when asked about this, 'Look, we're a business; we're going to try and find the lowest cost option for storing this data,' and right at the moment the lowest cost option for storing data is in China. So there is a very real risk also—as this committee, I am sure, is only too well aware—of this sort of information being compromised by foreign intelligence agencies as well.
Mr CLARE: And I am very conscious of the fact that with security comes cost and that the more obligations parliament places on ISPs the more costly this scheme will be. I would not be misrepresenting you, I am sure, if I were to say that it would be your view that it is important to make this data as secure as possible.

Mr Lawrence: Of course.

Mr RUDDOCK: Encryption is costless, is it?

Mr Lawrence: Encryption is costless?

Mr RUDDOCK: Yes.

Mr Lawrence: No, not at all. Encryption adds very significant costs for a whole range of issues, such as processing power. I have a history degree; I am not a technologist—but there are processing costs, there are additional interface costs in terms of managing data and so forth. So encrypting data is far from costless.

Mr CLARE: One of the other things that this committee recommended in 2013 was a breach notification system. I have the report in front of me. Recommendation 42 included, inter alia, 'a robust mandatory data breach notification scheme'. That is another recommendation that has not been picked up in this legislation. I am keen to seek your views about the relevance of such a scheme.

Mr Lawrence: Absolutely. I touched on this in my opening statement. There was a very recent incident which I think bears out the need for this legislation, which was the hacking of the database of an Australian travel insurance company, Aussie Travel Cover, which resulted in the very personal details of hundreds of thousands of Australians being compromised—and of course insurance companies are one of the organisations to which people do tend to give very, very detailed information, for obvious reasons. That was an incident which was uncovered and reported in the press. What was interesting was that the company had actually made a conscious decision not to disclose to the affected customers the fact that this information had been breached. That, to EFA, is just unconscionable behaviour. We believe that it is good business for companies to treat their customers with due respect and to make them understand that they take their personal information seriously. This is increasingly becoming a competitive issue across a whole range of industries. People are generally becoming more conscious about the privacy and security of their data. What was also quite ironic is that this story broke on the same day that President Obama announced plans to legislate in the United States for such a mandatory data breach notification scheme.

Mr CLARE: This committee also recommended in 2013, at recommendation 42, inter alia, that 'an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers'. That was another recommendation of our committee that I understand the legislation has not taken up. Does EFA have a view on that?

Mr Lawrence: I believe there are certain circumstances, such as—not to labour the point too hard—where a data preservation notice has been issued, where storage of content and communications is required. Other than that, I genuinely cannot see any reason why a company would choose to do that.

Mr CLARE: I think that what was proposed—and I was not a member of the committee at the time—was that this independent audit function would be established within a government agency as opposed to within the ISP. My question to you is: would EFA support the recommendation proposed by this committee in 2013, which is that 'an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers'?

Mr Lawrence: Yes, we would support that.

Mr CLARE: Another recommendation of the committee in 2013 that the government has taken up in this legislation is ‘oversight of agencies’ access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security’. This is something that I understand the government has taken up in this legislation, but I am interested in the views of EFA, about whether they think that is the correct oversight model for a proposed scheme such as this.

Mr Lawrence: I think it is self-evident that additional oversight and additional resourcing of oversight is required. To be fair, the government has recognised that, but it still remains the case that the Inspector-General of Intelligence and Security has, I believe, 11 staff, which does not strike me as a whole lot of oversight going on. I do not believe that there is much proactive oversight on the part of that body. That may be something that could be addressed. I note that Mr Dreyfus has supported calls for the powers of this committee to be expanded to include the ability to look at operational issues in line with the equivalent committee in the United Kingdom's House of Commons. We would certainly support that. It is very important that this committee has real power to
provide that sort of parliamentary oversight and scrutiny that is, I would suggest, more important in the context of particularly secret intelligence activities than it is in many other contexts.

**Mr CLARE:** Finally, I go to the issue of access to metadata through a court order for the purposes of civil litigation. I am conscious that you may or may not have an answer to this question, but it is one that vexed this committee when we last met and it will be the subject of further questions to a number of organisations giving evidence over the next two days, I am sure. Whether it is piracy and copyright infringement, or whether it is health care companies using information acquired via your Fitbit to determine how many steps you took each day, there are legitimate questions about how this data could be used through the court system. No-one has presented an answer to this committee yet about whether or not any changes should be made to limit that, or whether that is a good or bad thing. My final question to you is, does EFA have a view about that.

**Mr Lawrence:** Yes. You have touched on the issue of alleged copyright infringement. In 2014 we have already seen the emergence in this country by the creators of the movie *Dallas Buyers Club* of the rather dubious business practice of what we might call speculative invoicing. That is a business practice that is fairly rampant in the United States. The creation and retention of this information for a two-year period will absolutely enable the expansion of that activity. We do not believe that that is in anyone’s interest.

I will preface my remarks by saying that I am not a lawyer. I am not aware of how the parliament could legislate away the ability of a competent court to issue a subpoena or court order, or whatever the proper terminology is, that would enable access to this information. I think it goes back to the earlier point I made about these databases being honey pots. They will be equally as attractive to hackers as they will be to commercial litigants.

**Mr DREYFUS:** Have you seen a finalised data set yet?

**Mr Lawrence:** No. I would be happy to write one for you!

**Mr DREYFUS:** As I understand it, your recommendation to the committee is that the bill be withdrawn, but, if it were to proceed, there should be a definition of the data set out in the legislation.

**Mr Lawrence:** Absolutely.

**Mr DREYFUS:** I thank you for the detailed submission you have provided to us, because it means we have in writing from you a detailed position. So, in view of the time, I am going to restrict myself to a couple of things that I want to tease out. The first relates to something on page 3 of your submission. It is a particular recommendation you have about the bill’s provision 187C(3). That provision reads:

> This section does not prevent a service provider from keeping information or a document for a period that is longer than the period provided under this section.

I raise this because we have just heard from Telstra a very clear exposition of their responsibilities under the privacy legislation, which is that they are prohibited from keeping information any longer than they need it for the business purposes for which they have collected it, and that they honour that obligation and propose to continue to honour the obligation. Is that the context in which you are suggesting that this section simply should be deleted?

**Mr Lawrence:** Yes.

**Mr DREYFUS:** Given that it simply says ‘This section does not prevent a service provider from keeping …’ in your view does the provision do harm by being there? In other words, what we have here is a statutory provision that imposes and obligation to keep information. It forces telecommunications companies to keep information that is to be prescribed by regulations—so you cannot tell from the bill what it is that is to be kept. But then it goes on to say that it does not prevent keeping it for longer. What is your objection to that provision?

**Mr Lawrence:** Because, as you have touched on primarily, it almost directly contradicts the Australian privacy principles. But, as you say, it may not be of significant harm for it to remain there.

**Mr DREYFUS:** And the other point that you have made here is the need for the list of agencies to be named. Are you able to speak to that for a moment—as to why it is that you think that there should be a complete list of agencies?

**Mr Lawrence:** As I said earlier, I think that is one element of the legislation that we do welcome, which is restricting the list of agencies that are able to access communications data. Our concern is that there is a big kind of ‘but’ statement at the bottom of that page, which says essentially ‘or any other agency that the Attorney chooses to appoint or to add to that list at any time’. We believe that that process, in the same sense that the dataset should be defined by legislation, should be something that is subject to proper parliamentary oversight and scrutiny.

**Mr DREYFUS:** And the final point I want to tease out is that you have here, in the submission, a concern expressed about the supposed exemption that is provided on the face of it by 187A(4) for content. Are you able to
explain further what your concern there is in that regard? You have described it as a supposed web-browsing history exception.

Mr Lawrence: Our general concern is, firstly, that we are yet to see a finalised definition of the dataset, which is obviously a massive problem. We believe that a political decision has been made that web-browsing history must be excluded from this scheme. We believe that that is probably quite a sensible political decision, because it would be deeply, deeply unpopular within the society, and our current Attorney-General is on record as saying that when he was a member of this committee in the last parliament. What we see, however, in the drafting of the legislation is a number of really quite serious inconsistencies and contradictions, which flow from this desire to exclude web-browsing history. And we have genuine concerns about the level of technical understanding of some of the people involved in drafting this legislation. It does tend to suggest that web-browsing history is intended to be included in the dataset at some point, and at the moment this is a political decision that has been made to exclude it. So, really our point there is that these schemes, by their very nature, as history tells us very clearly, tend to expand over time, often quite quickly. We would expect that this rather difficult and awkward exception for web-browsing history would potentially, at some opportune moment in the future, be quietly removed and that that sort of information on all Australians would be retained. And there are serious issues in the legislation even about things such as defining what the term 'communications' means that we have genuine concerns about.

Mr NIKOLIC: Perhaps I could ask a follow-up question on that. How do you quietly and surreptitiously amend legislation?

Mr Lawrence: Well, that is our point. It would not be in the legislation. As the legislation is currently drafted, the dataset would be done by regulation.

Mr NIKOLIC: Or regulations that are subject to disallowance. How would the government surreptitiously change the regulation to include web-browsing history? How would they do that surreptitiously and quietly?

Mr Lawrence: To be frank, at the moment, the way the legislation is written, we are not entirely convinced that it is excluded.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of the evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward it to the secretariat as soon as possible. If the committee has any further questions the secretariat will write to you. Thanks, Jon.

Mr Lawrence: Thank you.
CAMPBELL, Ms Suzanne, Chief Executive Officer, Australian Information Industry Association

ROCHE, Ms Suzanne, General Manager, Policy and Advocacy, Australian Information Industry Association

[11:14]

Evidence was taken via teleconference—

CHAIR: Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and it warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Ms Campbell: Thank you for the opportunity. The AIIA is the peak national body representing Australia's information technology and communications industry's interests. The Australia Information Industry represents over 400 member organisations nationally, including hardware, software, telecommunications, ICT services and professional services companies. Our members include global companies like Apple, Hewlett Packard, EMC, Google, HP, IBM, Intel, Novo, Microsoft, PwC, Deloitte and Oracle; international companies including Telstra and Optus; and national companies including Data#3, SMS, Tyrrell, Technology One, Oakton and a very large number of ICT SMEs.

We appreciate the opportunity to provide this response to you and to engage with the committee in this way in relation to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. As you will have read in our submission, while we support the objective of public safety and security proposed by this initiative, we do have a number of serious concerns in relation to the draft legislation and, in particular, that it may not be the most effective means to achieve the proposed objectives.

Our members' concerns relate specifically to the non-specific, all-encompassing nature of the draft dataset and the ambiguity that is currently present for service providers. We urgently need clarity in respect of the proposed exempt services. We are deeply concerned in relation to the financial impact on service providers and obviously, ultimately, consumers in relation to the proposed amendments. Our members are also concerned in respect of the two-year data retention period as proposed, noting in particular the inconsistency with international organisations.

Given these concerns, the AIIA has recommended a number of changes, principally, that the bill be delayed to allow more efficient consultation with various interested stakeholders and, in particular, to consider the reduction of the two-year data retention period to allow sufficient time to implement the necessary changes to infrastructure in order to provide for security and privacy concerns which have been raised and to allow for a better cost-benefit analysis so that the implementation of these proposed changes can be more fully understood by all interested parties.

We are also keen to ensure that changes are effected to provide for information which is only necessary for financial security to be retained and where we observe that this data is in fact a major security risk in its own right, is highly sensitive and therefore must be adequately protected. We are also concerned to ensure that any potential unintended security risks are appropriately managed and that consideration is given to that matter with the implementation of the bill. Thank you for the opportunity to provide opening comments.

CHAIR: Thank you. Do we have any questions?

Mr Ruddock: I had some difficulty earlier in the day in relation to a request from ASIC that it be allowed to access data. I asked for reasons why for issues relating to essentially a white collar crime but one that might occasion very significant loss to superannuation funds and individuals through activities that can be undertaken. They forcefully put it. You are arguing that we should only allow access to data for security purposes. You said 'changes only to ensure information related to national security is obtained'. Would you tell me why, for instance, serious law enforcement issues and significant white collar crime should be exempted?

Ms Campbell: The concern here for the purpose of the bill to be very precise and clear and harmonised with any other legislation, particularly legislation relating to privacy. We do not think that is the case at the present time.

Mr Ruddock: For instance, if you were investigating a murder—where right to life might be important!—you consider a right to privacy to be pre-eminent over right to life?

Ms Campbell: No. What we are saying is that we need clear harmonisation of the legislation with any other legislation.
Mr BYRNE: I notice that you represent Facebook, Twitter and Google.

Ms Campbell: Google is a member; Facebook and Twitter are not.

Mr BYRNE: Are these organisations you represent telling you that there is anything they are not capturing now that they would be required to capture and store under the draft dataset?

Ms Campbell: The telecommunications members of the AIIA have been clear about the current obligations under the Telecommunications (Interception and Access) Act 1979. They are also clear that they are compensated for what they provide under the data holding or data capture provisions of that act. The concern of providers about the over-the-top services such as web based mail services, VoIP services and Cloud services is that they are not clear as to whether they are captured by these provisions are not.

Mr BYRNE: VoIP is basically Skype; is that right?

Ms Campbell: It could be Skype. It is voice over IPs.

Mr BYRNE: You are saying that the people you represent who could administer that are unclear at this point in time, given that we are looking at the draft legislation, as to whether or not they are captured?

Ms Campbell: That is correct.

Mr BYRNE: Who has been consulted? Why would there be this ambiguity? I am concerned. Are you saying that, of all these organisations that you represent, a number of them are very unclear about whether or not they are going to be captured under this draft legislation?

Ms Campbell: That is correct.

Mr BYRNE: Have you been consulted by any organisation connected with the government or the technical working group?

Ms Campbell: Clearly we are participating in this process and were part of the consultation, and the ambiguity remains.

Mr BYRNE: So even though you have had detailed discussions with the technical working group and the Attorney-General's Department there is still ambiguity about whether or not these services will be captured?

Ms Campbell: That is what my members are saying.

Ms Roche: Can I just clarify that we have not been involved in the working group.

Mr BYRNE: You have mentioned Cloud providers—and obviously a lot of people are using cloud to store information and also services—and VoIP operators. How many organisations, people or groupings that are not aware if they are going to be captured under this draft data set would there be?

Ms Campbell: Our members have provided us with feedback in an anonymous way. I am not prepared to provide their names in this forum. We have to take the question on notice.

Mr BYRNE: So we could get that information? Then that would be confident.

Ms Campbell: If they are prepared to do so, yes.

Mr BYRNE: Yes, because other than that, that is hearsay. Consequently for the committee we need to have specific examples because the scope of the problem that you have mentioned is substantial. For the committee's
purposes, we would like to have specific examples from organisations that you represent. Otherwise I am afraid, knowing that sort of set of circumstances, it is hearsay. Other than us having hard evidence about that because the committee's task is to look at the draft set or draft regulations or the draft data set, and to make suggestions without— You have raised a very, very significant point, where this committee is going to need harder evidence than the verbal evidence that you have just provided to clarify that very substantial problem which you have identified.

Ms Campbell: I am very happy to take the question on notice. I am not at all happy with the characterisation of our evidence as hearsay. We are engaging in this process in good faith. Our members have provided us with their feedback. We have represented that feedback in our submission.

CHAIR: You do have the ability to provide us with a follow-up confidential submission. If you deem that as appropriate, I think that would help the committee in its deliberations and that can be commercial-in-confidence as well.

Ms Campbell: Thank you Chair, I appreciate the opportunity.

Mr CLARE: To follow on that line of questioning, I am very conscious that the organisations you represent have expressed some concern or doubt about whether and how they are captured by this legislation, has the Attorney-General's Department endeavoured to provide you with answers to those questions or is it your expectation that you might be getting some better information from the Attorney-General's Department on the issues that you have raised that are of concern to your members?

Ms Roche: Despite contact with the Attorney-General's Department they have not subsequently followed up other than to alert us to the opportunity to provide submissions—

Mr CLARE: I think we might have lost the end of that sentence, but if I heard you correctly, you said that you have not got that confirmed from the Attorney-General's Department yet?

Ms Roche: We have reached out to the Attorney-General's Department, but with the exception of notifying us of the process to input via this process of consultation, we have not had any other engagements with them.

Mr CLARE: Right. You have reached out but the Attorney-General's Department have no answered the question that really is of concern to your members and that is are they captured by the legislation or not? You do not have an answer to that question from the department?

Ms Roche: We were not invited to participate in any working group's process.

Mr CLARE: And you have not pursued that concern separately with the department?

Ms Roche: No, we have not. We have chosen to raise our concerns—

Mr CLARE: That might be something for this committee to pursue with the department.

CHAIR: Just to clarify this: your group was not but you have members who are participating in the working group?

Ms Campbell: We understand that to be the case. They are doing that in their own right; not as representatives of the AIIA.

CHAIR: When you have consultations around the bill, they obviously sit at the table as part of those consultations.

Ms Campbell: They may or may not choose to be part of that consultation process.

Mr DREYFUS: I have a follow-up question on the concern that you expressed in your written submission where you say:

Cloud providers and VoIP operators, for example, are unclear the extent to which they will be subject to the new legislation.

I think the committee would be really assisted if you were able to provide us with a little more detail as to why that is so. I am certainly not seeking to have it specific to a particular company. That is not our concern. The concern that we would have is that this bill proposes to insert a quite detailed provision in the Telecommunications (Interception and Access) Act 1979—a new part 51A, headed 'Data retention'. The first words of the new section 187A, which is right at the start, are:

A person (a service provider) who operates a service to which this Part applies (a relevant service) must keep— and then it goes on to prescribe what telecommunications companies are to keep.

Further, we read in 187A(3) a quite lengthy provision describing which service providers are caught. I will not read it all but it starts with:
This Part applies to a service if:

(a) it is a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both;

It is a very general provision. It then goes on to add:

(b) it is a service:

(i) operated by a carrier;

(ii) operated by an internet service provider—

Because it is apparent that the drafters have made some attempt to be specific about who is caught, it would be of real assistance to this committee in examining the detail of this legislation to have from you why it is that there is an uncertainty or a lack of clarity about who is to be caught. Because it is obviously pretty crucial—and we understand the scale of some of your members and the global nature of some of their operations—it is of concern to this committee. Sorry for the longwinded question, but do you think, you are going to be in a position to provide us with just a little more detail about why there remains a lack of clarity as to which operators and providers are caught?

Ms Campbell: I will attempt to answer the question—and I have already noted the opportunity to come back to you in a confidential way. Many cloud providers and VoIP operators do not understand themselves to be providers of telecommunications services. They operate applications that are used by you and I in our homes and on mobile devices. They do not necessarily understand themselves to be telecommunications service providers at all. They might be a provider of an application for a business purpose—recording of accounting data or the facilitation of communications—and they do not see themselves at all as providers of telecommunications services. We will come back to you in detail, as and if our members are prepared to provide additional information, but the heart of it is: they are not telecommunications providers.

Mr Dreyfus: That is helpful; thanks very much. We would welcome anything additional that you can provide to the committee.

Chair: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material—which we have sought, if possible—please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.

Ms Campbell: Thank you very much, Chair, for the opportunity.
GRiffin, Mr Michael, AM, Integrity Commissioner, Australian Commission for Law Enforcement Integrity

MARSHALL, Ms Sarah, Executive Director, Operations, Australian Commission for Law Enforcement Integrity

MCKAY, Ms Penny, Principal Lawyer, Australian Commission for Law Enforcement Integrity

SELLARS, Mr Nicholas, Executive Director, Secretariat, Australian Commission for Law Enforcement Integrity

[11:36]

CHAIR: Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Griffin: Thank you, Chair; I do have an opening statement that I propose to make.

CHAIR: Thanks, Michael.

Mr Griffin: I am the Integrity Commissioner and statutory head of the Australian Commission for Law Enforcement Integrity, also known by its acronym of ACLEI. I commenced as Integrity Commissioner on 19 January this year. As a result of my short time in this role, I will be relying on my colleagues to assist me today.

In preparation for this hearing, I have familiarised myself with ACLEI’s operational practices relating to telecommunications data, and I have three main observations to make. Let me first say that I recognise the privacy concerns that attend the data retention issue. It is pleasing for me to note, as someone who has had a career-long interest in justice and integrity matters, that the data retention bill broadens the role of the Commonwealth Ombudsman to oversee the way law enforcement agencies manage telecommunications data. The Commonwealth Ombudsman’s office has an outstanding reputation within government and among the many thousands of people who access that office every year for assistance in dealing with the government. I welcome the introduction of an oversight mechanism for telecommunications data and consider that the Commonwealth Ombudsman is well suited to that role.

Secondly, I have had the benefit of being briefed on all of ACLEI’s current operations as well as a number of past investigations. In my review of these cases, the thing that has struck me the most is the lengths to which corrupt officers will go to cover their tracks. Accordingly, telecommunications data is essential to finding corrupt conduct and can be crucial to its successful prosecution. For these reasons, I am convinced of the appropriateness of the data retention measures being proposed by the Attorney-General, and I am satisfied that the claims put to you in ACLEI’s written submissions are justified.

Thirdly, I observe that ACLEI, although a very small agency, has achieved some remarkable investigation outcomes. By any measure, the disruption of a gang of corrupt officers and their criminal counterparts at Sydney International Airport is a good result. The value of drugs involved in that case was $46 million. As our written submission shows, retained data was a significant factor in being able to catch the whole of the network of the people involved in that conspiracy. I would like to thank the committee for the opportunity to appear and I would be pleased to answer any questions you may have.

CHAIR: Thank you.

Mr RUDDOCK: I have a question arising out of evidence we received earlier in the day. My question is whether your organisation has had any specific investigations into use by law enforcement officers or misuse by law enforcement officers of access to metadata?

Mr Griffin: I will refer to my director of operations for that historical fact.

Ms Marshall: We have not had any specific investigations into that issue. However, should a public official who is a member of a law enforcement agency within our jurisdiction be misusing metadata or accessing it for a corrupt purpose, it would be notifiable as a corruption issue under the Law Enforcement Integrity Commissioner Act.

Mr RUDDOCK: You are not responsible for state law enforcement.

Ms Marshall: That is correct—Commonwealth law enforcement.
Mr RUDDOCK: Do you liaise with bodies that are responsible for overseeing state law enforcement agencies?

Ms Marshall: We do. We have close relationships with our state counterparts.

Mr RUDDOCK: There were suggestions by an organisation, Electronic Frontiers, which spoke to us of misuse of metadata for stalking purposes in a police authority. I would like to know whether matters as serious as that have been the subject of any investigation. There were also suggestions that metadata was being misused by law enforcement agencies linked with bikie gangs. I would like to know whether any complaint has been made to any organisation alleging that misuse and what the result of those investigations has been.

Mr Griffin: Mr Sellers is in the best position to deal with that question.

Mr Sellars: Thank you for the question, Mr Ruddock. It is the case that from time to time those allegations are made. I understand the committee has already spoken to the AFP and may be doing so again. That might be a question you would refer to the AFP. ACLEI is aware that some instances—in fact, I think no more than one—where an allegation was made about a law enforcement officer and I think it was an AFP officer—please forgive me if it was some other agency in our jurisdiction—where that allegation was made about them. It was not in our view done for a corrupt purpose. So it was not investigated under our legislation but it was investigated by the policing agency itself.

Mr RUDDOCK: Do you think access to metadata might help in investigating allegations of misuse?

Mr Sellars: That is exactly the case, Mr Ruddock. It is used in that way. If I may say so, it does add to the safeguards available. I did hear the evidence of Electronic Frontiers Australia and there is sometimes this characterisation of a honey pot of information. If that were the case, one would expect to see more instances of inappropriate use, but that is not the experience of ACLEI.

Senator BUSHBY: Thank you, Mr Griffin, and congratulations on your new appointment, and welcome to the role. You mentioned the case of Operation Heritage-Marcia, where ACLEI got involved in a $45 million drug importation ring, and how metadata was useful for you, particularly in identifying additional participants in that criminal matter. In general, with the investigations undertaken, with what percentage of them would you use historical metadata?

Mr Griffin: My review of the material of current and recent operations suggests that almost all involve consideration of telecommunications data.

Senator BUSHBY: I used the term historical. Clearly there is a case for more intrusive access into telecommunications use when somebody is a person of interest. But in terms of piecing together your investigative work, historical metadata—just to clarify—is used in almost all if not all of your investigations?

Mr Griffin: Indeed, because we are looking in the main at people who are skilled themselves as investigators, who, almost by definition, are skilled in counterintelligence, and at the time they come to interest to us it may well be that they have already started laying the cover for their tracks. So it is the historical evidence of their involvement with others that is crucially important.

Senator BUSHBY: And, as you have indicated, it can also help identify other persons of interest. If you have one person you suspect of some activity that is corrupt, looking through their metadata records may then open up a network of other people who may well also—

Mr Griffin: Precisely. It may even be compared to building a mosaic. Each of those pieces on their own is not necessarily helpful. It is the broader picture that is created historically.

Mr DREYFUS: I have a question related to the committees’ inquiries of a lot of agencies. I saw from your submission that you had said that based on its investigative experience, ACLEI supports a data retention scheme based on mandatory two-year retention. The committee has made a number of inquiries to police and other agencies about why two years has been selected, and we are still looking for more information about what is the most common time period that is focused on. Are you able to flesh out for us what the investigative experience has been that leads you to say that a two-year period should be supported?

Mr Griffin: Thank you for that question. It is indeed a question I myself have asked. It relates to the previous answer I gave, which is that the particular area of interest to us relates to people who are presently covering their tracks, and very recently covering their tracks. It is unlikely that the connections they have made will be present contemporaneously. Therefore, it is the historical record that is important to us, and looking at our history of investigations, we are of the view that the two-year period works for us. Although, as you will see from Operation Heritage-Marcia, we have looked at historical data, where it has been available, that has gone back several years, indeed to 2006 in Operation Heritage-Marcia. But we are comfortable with the two-year period.
CHAIR: Thank you for your evidence today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.

Mr Griffin: Thank you for the opportunity to appear today.
Mr BYRNE: I am going to ask you about the destruction of data that is obtained by ASIO. I think you were saying you had just found this out. Is that correct—that this is something that has just been brought to your attention?

Dr Thom: I would not say that we have just found it out. We have been looking at this over the last few years, but I think it is really highlighted by the questions that were asked by this committee in a hearing towards the latter part of last year, and we looked into it more deeply and asked perhaps more specific questions about the retention of data. But also, because the disposal authority had been changed only in 2012, that really needed to be bedded down before we had another, more thorough, look at it.

Mr BYRNE: So, is it your understanding that data that has been collected by ASIO and is finished with is then given to the National Archives?

Dr Thom: Where it actually resides I am not sure, but there has to be an agreement between the archives and ASIO as to what gets deleted. I think it actually stays with ASIO, but there has to be an agreement.

Mr BYRNE: You have just started looking at this. For example, with the metadata that has been collected over the past number of years, is it your understanding that ASIO would still have that or has it been destroyed?
Dr Thom: There is an agreement that sets out what happens to different classes of information. For example, field inquiries, investigations, telecommunication intercepts et cetera can be retained forever. However, there is another provision that says: where they are identified not of security interest, they should be disposed of after five years. The question I am looking at at the moment is: at what stage do they decide whether they are not of security interest and when do they dispose of them? That is an ongoing project. I am afraid I do not have the answers for that today.

Mr Byrne: It is pretty interesting to the committee in light of what we are examining. For example, where information has been relevant to an investigation, you are saying that that information can be kept indefinitely?

Dr Thom: I do not think it is indefinitely. It is retained in the National Archives—yes.

Mr Byrne: So it could be. Again, coming back to the question about metadata that has been used, effectively you are starting the discovery process, but there is basically a lot of that housed in the National Archives. Is that your understanding?

Dr Thom: I do not think it is actually transferred to National Archives. I think it is kept with ASIO. My concern is not so much the material that is actively used in an investigation but the material that is lawfully collected but found later to be not of security interest or no longer of security interest.

Mr Byrne: To your knowledge at this point in time, you are not sure whether that is being destroyed?

Dr Thom: That is correct.

Mr Byrne: Also, with respect to information that is useful to the agencies—and that, obviously, is a fairly broad scope, one would imagine—that can be kept at ASIO indefinitely?

Dr Thom: That is my current understanding, but perhaps you could check that with ASIO.

Mr Byrne: We will of course check that. That could mean that you have this ever-growing database that ASIO could be cross-referencing on an ongoing basis. In a sense, they are storing metadata at ASIO. Is that a fair thing to say?

Dr Thom: The Attorney-General's guidelines say:

In performing its functions ASIO may:

(a) collect, maintain, analyse and assess information related to inquiries and investigations;

(b) collect and maintain a comprehensive body of reference material to contextualise intelligence derived from inquiries and investigations; and

(c) maintain a broad database … against which information obtained in relation to a specific inquiry … can be checked and assessed.

So it is our suggestion that perhaps, when the guidelines are reviewed, those sorts of issues could be considered in the context of the bill that is being discussed today, including the increased amount of data that might be kept.

Mr Byrne: The concern that I would have is that you would have a very large and growing amount of data kept, and particularly if it has been finished with, but it continues to grow and it is stored for some period of time. So you have meta-database that expands and there is no compulsion for it to be destroyed after its utility has been finished with with the agencies. Then you have another issue: you could have incidental data and other data with the National Archives at the same time. I commend you on the work that you have done in discovering that, but I must say that, as a committee member, it does pose a substantial concern to me. I very much look forward to hearing further from you in terms of the protocols being looked at further and discovering what information ASIO does in fact have, what it does destroy and what it keeps.

Dr Thom: We would hope to feed the results of this into the review of the Attorney-General's guidelines.

Mr Byrne: When do you think that will be completed?

Dr Thom: We are not responsible for the review, but I would hope to complete our deliberations by the middle of this year, certainly.

Mr Byrne: Thank you for that, Dr Thom.

Mr Ruddock: I note that in your submission you say that ASIO 'takes appropriate action to remove incorrectly received material from its holdings'.

Dr Thom: If it is sent incorrectly by the carrier, then it is promptly removed from its holdings. That is the warranted data. I understand that, for some categories of telecommunications data, it does not even enter into its holdings. That is a very small proportion we are talking about here. We are talking about material that should never have been sent—
Mr RUDDOCK: I understand that and I understand what you are seeking, and I think it is an appropriate issue to raise. In relation to the material received and held, do you have any evidence that that material has been compromised in the hands of ASIO?

Dr Thom: No, I have no evidence that it has been compromised in the hands of ASIO.

Mr RUDDOCK: Thank you.

Dr Thom: If I may add, though, there is a general proposition that personal information that is not required by a government agency should not be retained by a government agency. I am certainly not suggesting that it has been inappropriately used or compromised.

Mr BYRNE: My concern—sorry to cut across you, Chair—is that you have an ongoing database that can be cross-referenced historically. So, even if a person of interest does not continue to be a person of interest, that person's data is there and can be accessed; and, from what I am hearing you say, there does not seem to be a public, or more public, check and balance about what ASIO is actually doing with respect to that. That is the concern that I have from listening to the evidence that you have provided so far and from reading your submission.

Dr Thom: And that is what we are looking into at the moment.

Mr BYRNE: Okay.

CHAIR: Have you had discussions with ASIO about this?

Dr Thom: High-level discussions—but it really is getting down to the detail at the moment in terms of volumes and amounts, and what actually happens.

Mr RUDDOCK: And it goes to Archives as well. They are involved, additionally.

Mr Blight: Because most of the material is classified, under the agreement with Archives it is retained by ASIO, even though it may be archived material. I think that is one of the issues we are still looking at. But there is a different treatment of classified information in relation to Archives and where it is physically held.

Mr BYRNE: Do you have a sense of the amount of information that is being kept by ASIO?

Dr Thom: I think, even if I did, that would probably be classified information. So I am not sure. I think you should ask them.

Mr BYRNE: Thank you.

CHAIR: David?

Senator FAWCETT: My question is essentially the same as Philip's. My sense is that the indication is that ASIO have no desire to collect volumes of data for no purpose. What you have said here is that, where it has no purpose, ASIO are diligent in getting rid of it. But what they keep—I am taking from your comment—they keep for a purpose.

Dr Thom: I am not sure that that is what I said. What I was saying was that if information is collected in error, if it is sent to them in error, then it is deleted. But, in terms of turning their minds to whether data is needed in the future or not and disposing of it according to the authority or according to the legislation in terms of warranted data, I am not sure that they are applying the resources to do those deliberations.

Senator FAWCETT: Can I just take you to a slightly different issue. We have had a lot of comment around the dataset. You made the comment in your submission:

- The proposed amendments set minimum data retention requirement …

Based on your oversight of ASIO over a long period of time, I take it that this means, in your view, that what they are laying out is in fact the minimum dataset that the security agencies would need. You go on to say that there may be other data that businesses collect that they should be able to continue to access, but this is a minimum dataset.

Dr Thom: I was not actually making a comment on whether this is the minimum that the security agencies need; that is an operational matter for the security agencies. I do not think I am qualified to say. What I was saying, however, was that the legislation is addressing the minimums that the carriers must keep but it is not addressing any other information that the agencies might access, which is a different issue. The amount they must keep may not be exactly the same as what they actually keep, and the agencies can still access the extra. I am not sure if that is clear.

Senator FAWCETT: I understand that.
Mr BYRNE: Do you think, Dr Thom, that there should be a compulsion for the agency, when it is finished with the data and it is not of any use in terms of legal purposes, to destroy the data?

Dr Thom: I can understand that there would be an impost in terms of resources to assess that at a certain point in time. However, I think that needs to be balanced against what I would consider to be the general public expectation that, if matter is found to be not relevant to security or no longer relevant to security, it should be deleted. I am not sure that balance is correct at the moment.

CHAIR: When were the guidelines put in place?

Dr Thom: The Attorney-General guidelines, I think, were done in 2007, and the records authority in 2012. Prior to the 2007 Attorney-General guidelines, there was a prohibition on what was called speculative data-matching, I think, which would appear to have been a stricter requirement in the previous guidelines and was changed in 2007. That was before my time in this position, so I am not completely on top of that.

CHAIR: But the guidelines are going to be reviewed?

Dr Thom: There was a recommendation from this committee that they should be reviewed, and the government accepted that recommendation.

CHAIR: Yes. Andrew?

Mr NIKOLIC: Dr Thom, on your point about the judgements that ASIO might make on the relevance of information: if I understand some of the briefings we have got not just from ASIO but also perhaps from other agencies involved in counter-terrorism and counter-crime investigations, they are often complex investigations that might go for some years. So the contemporary relevance of information and the future relevance of that information, as you look at patterns between individuals and networks of concern, might be hard to predict. Do I take it from your comments that, despite understanding that some of the information ASIO might have will not definitely be useful in the future, they are nevertheless choosing to retain it, or is your comment simply that they retain it on the basis that they are unsure and those patterns today may develop into something more sinister in the future?

Dr Thom: There are a few questions there. I am not sure that they are choosing to retain it. I think they are not choosing to destroy it, which is a different question. With one you are asking a question and choosing to retain it; with the other you are not actually addressing the issue.

Mr NIKOLIC: Do you have a sense of why?

Dr Thom: No, I do not. I think it could be resources, but I would not want to speak for them. The other issue is that they can conduct activities quite legitimately and correctly to rule people out, and so they can completely rule somebody out of being of security interest. It is that kind of data—once they have decided that they are definitely of security interest—that I think they should turn their minds to and perhaps delete, after a period of five years as set out in the authority.

Mr NIKOLIC: But I take it equally in your response that there could be elements of that information that they hold today—that pattern of life analysis for individuals and networks—that they retain to see where investigations might take those patterns into the future. Is that a fair comment?

Dr Thom: Absolutely. There is a large amount of information that would have to be retained forever according to the guidelines, and I have no concerns about that at all.

Mr NIKOLIC: Thank you.

CHAIR: I am just going to do one last question, and it is page 3 of your submission, where you say:

… our preference would be to have early engagement with agencies in advance of commencing the telecommunications data inspections. This would allow us to pursue a proactive oversight role, where we can familiarise ourselves with agencies' procedures, identify best-practices, and confirm any areas of high risk on which to focus our inspections.

You say:

Some agencies have already expressed in-principle support to our proposal …

Dr Thom: I think that that is actually the Ombudsman's submission.

CHAIR: Sorry, I am one step ahead of myself. Sorry, that is the Commonwealth Ombudsman's submission. I will still stick on the same line of questioning: do you normally find that there is a proactive engagement with the agencies on these types of issues with your role?

Dr Thom: We consider our whole inspection regime to be proactive, in that we go and look at things. However, if there are any concerns, the agency—we are talking only about ASIO in this case—will proactively
alert us to anything that might be out of the ordinary. So I would consider our whole inspection regime to be proactive, in fact.

**CHAIR:** Thank you.

**Mr DREYFUS:** I just want to give you an opportunity, Dr Thom, to talk a bit more about this. The inspection regime that you maintain is one which focuses very intensely on warrants, they being a more intrusive form of surveillance than these telecommunications authorisations. I just want to give you the opportunity to explain, within the limits of what you can, how you go about this task.

**Dr Thom:** Up until a couple of years ago, we looked at warrants as one category of activities and maybe telecommunications and data authorisations as another. Now what we tend to do is look at an investigation holistically—I do not like that word—or as a whole. We review a sample of whole investigative cases, and in that case we would look at all the different activities that have been conducted in respect of that case. We would look at any warranted activity or authorised activity. We would look to see whether the particular power, be it a warrant or a telecommunications data authorisation or some other action, is proportionate in terms of the Attorney General's guidelines. We would look at the intelligence that existed at the time, and then we would look at the level of authorisation and delegation. So we do not nowadays separate the warrant inspections from the telecommunications data inspections. Having said, warrants give ASIO the authority to use more highly intrusive powers, so we would pay closer attention to the warranted activities.

**Mr DREYFUS:** With the inspection that you are conducting, once you have decided to look at a particular case, it is a full inspection—

**Dr Thom:** Yes.

**Mr DREYFUS:** including looking at every record and potentially interviewing officers?

**Dr Thom:** We have access to every record, but whether we look at every record or not for every case would be a matter of a case-by-case basis.

**Mr CLARE:** Just one question: the Law Council of Australia's submission makes some reference to your organisation in its submission. I am not sure if you had a chance to look at that submission.

**Dr Thom:** I read the Law Council's submission when it was on the website. I cannot recall what they said, I am afraid.

**Mr CLARE:** Perhaps then if I could draw your attention to page 29 of that submission where it recommends:

- ASIO's record keeping procedures in relation to preservation notices, stored communications and telecommunications data, should be brought into line with other enforcement agencies under proposed sections 151 and 186A of the TIA Act; and
- IGIS should be required to inspect those records annually in similar terms to proposed subsection 186B(1) of the TIA Act.

I am interested in the view of IGIS as to whether it would support such an amendment.

**Dr Thom:** Based on my experience, I do not see the need for such an amendment in that ASIO records are comprehensive anyway and we have full access to ASIO records. Although we are not required in my legislation to conduct particular inspections, we have hitherto seen ASIO powers as intrusive and always conducted those inspections. For a small office, I think we do need to have the flexibility to adjust our resources according to what we consider to be most sensitive at any particular time. Having said that, we would never ignore the use of these powers by ASIO. We would always conduct inspections. In my view, the current system is working perfectly well and I do not see the need to have more prescriptive legislation for our oversight.

**Mr CLARE:** Thank you very much.

**CHAIR:** Dr Thom and Mr Blight, thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward it to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.

**Proceedings suspended from 12:12 to 13:22**
GLENN, Mr Richard, Deputy Ombudsman, Office of the Commonwealth Ombudsman

NEAVE, Mr Colin, Commonwealth Ombudsman, Office of the Commonwealth Ombudsman

WELTON, Ms Erica, Director, Inspections and Law Enforcement, Office of the Commonwealth Ombudsman

CHAIR: Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. I invite you to make an opening statement before we proceed to questions?

Mr Neave: Thank you for the opportunity to appear here today. I thought it might be useful to highlight a few of the matters we raise in our submission. Overall, we support the proposed provisions regarding the expanded and additional oversight functions for the Commonwealth Ombudsman, under chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979, regarding the preservation and access to stored communications and access to telecommunications data. The proposed emphasis of the inspection roles and reporting requirements align with the work that we presently do in the office. The minister to whom we report—and this is a provision we support—must also table in parliament my report on the results of our inspections, thus making it publicly available.

It should be noted that if the bill is passed our current inspection function under chapter 2 of the act, regarding telecommunications interceptions, will be the only inspection function out of step with the other oversight functions that are created by chapters 3 and 4. In chapter 2, we are required to assess compliance with the destruction and record keeping provisions only. I should note that I also have the power to report to the Attorney-General under chapter 2 on any other contravention identified as a result of assessing compliance with those provisions dealing with destruction and record keeping. We also have an overall responsibility to assess the veracity of the records we must inspect. Additionally, in relation to chapter 2 there is no automatic public reporting mechanism. So, given that the bill that is proposed improves the oversight arrangements under chapter 3, I wanted to make the point that under chapter 2 the oversight function is somewhat different and may well be something that those responsible might look at when the broader reforms to the act are considered—at some time in the future, no doubt.

As I said, we are satisfied that the design of the oversight functions proposed by the bill are sufficient for my office to provide the expected level of assurance that agencies are meeting their obligations in complying with powers under chapters 3 and 4 of the act. We have appreciated the work we have done with the Attorney-General's Department, which has consulted with us extensively. As noted in the submission, we have the necessary expertise and experience to perform the functions, but at the moment we do not have the resources to do so.

Over the past 10 years the Ombudsman's presence in the area of overseeing agencies' use of covert, coercive and intrusive powers has grown significantly. We no longer just investigate matters of administration on complaint or on our own motion of action taken by the majority of Australian government agencies. The role of providing public assurance that agencies are using their intrusive powers as parliament intended is a key function of the Commonwealth Ombudsman. This oversight is extremely important, for, unlike the matters about which my office receives complaints, the public would not—and in most cases should not—have knowledge of agencies undertaking these covert and intrusive activities.

Under nine different regimes authorising these types of powers, during a financial year my office currently oversees approximately 20 Commonwealth, state and territory enforcement agencies; conducts 60 inspections and reviews; generates approximately 100 reports on the result of these inspections; and regularly reports to parliament on the results of our oversight activities. However, I am concerned that this bill is proposing expanded and new oversight functions in an environment where my office continues to have oversight functions without any additional resources. Just lately, we were empowered with an oversight role in relation to preservation notices under chapter 3 of the Telecommunications (Interception and Access) Act 1979 and the delayed notification search warrants under Part IAAA of the Crimes Act 1914, as well as the role of Norfolk Island ombudsmen. All the additional important functions were prescribed without any funding to my office.

The oversight function being proposed under chapter 4 will significantly increase our inspection workload. If my office continues to be the prescribed statutory oversight function authority without funding, this will reduce the level of assurance that we can provide in overseeing covert and intrusive powers. Furthermore, this pressure reduces my office's ability to provide effective oversight of other extraordinary powers of law enforcement where
we do not have a statutory inspections role. That said, we appreciate the work we are doing with the Attorney-
General's Department to work out what additional resources are required to take on the additional responsibilities
created by this bill.

On the other hand, and on a much more pleasant note, if my office is appropriately resourced it will be well
placed to effectively perform the proposed roles under chapters 3 and 4 of the act. I should also say in relation to
resources that our strong preference is for the Ombudsman's office to be directly funded for the oversight role. If
the bill is passed, there should be a budget mechanism for my office to receive departmental appropriations
directly and not through other departments.

As noted in my submission, our proposed approach to overseeing chapter 4 would be proactive engagement
and oversight. Prior to the commencement of inspections, we would meet with agencies in order to familiarise
ourselves with their processes, procedures and systems. This, in turn, will inform our risk assessments, the focus
of our inspections and tests. Our office would also be in a position not only to confirm that agencies have kept
particular records in accordance with their legislative obligations but to understand what processes occurred to
result in that particular record being created. As well as improving the level of assurance that my office can
provide, these activities enable my office to also identify any agency practices that may lead to non-compliance—
in other words, anticipate problems which could arise.

Some agencies have already expressed their in-principle support to this approach, and I would like to
acknowledge their positive attitude towards our independent oversight performed in relation to other functions. It
is not uncommon for agencies to come to us not as part of the inspection process but separately in order to discuss
issues which might arise for them. As a result, at subsequent inspections the effectiveness of this engagement and
agencies' efforts become quite evident.

Lastly, I would like to highlight that the proposed oversight functions for the Commonwealth Ombudsman are
in relation to agencies' actions, not carriers. Occasionally it is misunderstood that my office has oversight of
 carriers' actions. It does not. I note the respective roles of the Privacy Commissioner and the Australian
Communications and Media Authority in that regard. Under chapter 4 the proposed scope of the Ombudsman's
oversight role does not include assessing the effectiveness of or adherence to the proposed mandatory
telecommunications data regime by carriers. My office would only be required to assess agencies' compliance
with their statutory obligations in accessing telecommunications data subject to appropriate funding—I am sorry
to highlight that point once again! My office is well placed to perform this role. Thank you.

CHAIR: Thank you, Philip.

Mr RUDDOCK: I have one question. Given you are not monitoring the security agency but some
investigations in relation to counterterrorism measures are very sensitive, I note that before you report you have to
have your report vetted by the relevant agency. Is that the way in which you would ensure that investigations
might not be compromised by matters on which you have to report?

Mr Neave: I think a regime of consultation—and appropriate consultation in such a way as not to prejudice
the efficacy of whatever the investigation might be—would be the way in which we would tackle that, but my
colleagues may have some other comment to make on that point. But our general approach in this jurisdiction, as
in all jurisdictions, is to consult appropriately and sensitively and ensure that whatever came to our attention only
came to the attention of the appropriate authority so as not to so prejudice any inquiries.

Mr Glenn: Certainly that is typically the way we work under our existing roles. We work very hard to make
sure the information we are putting in our reports is about compliance with the legislation and does not reveal the
subject matter of the investigations to which the powers relate. The key mechanism is being able to talk to the
agency concerned about the sorts of matters they are putting in the report to make sure they are not saying
something we do not, which would lead to the inappropriate disclosure of information about the investigation.

Mr CLARE: I take you to the concerns you raised about being properly resourced. You indicated that the
Ombudsman's office is in conversation with the Attorney-General's Department about proper resourcing at the
moment. Would you care to elaborate on those discussions and whether you are confident that additional
resources will be provided?

Mr Neave: I think one always starts off with the feeling that one should be confident about such matters. We
have provided initial costings to Attorney-General's Department, which in principle seen the value of our
contribution in that regard. The costings are based on our current oversight functions. Given that we have had 10
years experience in this space, we do have a pretty good idea how many people you need to perform various
tasks.
So we are looking at issues around the number of staff, training of staff, getting security clearances for them, the number of inspection days which one might expect to have staff involved, the associated travel costs, the reporting obligations—that proactive role that I referred to in the introductory remarks is important because we want to have the right working relationship with the people we oversee, not in such a way as to prejudice our role, but that does involve quite a deal of communication and discussion—other associated administrative costs and also developing technical systems. The costings are based on us applying a sampling methodology; we do not intend to inspect every record relating to a request to access data. Broadly, the discussion so far has been very encouraging and we are looking at what we need to do the job from what I think are the appropriate angles in order to make sure that we can provide that public assurance that I also referred to during my opening remarks.

Mr CLARE: How many additional staff do you think you would need to do this work?

Mr Neave: We are not totally focused on the actual number of staff, because I think we are going to need to supplement some of the skills in our office. We are looking at a total estimate of around $2.3 million in the first year and $1.65 million thereafter, but the actual staff mix, I think, will depend, once we look at what is involved, the sorts of people we will need and what sort of levels those people should be at. So concentrating on actual numbers I do not think is the way; rather, we would look at overall cost and then work out exactly what we want—particularly, just to emphasise the point, we do need people with the right skills and experience. It is not that we do not have them already, but we need more of them.

Mr CLARE: But, in putting those estimates together, have you made some assumptions around including the cost of employing additional people?

Mr Neave: Yes, that includes the additional people.

Mr CLARE: How many additional people?

Mr Neave: As I say, we have looked at an overall labour cost within that figure of $2.3 million in the first year and $1.65 million thereafter, but exactly how many we are not absolutely sure.

Mr CLARE: I appreciate that, because you are still engaged in that discussion with the department, but I was really trying to get a ballpark figure just to get a feel. In your submission you make the point that it will significantly increase workload, and so I am trying to understand the additional size of the team required to do the work.

Mr Neave: I think we could say around a dozen extra people.

Mr CLARE: Thank you very much.

Mr DREYFUS: I want to ask you about the oversight and, in particular, to be direct, I want to ask you about the proposal of the Privacy Commissioner, who is also here with us, that the oversight function might better be conferred on his office. Have you had a chance to read the Privacy Commissioner's submission?

Mr Neave: In the office, we have read the submission, yes.

Mr DREYFUS: And the bill in its present form does not provide oversight of how, if at all, service providers might be complying with the law or, in particular, their obligations under the Privacy Act.

Mr Neave: Yes, that is right.

Mr DREYFUS: Is it any part of your role to look at compliance with the Privacy Act?

Mr Neave: I think it is not specifically referred to in the bill, but I am sure that, if we came across something in the inspection process which suggested that there might be an issue in relation to privacy, that is not something that we would allow to go unremarked upon.

Mr DREYFUS: I did not mean to suggest that. It was probably a poorly phrased question. You have a role as an overarching Commonwealth integrity agency to ensure compliance with the whole of the law.

Mr Neave: We are certainly interested in complying with the law.

Mr DREYFUS: Can I ask you an open-ended question and I am not inviting some dreadful demarcation dispute! Do you have a view on whether you or the Privacy Commissioner is the more appropriate person—and I appreciate this is a matter for government and for the parliament—and whether, if your agency continues to be a part of the oversight arrangements, there might be an additional role for the Privacy Commissioner?
Mr Neave: I think the general statement which we would make in the Ombudsman's office is that we are happy to work as part of the integrity framework as a whole. There are a lot of agencies that we work with in a way which leads to, first of all, greater assurance for compliance with legislation for the community. I would see this as being no different from the general approach that we take to performing our role. Accordingly, we already have a very sound working relationship with the Office of the Privacy Commissioner and I see no reason for that not to continue. I agree with your statement, which is that it is up to the government and parliament itself to decide whether that should be referred to in legislation because that is really a matter of policy.

Mr DREYFUS: Thank you.

Mr RUDDOCK: The Privacy Commissioner does not appear to want any extra money. Are you prepared to bid for it?

Mr Neave: If I might say so, that is a matter you should ask the Privacy Commissioner.

Mr RUDDOCK: I intend to.

CHAIR: I have one final question. In part 4, on page 3 of your submission, you state:

… our preference would be to have early engagement with agencies in advance of commencing the telecommunications data inspections. This would allow us to pursue a proactive oversight role, where we can familiarise ourselves with agencies' procedures, identify best-practices, and confirm any areas of high-risk on which to focus our inspections.

You then say, 'Some agencies have already expressed in principle support to our proposal.' Could you just explain in a little bit more detail not only for the committee but for the broader audience, who are obviously paying attention to this hearing, what you have in mind there and how it would work?

Mr Neave: Our general approach in the Ombudsman's office is to work appropriately with agencies who are subject to our jurisdiction, whether that be in our complaint-handling function or in this oversight function. That means meeting with representatives of agencies—and if this bill is passed, we would anticipate doing that—to get a good idea of what the agency propose to do in order to comply with the content of the act, on the assumption that it becomes an act. We would also then in those sorts of discussions be able to use the experience, which we already have, when we are performing similar roles, which we have been doing for the last 10 years or so. We may be able to make a suggestion to the agency about how they might structure their processes and procedures in order to assist them to comply with the content of the act. We see that as a way of avoiding problems and also setting up a good line of communication so that even when an agency is not being inspected by us then that agency might make contact with us and ask us for assistance in developing processes and procedures in order to comply with the act. It is what I would call an appropriate engagement with agencies to make sure that the intention of parliament expressed in the act is carried out and that we are able to conduct ourselves in a way which, as far as the agency is concerned, is useful to the community and in turn useful to the parliament.

CHAIR: Are there any further questions? No? Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you. Thank you very much for your time today.
FALK, Ms Angelene, Assistant Commissioner, Regulation and Strategy Branch, Office of the Australian Information Commissioner

PILGRIM, Mr Timothy, Australian Privacy Commissioner, Office of the Australian Information Commissioner

[13:46]

CHAIR: Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Pilgrim: Yes I do, thank you. Firstly, thank you for the opportunity to appear before the committee today. The Privacy Act contains a number of objectives, the first of which is to promote the protection of the privacy of individuals. This sits alongside other objectives, one of which is to recognise that the privacy of individuals must be balanced with the interests of entities in carrying out their legitimate functions and activities. This is consistent with international law, which recognises that the right to privacy is not absolute and requires an assessment to be made of whether the measures that may limit privacy are both necessary and proportionate to achieve that objective. Applying this in the context of the introduction of a data retention scheme, privacy interests must be balanced with the need to ensure that law enforcement and security agencies have access to the information necessary to perform their functions.

The bill would require the collection and retention of a very large volume of personal information. In doing so, it would remove the discretion that would otherwise be afforded to service providers to determine whether to collect and retain certain types of personal information.

The Australian Privacy Principles state that entities should only collect personal information that is reasonably necessary for their functions or activities. They further state that entities should only retain information for as long as necessary to carry out their functions and activities. Therefore, where the collection of telecommunications data is not necessary for a service provider's business purposes, and the retention of the data is for longer than otherwise needed, a mandatory data retention scheme has the potential to significantly impact individuals' privacy. It creates a risk that the data may be misused, such as through inappropriate access or the risk of identity theft and fraud as a result of data breaches. To minimise any impact, I would suggest that the committee should satisfy itself, firstly, that each item of the dataset that service providers would be required to collect and retain under the scheme is necessary and proportionate; and, secondly, that the retention period imposed in relation to each item of the dataset is also necessary and proportionate.

Turning to the proposal that a two-year data retention scheme be introduced, I make these comments. On the face of the publicly available information and evidence, including evidence provided to this committee by law enforcement and security agencies, there would appear to be a case as to why it is necessary to require service providers to retain certain telecommunications data for a period of time. The challenge is determining what is the appropriate time period for retention that balances the privacy interests of individuals with the needs of law enforcement and security agencies.

Statistical evidence, both international and domestic, seems to suggest that a large proportion of investigations use telecommunications data that is up to or less than one-year old. Acknowledging that there are differing views on what this evidence shows, it could nevertheless support a case for a shorter one-year data retention period. However, the case for a two-year data retention scheme is less clear. It may rest on information that is being made available to the committee but which is not being released publicly—I assume there to ensure that it does not prejudice the activities of law enforcement and security agencies. It is therefore important that close consideration be given to whether the evidence provided to the committee establishes that it is necessary to retain each item of telecommunications data for a minimum period of two years or, alternatively, whether a shorter retention period would meet the needs of law enforcement and security agencies.

However, I want to emphasise that any data retention scheme must be accompanied by privacy safeguards. I recommend that further enhancements be made to the safeguards currently in the bill. To that end, I recommend that the bill should ensure that all service providers who are required to collect and retain telecommunications data under any data retention scheme are subject to the Privacy Act. This is currently not the case. The bill should limit the purpose for which an authorisation to disclose information can be made to the investigation of serious offences and threats to national security. I will return to this point in a moment.
The bill should be amended to give the Australian Privacy Commissioner oversight of enforcement agencies' compliance with chapter 4 of the Telecommunications (Interception and Access) Act. This would complement the commissioner's existing oversight role of telecommunications data. The bill should include an obligation for service providers to notify the Australian Privacy Commissioner and any affected individuals if they experience a data breach that involves retained telecommunications data. The bill should be amended to include a sunset provision that the scheme expire five years after the end of the implementation period, unless reauthorised by the parliament.

I want to turn now to the issue of warrants. The types of data that service providers will be required to collect and retain under the proposed data retention scheme has the potential to build a detailed picture of a person's activities, relationships and behaviours. However, I am also mindful that the scheme does not require the retention of the content of communications—and this is an important consideration. The committee will have heard evidence about the impact of a requirement for a warrant to be obtained on an investigation-by-investigation basis. The issue is whether such a warrant scheme would achieve the right balance between the protection of privacy and the need to enable law enforcement and security agencies to efficiently and effectively investigate serious crime and national security issues.

In my submission, I did not advocate for the imposition of warrants. I took this position on the proviso that the bill be amended to limit the purposes for which telecommunications data can be used and disclosed to the investigation of serious crime and threats to national security. However, since lodging that submission, I note that the Attorney-General's Department has suggested that to meet Australia's obligations under the Council of Europe's cybercrime convention access to telecommunications data cannot be limited in this way. If that is the case then I consider that further thought needs to be given to what additional safeguards might be put in place when access is for the purpose of the investigation of minor offences.

As a final comment, I would like to address the issue of the regulations. The bill allows for regulations to be made that significantly affect the scope of the data retention scheme. In particular, the bill allows for regulations to be made relating to the services covered by the data retention scheme and the kinds of telecommunications data that service providers will be required to collect and retain. To ensure the greatest level of certainty, transparency and accountability possible, my preference would be for these matters to be included in the bill itself. However, I do note that in a period of rapidly changing technology this may not be achievable. In the event, then, that a decision is made to continue with the current model, with these matters being addressed in regulations, I consider that the bill should be amended to include a requirement for the undertaking of a privacy impact assessment, before any changes are made or new regulations are made, and that the Australian Privacy Commissioner be consulted in the making of any new regulations or changes to the existing regulations. This is particularly important where regulations authorise the handling of personal information in a way that is otherwise inconsistent with the standards set out by the Privacy Act.

**Mr RUDDOCK:** Congratulations on your award.

**Mr Pilgrim:** Thank you very much.

**Mr RUDDOCK:** I was pleased to see that. I will start by saying that I was interested in paragraph 4, the Office of the United Nations High Commissioner for Human Rights, because you rely on proportionality in relation to your observations about privacy, and I must say that I have always had some difficulty in understanding what 'proportionate' means. I was interested that the high commissioner suggests that where the right to life is involved—and that is terrorism—there must be a 'some chance' test. Would you accept that?

**Mr Pilgrim:** I would accept that, in considering the right to life issue, clearly the right to life is an extraordinarily important right, and where there is a clear threat to an individual's life then in those circumstances—

**Mr RUDDOCK:** A clear threat—not 'some chance'?

**Mr Pilgrim:** In my view where there is clear evidence that there is likely to be a threat to a person's life then certainly the privacy issue should take a step back, for want of a better description.

**Mr RUDDOCK:** The difficulty I have about warrants and people arguing about other procedures is that it seems to me that it ignores the fact that metadata is sought on the basis that you recognise that there is a potential threat but you do not necessarily know who is involved. So what you are seeking to do is to put together patterns of usage that will give you an idea about where you may in fact make your further inquiries. I can understand that with warrants, which require an enormous amount of work—and I have looked at a large number of warrants over time and I know the sort of evidence that is necessary—and I could not imagine that if you had to get access to metadata and present that level of evidence that you would ever get to first base in relation to terrorism inquiries.
That is my concern. And I must say that I am going to put great weight on the human rights commissioner's test that it be 'some chance'. I certainly would not accept that it has to be clear evidence. I just say that.

Mr Pilgrim: Certainly. And I did not want to misuse the word 'clear' in that particular circumstance. And, yes, I do agree with the Commissioner for Human Rights.

Mr RUDDOCK: Who is not subject to the Privacy Act?

Mr Pilgrim: Regarding the reference I was making in my opening statement to service providers who may not be covered by the Privacy Act, within the Privacy Act itself—and you may recall this, Mr Ruddock—there is an exemption for small businesses—that is, businesses with an annual turnover of $3 million or less. As I understand it—and I expand on this in the submission—from information I have received from the Telecommunications Industry Ombudsman it can be assumed that there are likely to be quite a large number of small ISPs for example who may fall under the $3 million threshold and will still be collecting—

Mr RUDDOCK: You are suggesting that they should be included?

Mr Pilgrim: I have put forward two options of how that may work. Basically, yes, I believe there should be some level of regulation for them. The two options could be that they could be brought into the coverage of the act, and there are already a couple of mechanisms by which that could happen—for example, for them to be brought in by regulation. Otherwise, the other suggestion I make is that there could be a provision put into the bill that allows for the making of binding rules by me that would apply to those service providers. So there are a couple of suggestions I make in the submission.

Mr RUDDOCK: Were you bidding to carry out this work without budget supplementation.

Mr Pilgrim: I would like to say, yes, but I have to fess up and say no! I have had some discussions with the Attorney-General's Department about the possible implications of some of the additional functions in the bill.

Mr DREYFUS: I want to follow on from Mr Ruddock's questions about proportionality. Starting with the proposition that the collection of data is an interference with privacy—that proposition is beyond argument; it is the basis of your entire legislative framework—how is proportionality to be approached?

Mr Pilgrim: I think what we are seeing through this very process is part of that approach—how it is to be assessed. Without wanting to sound arrogant in any way, it is going to be the responsibility of the committee to weigh up the evidence—some of which many of us will not be privy to, particularly evidence that is given in camera—to form a view about whether the intrusion or the interference in a vast number of the Australian community's personal information is going to be balanced against the need for increased security through the investigative work that is being done by the law enforcement agencies and the security agencies. This is a balance—for want of a better description—that occurs quite frequently in the law enforcement agencies' work, as you would be aware, about the need to intrude on people's privacy for some greater social good, in particular a safe society.

Mr DREYFUS: Can I offer you a couple of the calculations that might be made. Let us say the great bulk of authorisations of requests for telecommunications data up until now have been for data that is less than six months old. To take the ASIO example, which I think you offered in your submission, 90 per cent of ASIO's requests fall in the category of under one year old. The committee, and the public of Australia, are provided with one example—for argument's sake, an egregious crime, a dreadful example, where telecommunications data has been of assistance in finding the perpetrator, solving the crime and getting a conviction. Does that one instance in this illustration that I am offering you constitute sufficient evidence or is it sufficient to say that it is proportionate to say we could go to two years?

Mr Pilgrim: There are a number of steps I would take there. If it was relying on just one piece of evidence about one case, it is questionable. What I have been hearing through the evidence provided publicly is that there are more than that many cases. We should not just limit it to the number of cases because, as we start looking at some of these matters—I am feeling a bit odd here because it seems like I am starting to defend the position of the law enforcement and security agencies—it is about how large an impact they could have on the community. A particular investigation could be one that prevents an attack which could impact on hundreds or thousands of people. So I think we need to look at the evidence, some of which we have heard throughout the committee process. And from what I am seeing, from what I have taken on board, there is, as I said in my opening statement, evidence to suggest that there is a case for some data retention scheme. The question we need to weigh up—which is what you are getting at—is: what is the length of that scheme? In my opening statement I suggested that there appears to be evidence that has been put forward that suggests that that information has been useful in those particular investigations. But it seems to be—as you have reminded me through our submission—that the
majority of those pieces of information have been under 12 months old and in many cases under six months old. So the question is: what length of time should the data retention scheme be, if in fact there is a need for one?

Mr DREYFUS: What I am trying to get to is: how does the proportionality decision get made? I will give you a more extreme example. It is always going to be possible to find examples of crimes being solved by reference to very old data in some cases. Cold cases, almost, can be solved potentially by looking at five- or 10-year-old telecommunications data. And there is still in existence in Australia five- and even 10-year-old telecommunications data—not much of it, but some. Would the fact that it is possible for some agencies to provide this committee with examples of crimes that have been solved using much older data than even two years provide sufficient justification for a longer period than two years, as some of my colleagues on the committee have suggested in earlier questioning?

Mr Pilgrim: Again, I think we need to weigh up a number of issues. As we go and look at a scheme that is possibly going to require a longer retention period, we have to look at what risks that may incur to that information. If we are looking at information that is being held on the vast majority of the population we need to look at what the risk is to the population in terms of that information being misused or inappropriately accessed and then look at the potential of what cases may be able to be resolved as a result of that. I have been trying not to get down to a hard, clinical comparison between the numbers that may be resolved as a result of holding data on tens of millions of people. It becomes a fairly clinical exercise.

Mr DREYFUS: It is an inherently difficult value judgement to make, isn’t it, because you are comparing values which are in themselves of a quite different nature and therefore hard to compare—on the one hand, privacy values and values of liberty as against the need to protect life and to investigate serious crime?

Mr Pilgrim: It is. It is a very hard call to make and it is one that is dealt with in the privacy sphere on a number of different levels over a number of different sectors and jurisdictions—which is why we keep coming back to the point that, if a decision is made to implement a scheme such as this which is going to require, as I said, the holding or the collection and retaining of huge volumes of data and personal information about people for a long period of time, we need to look at what else we can put in place to do our best to secure that information. So we may need to make a call. The committee and the parliament ultimately would need to make a call on this bill. I see my role as part of this debate as saying that, if that call is made, what can we do to make sure that we strengthen the protections for that information wherever it is held. And I go into that in some areas in terms of security, data breach notification and the like.

Mr DREYFUS: On that last point, the mandatory data breach notification is something that you have gone to at page 19 of your submission. You would be aware that this requirement for a mandatory data breach notification was something recommended by this committee in May 2013 when considering mandatory data retention.

Mr Pilgrim: Yes, I recall that.

Mr DREYFUS: And you would also probably be aware what a bill, known as the Privacy Alerts Bill, lapsed on the proroguing of parliament in 2013.

Mr Pilgrim: I remember that well.

Mr DREYFUS: Would that legislation of that nature of general application—and in fact fulfils a recommendation of the Australian Law Reform Commission—satisfy the need for a mandatory data breach notification scheme?

Mr Pilgrim: As I recall the bill, the short answer to that question would be that, yes, it probably would. What I am recommending here is a mandatory data breach notification program. I am particularly putting it in the context of this bill because, as I said, this bill will require the collection and retention of quite a huge amount of personal information on individuals that would not necessarily otherwise need to be kept by those organisations for a long period of time and therefore it does increase certain risks. So just dealing with that issue in isolation to this bill, because of the huge amount of information that is going to be required should the bill pass, I think a mandatory data breach notification requirement will add an extra layer of protection for individuals should something occur to present them with some particular harm.

Mr DREYFUS: Just to flesh that out: if there cannot be a scheme of general application of a mandatory data breach notification scheme, in general, your recommendation is that at the very least there ought to be a mandatory data breach notification scheme for data retained by telecommunications providers under this legislation?

Mr Pilgrim: Yes. As I say in my submission, I think that a mandatory data breach notification scheme is warranted given the amount and volume of information that would be required to be collected and retained under this bill.
Mr DREYFUS: If this committee were to accept that suggestion—and it would indeed be acting on its own previous recommendation if it were to do so—your suggestion is that the notification requirement would be to notify your office and any affected individuals? We do not really have time—

CHAIR: No, we have time. I for one would be very interested if we could just get a sense of how this would actually work or what you are proposing.

Mr DREYFUS: There is a particular vexed question about notification of affected individuals, about whether or not it should be instant or whether there should be some discretion given to take a bit of time as to how to notify them. As you are aware, but perhaps others here are not, there have been some vast data breaches—that is probably a fair description—in the United States, even larger data breaches than here. I have in mind 70 million customer details from Target or, more recently, the 54 million customer details from Home Depot. We have had some pretty big ones here involving Sensis and the ABC—I do not mean to single them out but mention them by way of cross-reference— involving tens of thousands of customer details. Would the scheme in broad outline at least, and particularly the notification process that is set out in the privacy alerts bill, be what you have in mind for a requirement for service providers to notify any affected individuals?

Mr Pilgrim: There are probably several points I would make in terms of a notification scheme. I could refer the committee to a set of voluntary guidelines that our office has issued which have been in place for a number of years now. They were written and designed to assist both government agencies and private sector organisations covered by the Privacy Act to deal with data breaches and to decide what steps they should take. It sets out a four-stage process. I will not go through each of those processes, but clearly an important consideration is when and if notification should occur. What we have done in those guidelines is use the concept of 'serious harm' as being a step in which to start the consideration. Is there likely to be serious harm to an individual through the data being breached or being released inadvertently? This in itself is a difficult concept to get around—what would constitute serious harm?

So the starting point for an organisation to consider is: is there likely to be serious harm? An example could be that, if an organisation holds people's credit card details, those details are breached and are released, say, online. In those circumstances, we would suggest there is very strong likelihood of serious harm because, having got a hold of those credit card details, there could be, as I have suggested, identity fraud, theft or even accessing of accounts.

In those sorts of circumstances—and I am trying to generalise here because I never know what matter may end up before me—we think that that would constitute a strong argument for notifying those individuals so they could take immediate steps. In that circumstance, as soon as the organisation is aware that, say, the credit card details have been compromised, you would hope that there would be very quick steps taken to advise individuals so they can take remedial action with their banks, such as stopping the accounts, stopping the credit card or the like. So there are strong reasons there for notifying immediately.

But there will be other cases where you may not want to notify. If I could use one example without going into too much detail because of the nature of it, some years ago while I was in the office we had occasion to work with a law enforcement agency who itself had suffered an unfortunate data breach. They lost a database they held on an international investigation they were doing which included quite a substantial number of individuals' personal information, including their credit card details. It was not able to be found and the agency approached me to discuss what steps should be taken. In those circumstances, we weighed up the notification of those individuals against the issue of a very serious investigation that was being undertaken and what potential risk there would be to that investigation if people outside of the investigation team became aware that it was occurring.

So the steps we took there were to work with the law enforcement agencies and, through them, the financial institutions to find a way in which other steps could be put in place behind the scenes to monitor what may be going on with any of those live accounts to make sure that individuals were protected. Again, going back to your other question about proportionality, we had to weigh up the risks of a serious investigation being compromised and the potential for some individuals to perhaps have some of their financial accounts impacted on. It was not my final decision because we were not the agency responsible, but in giving the agency advice we came down on the steps where we were able to put other protections in place and allow the monitoring of those people's accounts to occur in case there were any illegal activities against them.

I am going through this long explanation because we work through these issues under the guidelines we have that are applicable to government agencies and the private sector—that is, our voluntary data breach notification guidelines. I think that would form a good model for any particular scheme, should one be agreed to through, say, an amendment to the bill to introduce a mandatory requirement.
Mr DREYFUS: Thanks, Mr Pilgrim. I was just checking and perhaps making sure we have on the record that there is a great deal of work being done already on what a mandatory data breach notification scheme might look like. There is not only your guidelines but a bill that this parliament has previously had before it—indeed, it passed the House of Representatives in June 2013—that we could refer to in thinking about what would be an appropriate mandatory data breach notification requirement to be inserted in the bill.

Mr RUDDOCK: I had a constituent come to me fairly recently with a letter from the Commissioner of Taxation saying, 'Somebody has accessed our database. You do not have to do anything about it; we just thought we should tell you.' I wondered what the value was in that and what the cost was. The Commissioner of Taxation was not telling the constituent anything about the nature of the database breach, just that there had been a breach.

Mr Pilgrim: That goes to a very important point. One of the things that is a risk is notification fatigue. In introducing any scheme, we would want to make sure we avoided that. That is why we are looking at a concept of serious harm happening to an individual, because there can be inadvertent breaches within large organisations. I could use the example of some of the public reports that have come out of some of the larger government agencies where they quite appropriately and for good transparency reasons in their annual reports will say that they investigated a certain number of cases of inappropriate access to their databases. These could be as simple as someone, say, typing in an incorrect client number. A person in the office could type in an incorrect claim number and the wrong name would come up. Quite appropriately, that officer would then say, 'That is the wrong person,' and get out of that person's information. But the system still may show that they have accessed it. That is a case where nothing has been done with the person's file and I would say it is a very minor issue, and I would certainly not expect the individual to be notified in that sort of scenario.

Mr DREYFUS: I would like to move to another matter, Mr Pilgrim, and that is that you have heard me put to Mr Neave your suggestion that the Privacy Commissioner, your agency, is a more appropriate oversight agency. Again, I am not seeking to encourage a demarcation dispute here, but Mr Neave's function already includes oversight of the enforcement agencies. That is the Ombudsman's role. It has been for many years. Your role already includes oversight of privacy compliance by, I would suggest, the overwhelming majority of the service providers. There might be a few mum-and-dad operations that you do not have oversight of, but all of the others are already captured by the Privacy Act. Mr Neave has helpfully identified for us that in the bill in its present form there is no oversight role conferred on him in relation to service providers. It is purely an expansion of the existing role that the Ombudsman would have in relation to enforcement agencies. I wonder if you could speak to that. We have your written submission, but I would like you, to assist committee members, to speak to the proposition that you have expressed at paragraphs 125 to 127—which is our page 113—that the privacy commissioner, your agency, is an appropriate oversight agency for the purposes of this large additional requirement that has been placed on telecommunications providers to keep, as you have described it, vast amounts of data.

Mr Pilgrim: Certainly, and I think that from my long understanding of the Ombudsman's role over many years of working with them they do an extraordinarily good job in terms of their current responsibilities under the telecommunications interception act. And I have no doubt that, should this bill in its current form go up, they would be able to undertake as high-quality a role.

Mr DREYFUS: Yes, and I would not want you to take as an implication from my question—

Mr Pilgrim: No, I was not.

Mr DREYFUS: I am exploring this. It is not any criticism of Mr Neave or of the Ombudsman's role or of his office or his excellent staff. There is just a question here for this committee and for the parliament as to how to make sure. And we all seem to agree that we need additional oversight. It is how that oversight is best delivered. That is what I am exploring.

Mr Pilgrim: And I certainly did not take your comments as being criticism of the Commonwealth Ombudsman. It was more of a comment to show that we all got on very well and recognise the good work that we each do.

In terms of this, though, what I was looking at was probably trying to move away from what have been the traditional roles, if you like, of various integrity agencies within the Commonwealth and, more importantly, look at an issue that we are dealing with here in a broader sense, which is the impact of what new technologies can do by way of collecting information. And the whole concept of personal information and the flows of it is extraordinarily dynamic, and it is not constrained by boundaries; it is not constrained, as you would appreciate, by domestic or country boundaries, by jurisdictional boundaries. And certainly now, when we are looking at the flows of information even within Australia, it is not constrained by, as we are dealing with here, issues such as
what a Commonwealth government agency might hold and a private sector agency may hold. The data flows quite smoothly and quite regularly between entities. And the changes to the Privacy Act that came into force early last year reflect that. We moved away from having one set of privacy principles to regulate Commonwealth government agencies, including the enforcement agencies, and a separate set of principles for the private sector. That was a regulatory burden, because it recognised that the flow of information moved between those entities much more than it had, say, 20 years ago—or more than 20 years ago, when the Privacy Act was written.

So, in putting forward this proposal, if we are going to have an oversight mechanism, the proposal basically is saying, 'Well, let's look at this in terms of how the information flows' and 'How can we make sure that there is an oversight agency that can follow and track that flow of information through holistically?' So, we start off with the point that the service providers, should this bill go through parliament and pass, will be required to collect certain types of data and retain them for certain periods of time. I already have jurisdictional oversight for those large telecommunications providers who will be holding the largest amount of that information. I have a raft of powers there that I can use to check on what is happening with that information. For example, as you would be aware, I can undertake complaint investigations if an individual believes something has been mishandled. I can commence investigations on my own initiative without a complaint to see if I believe that there is an activity going on that might be in breach of the act. I can also do what is now called performance assessments; we used to use the term 'audits'. So, I can go in and randomly audit those service providers to see how they are holding that data. And to support that I also have a raft of powers for remedial action. I can use more. I try to conciliate matters, complaints. Or I can use a formal determination power to require an organisation to remedy an individual complaint and now also remedy a large systemic breach. And in the case of very serious matters I now have the ability to go to the courts to seek civil penalties.

So, there is a raft of powers there for me to be able to do that bit of work to oversight that information. And in doing that it looks at the whole issue of the collection of the information and also how long those organisations are retaining it, and make judgements on that. Under other various parts of this process—for example, under the Telecommunications Act, section 309—I have the ability to go into those service providers and check their records to see whether they receive an appropriate authorisation from a law enforcement agency to access the data we are talking about here. So I already have that power to check on the service providers.

Where I am going with this story is that, if we wanted to follow it holistically, I think it would also be a benefit for me to have the authority to check that the law enforcement agencies are actually undertaking the appropriate consideration when they first seek to issue an authorisation to get that information. Then I could follow that process of requesting that information into the organisation that is collecting it, through to how it is holding it, through to how it may be disclosing it back to the law enforcement agencies; and, ultimately, whether that organisation has disposed of that information after the set period it is required to keep it. So it is looking more at the totality of the information flows, if I can put it that way, and giving one view of whether it is being handled in accordance with each of the different procedures and requirements. I hope that was not too longwinded a response.

Mr DREYFUS: No, no—that was helpful. You do not have oversight of ASIO?

Mr Pilgrim: No. The Privacy Act has always excluded the intelligence agencies.

Mr DREYFUS: Yes—and that is the same proposition for the Ombudsman.

Mr Pilgrim: That is correct. You have already spoken to the—

Mr DREYFUS: There is a fence around the intelligence agencies.

Mr Pilgrim: That is right. You have already spoken to the IGIS today, I believe.

Mr DREYFUS: Yes. I am really just making that clear for all concerned. Going to another matter, a matter that was raised with us this morning by the Australian Information Industry Association, the trade grouping for the large—I am trying to think of the right generic term—

Mr Pilgrim: I am familiar with them.

Mr DREYFUS: telecommunications companies. I will call them that. They raised a concern, and they are going to come back to us, about the reach of this bill in terms of whom the retention requirement is being imposed on. That is something that you have touched on at some length on page 16 of your submission and in your recommendation 5, which is on page 6—our pages 85 and 95. Again, I ask you to speak to what the problem is with the range of services it is intended be captured by proposed new section 187A. We got some clarity from the Australian Information Industry Association this morning, in particular saying that it was not clear that 'cloud' services, VoIP, would be captured by the act or whether it was even intended that they be captured. What do you see as the problem that needs clarification here, Mr Pilgrim?
Mr Pilgrim: I will admit that, like a lot of people, I think, I am struggling with some of the technology based issues around this whole debate. But the examples that were given this morning are ones that I think we would agree with. We are just not clear whether they do fall in necessarily to the services that it is proposed be covered by the bill. I think from a regulator's point of view, that is possibly a bit of a challenge because, if we are not clear about whether those services do fall in or not, it is hard to be sure whom or what services we are supposed to be regulating—if we are to take some of our more proactive regulatory roles that I have described or if in fact we are going to be, say, pursuing individual complaints about a matter. I do not know that I can actually expand more on the examples we heard this morning and the ones we have in our submission, but they are the sorts of issues that we are not entirely clear on and we think there could be a little bit more clarity around those particular services.

Mr DREYFUS: A related point is your proposition that the data that is required should be set out in the legislation, as indeed the period of retention should be. I take it from that—I am paraphrasing, so correct me if I have not got this right—that your view is that members of the public are entitled to know what data the Australian parliament has legislated telecommunications providers be required to keep and for how long; and that it ought to be possible, simply as a matter of the democratic contract, if we can call it that, for people to go and look at an act of parliament and see what providers are required to keep.

Mr Pilgrim: Yes, that is true.

Mr DREYFUS: As to your suggestion that there ought to be a sunset provision on this legislation, if it is enacted: is that effectively based on a concern that this is an intrusion into privacy; that there ought to be continuing review; that five years is long enough to work out how effective this scheme, if it comes in, has been, and how effective oversight measures have been; and that legislating for a review is better than an indefinite imposition of what is going to be quite an onerous requirement?

Mr Pilgrim: Yes. Without repeating exactly what is in my submission, I think that, firstly, those issues are important ones to warrant a sunset clause. I also think that, given the changing nature of technology, it may be that we just cannot tell at this point in time—which we have an idea of the services and the types of information that will be covered, the change in technologies and devices that we are using, we cannot, I think, predict; they seem to be changing so quickly. So there may be bits of information that may start being collected that we had not anticipated or devices that may be able to collect them that we had not anticipated, and we may need to review whether in fact this scheme is working or whether there is more information that is being collected than we had anticipated. And I think that, given the volume of information that is going to be collected, that, in itself, warrants very considered reconsideration of the application of any scheme that may go into place.

Mr DREYFUS: Here is another possibility—and God forbid that this should occur: that a combination of increased use of technologies like VPN, Tor and encryption means that there has ceased to be a purpose in keeping data. If that were to occur, that might also be a basis for reviewing a scheme that is requiring the collection and retention of a large amount of data.

Mr Pilgrim: It could well be; yes. That goes to my point about the changing of technology, and I used the word 'devices' but certainly those over-the-top services, for example, could also change the very nature of the information, whether it is actually stored or collected at all.

Mr DREYFUS: The final matter I want to go to is: in your opening statement, you mentioned the proposition that you have put forward that the purposes for which—and, perhaps to make this clear, we are now talking not about the retention requirement; we are talking about the purposes for which data that has been retained is able to be used. Your suggestion was that it ought to be limited to national security and serious crime, but you then went on to say that more recent advice from the Attorney-General's Department has suggested to you that that limitation might not be possible. Could you speak to that for us, as to where that prohibition on limiting the use comes from and how it might be dealt with? I think what you said was that, for more minor matters, for more minor offences, some additional level of safeguard might be appropriate.

Mr Pilgrim: I firstly must admit to not having had a lot of opportunity to turn our minds more to it than yesterday, because we picked up that reference in the Attorney-General's Department's submission to the committee only yesterday. Do you have the exact reference?

Ms Falk: Yes. The Attorney-General's submission at page 44 states that:

As a party to the Council of Europe's Convention on Cybercrime, Australia has international obligations to make access to telecommunications data available for the investigation of all criminal offences. Article 14(2) of the Cybercrime Convention requires parties to ensure that telecommunications data is available for the investigation of any criminal offence, not just serious offences.
My understanding of the Attorney-General’s submission is that that would not limit their ability to confine the nature of enforcement agencies that have access to the data to those that are responsible for investigating serious crime, but it would constrain them from restricting the access to that data by those enforcement agencies to only investigating serious crime.

Mr DREYFUS: And, in the short time you have had, your thought was—which you have expressed to us in your opening comments, Mr Pilgrim—that perhaps some additional safeguards might be introduced for the use of telecommunications data for more minor crime?

Mr Pilgrim: And, if we could, I would be happy to take that on notice and probably give that a bit more thought and just spell out a couple of points about some thinking around that, rather than trying to do it on the run—

Mr DREYFUS: Through the chair, I think we would be happy to receive any additional comment you have, in writing, on that point.

Mr Pilgrim: Sure. I will do that.

Mr DREYFUS: Thanks very much, Mr Pilgrim.

Mr NIKOLIC: Mr Pilgrim, I am keen to explore your view that a year for data retention is sufficient, given the evidence that you have seen and that has been placed before the committee. Is that accurate?

Mr Pilgrim: Yes. What I said in my opening statement was that there seems to be evidence put to the committee that the majority of the accesses required for particular investigations were around six months and up to 12 months. That would seem to support a possible data retention scheme of around that period. I then went on to add that, obviously, the bill is proposing two years, and so I suggested there may be further evidence to support that but that I am not privy to that information.

Mr NIKOLIC: Indeed, you are not. At paragraph 37 of your submission, you state:

The evidence put forward by Australian enforcement and security agencies, including evidence provided to the Committee at the hearing on 17 December 2014, states that telecommunications data that is less than one year old is used in a large proportion of investigations.

You then go on to say:

Specifically, the Australian Federal Police … made submissions about the central role that telecommunications data plays …

And then at paragraph 38 of your submission, you say:

However, the case for a longer data retention period is less clear.

So I went to the comments of Commissioner Colvin to this committee on 17 December. He said:

The proposed dataset reflects the minimum crucial categories of data necessary to support investigations into serious criminal activity … Further, the AFP firmly believes the proposed two-year retention period to be a reasonable and appropriate time. Law enforcement agencies can then be confident that providers will not have discarded relevant data and seek access in clearly prescribed circumstances.

Long-term complex investigations have demonstrated the critical importance of access to the historical telecommunications data.

Given that you refer to the 17 December evidence, there seems to be a disparity that I am keen to explore between what you have said in your submission and what the commissioner said to this committee on 17 December. If you do not consider his comments about a two-year period as influential or as constituting evidence, why not?

Mr Pilgrim: I am certainly not saying that it does not constitute evidence. Reflecting on those particular figures, what I was looking at was the number or, I suppose, the percentage of matters they said that they used the particular information for, or the age of those matters seemed to be suggesting a longer—

Mr NIKOLIC: Why is the percentage important? You have placed a quantitative judgement rather than a qualitative judgement on this. If only 10 or 20 per cent of cases have this long-term need and result in 10 or 20 out of the hundreds of cases that come forward and stop 10 or 20 counterterrorism or serious criminal offences, why do you do it on the basis of the quantity rather than the quality of outcome that arises?

Mr Pilgrim: I am certainly not saying it is not based around the quality of the outcome. Earlier, as I was answering one of the questions, I suggested there are going to be matters that can impact. One investigation could have a potential impact on hundreds or thousands of people, and that is extraordinarily important. I suppose working through this information, as we interpreted it, we went off certainly the quantitative information. I am happy to review that, but I do not think we had seen a lot of qualitative information coming through to equate it. There were a lot statements around certain types of investigations. I am not saying that we have necessarily interpreted it entirely accurately, but I do not think we saw—
Mr NIKOLIC: The commissioner then went on to say on the quantitative side:

... I can advise that telecommunications data has been used in 92 per cent of counterterrorism investigations, 100 per cent of cybercrime investigations, 87 per cent of child protection investigations and 79 per cent of serious organised crime investigations.

He goes on to talk about operations Neath and Pendennis and a number of other case studies. I guess my question is: you are adamant in your submission that there is only evidence to support one year and you have come with the recommendation that one year is sufficient, yet here is the person, the commissioner, who is actually at the operational and tactical end of conducting these investigations saying, not with any sort of equivocation but definitively:

"... the AFP firmly believes the proposed two-year retention period to be a reasonable and appropriate time."

And:

Long-term complex investigations have demonstrated the critical importance of access to the historical telecommunications data.

Yet there is no evidence of that included, even though you mentioned the AFP in your submission, and I just find that an interesting omission.

Mr Pilgrim: We certainly recognise the evidence that was given to the committee about the number of cases in which telecommunications data was essential for those investigations; what we were looking at, when we referred to those numbers, was the age of the information that had been requested and saw that the majority of the cases were for information that was less than a year old. So we were taking it from that perspective.

I would also like to mention that I certainly have not said that there should only be one-year data retention; I said the evidence as we have assessed it certainly supports a case for doing that, but we have not ruled out two-year retention because we are saying that there is evidence that we have not been privy to, and probably for good reasons in terms of national security and the like, that the committee itself will have to weigh up to see if it supports an argument for a longer retention period.

Mr NIKOLIC: You comment at paragraph 37:

"... 90% of the telecommunications data obtained by ASIO is less than 12 months old. Therefore, on the evidence, you are happy to go with a one-year data retention period—"

Mr DREYFUS: Chair, I have to interrupt my colleague here. I do not find it helpful to the committee's deliberations, nor to the public's consideration of this matter, for Mr Pilgrim's evidence to be misrepresented here by Mr Nikolic. It is a real concern to me—

Mr NIKOLIC: How am I misrepresenting his evidence?

Mr DREYFUS: And it is unhelpful for all this questioning to be proceeding on the basis that that is what he said.

Mr RUDDOCK: I think my colleague is trying to clarify what he was saying.

Mr NIKOLIC: Absolutely.

Mr DREYFUS: Well, he should do so without verballing the witness—

Mr NIKOLIC: I am not verballing the witness at all.

Mr DREYFUS: and without misrepresenting what his written submission says.

CHAIR: I think Mr Pilgrim is big enough and brave enough to be able to make his point.

Mr DREYFUS: I am trying to save time here, Chair.

CHAIR: Okay. He did make that point and I am sure he will be able to make it again.

Mr NIKOLIC: You say at paragraph 37:

"... 90% of the telecommunications data obtained by ASIO is less than 12 months old. Therefore, you have expressed, on the available evidence as you see it, a preference for a one-year data retention period. Logically, 10 per cent of cases would, therefore, not be covered under your preference."

Mr Dreyfus interjecting—

Mr Pilgrim: What I have proposed in my submission is that I think, on the evidence before me—
Mr NIKOLIC: Listen, I—

Mr Pilgrim: that there is potentially a case for—

Mr NIKOLIC: Chair, with respect, I did not interfere with the Hon. Mark Dreyfus, QC when he was asking questions.

Mr DREYFUS: You did not have cause to.

CHAIR: I think what we need to do is let Mr Pilgrim answer the question.

Mr Pilgrim: Thank you, Chair. On the evidence before us, as I have interpreted the evidence provided by the law enforcement agencies, as you said, 90 per cent of the telecommunications data obtained by ASIO was less than 12 months old. On the basis of that, I said that there was possibly a case there to support a data retention period of 12 months, one year. What I then went on to say was that there may be additional evidence that is provided to this committee that we are not privy to—and I said there may be good operational reasons why we are not privy to—that could support a longer data retention scheme. That, again, without wanting to sound arrogant or telling the committee how it should do its job at all, is information that the committee will need to weigh up and, therefore, use when it comes down with its report for whatever length of retention scheme there should be.

Mr NIKOLIC: I guess I am referring to not just evidence that is available to the committee in camera but evidence presented by the AFP commissioner on a date that you yourself refer to in your submission. I just wonder whether you find influential his definitive comment about the necessity of a two-year period. If you do not, that is fine, but I guess my question is: if not, why not? It is not just something that the committee is privy to but something which is on the public record on a date you refer to yourself.

Mr Pilgrim: The information which I based my submission around is the information that suggests that the bulk of the data that is sought by the law enforcement agencies is data that is under 12 months old. So that is what I formed my view on. Again, without wanting to be too repetitive, I accept that there may be other, stronger information and data available to the committee that may support a longer period of time, and it is the role of the committee to decide that.

Mr RUDDOCK: Or whether you think proportionality has some chance.

Mr NIKOLIC: Given that that is the AFP Commissioner's strong and deeply held view, presented to the committee and to the public on 17 December, shouldn't we err on the side of caution in terms of detecting and preventing crime? What harm is there then in having a two-year period, from your perspective?

Mr Pilgrim: The question comes back to some of the additional protections I have put into the submission. If the committee decides that it would recommend a two-year data retention scheme, if such a scheme goes before the parliament and is passed, I would hope that therefore there would be some of the additional protections put in place, because some of the issues go back to some of the matters we have touched on through Mr Dreyfus's questions around potential data breach and the loss of that information or the compromising of that information, and we need to make sure that there are additional protections in place.

Senator FAWCETT: In paragraph 62, as part of your additional protections, you said:

... further safeguards should include:

- limiting the purpose for which an authorisation can be made to where it is reasonably necessary to prevent or detect a serious offence and safeguard national security

In the context of that additional protection, I am just wondering whether you have turned your mind to ASIC's submission and their request to be listed as one of the agencies in the legislation who have mandated access to the data?

Mr Pilgrim: I am not across ASIC's submission, and I would be happy to have a look at that and take that on board and give some comments on notice if you would like.

Senator FAWCETT: That would be good, thank you.

Mr BYRNE: In the lead-up to the drafting of the legislation was your office consulted by the Attorney-General's Department or the Technical Working Group?

Mr Pilgrim: Not by the Technical Working Group—I think that is correct. No, we were not by the Technical Working Group. I did have a couple of meetings with the department on a range of issues around the raft of bills, including the foreign fighters bill and the like, and we did discuss some aspects relating to this.

Mr BYRNE: When you say 'some aspects', could you elaborate on what you discussed?
**Mr Pilgrim:** To the degree that I requested meetings to discuss a number of issues around the tranche of three bills, as the data retention scheme became, I suppose, clearer before it was actually at the bill stage, I asked for a discussion around what some of the proposals were there. For example, I proposed a suggestion that there should be a privacy impact assessment done for the bill, and I am pleased to see that—

**Mr Byrne:** Exactly. They have taken that on board.

**Mr Pilgrim:** A privacy impact assessment was done and attached to the Attorney's submission. Unfortunately it was not in their table of contents, but we saw it was there. So we did have discussions with the Attorney-General's Department. I would not necessarily describe them as consultations.

**Mr Byrne:** Would you envisage a further role for yourself and your office in the implementation should this legislation be passed, other than what is being discussed in terms of privacy considerations—besides data breach notices and other matters?

**Mr Pilgrim:** Certainly. For example, as I have touched on, if there are to be regulations made, I would like myself or our office to be consulted as those regulations are developed, because I think we can provide a lot of useful advice given the experience our office has had over a number of years in handling this sort of information. Similarly, if there are changes to be made to regulations, as I suggested, there should be privacy impact assessments done on future changes, and I think our office can provide considerable advice and guidance in the undertaking of those privacy impact assessments.

Importantly, there has been reference made to security legislation to complement this particular bill. Our office again has recently issued a quite comprehensive set of guidelines which go to advising government agencies and private sector organisations about securing personal information, because it is a requirement of privacy principle 11 that all organisations take reasonable steps to protect the personal information they hold. As I said, we have issued just recently a revised set of those guidelines, which I believe would go a long way to assisting the development of any additional legislation to bolster the security protections around this information should it be required to be held.

**Mr Byrne:** Did you detail your concerns about prescribing enforcement agencies by regulation to the Attorney-General's Department?

**Mr Pilgrim:** Not specifically, no.

**Mr Byrne:** Is there any reason why you did not do that?

**Mr Pilgrim:** I think at the time of our last meeting we did not have a copy of the bill, which actually set that out. So it did not come up in discussion.

**Mr Byrne:** But had you had that bill in front of you, you would have raised that as a concern?

**Mr Pilgrim:** If we had had the opportunity to have the bill earlier and to be able to work through that, yes we would have raised issues we had at that time.

**Mr Byrne:** Did you raise the issue of exemptions to some carriers and service providers?

**Mr Pilgrim:** I cannot recall off the top of my head—Ms Falk was at the meetings—whether we specifically went to those issues in those preliminary or earlier meetings.

**Ms Falk:** My recollection is that there were some discussions around the kinds of service providers that would be covered by the bill and also the coverage of the Privacy Act in terms of the oversight of those entities but nothing further.

**Mr Byrne:** So at what stage of the bill's drafting did you actually have this conversation or series of conversations or whatever it was that you had?

**Mr Pilgrim:** I would like the opportunity just to confirm—

**Mr Byrne:** Of course.

**Mr Pilgrim:** Not because of any other reason, but I would hate to mislead the committee. I do not think we had a copy of the bill prior to our last meeting on this issue with the department.

**Ms Falk:** I think we would have to confirm that.

**Mr Pilgrim:** We would have to check the timing of that.

**Mr Byrne:** You were not given a copy of the bill or draft at any stage of the consultation process?

**Mr Pilgrim:** Again, sorry, but, if I could, I would like to confirm that to see when we did get the first copy of the bill.
CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.

Mr Pilgrim: Thank you.
CHAIR: Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Lobb: I do. Vodafone Hutchison Australia is Australia's third largest telecommunications company. We are owned by Vodafone Group Pty Ltd and Hutchison Whampoa, two of the largest telecommunications companies in the world. So we do bring to the committee an international perspective that we hope you will find useful. Consistent around the world, our starting position as a telecommunications company, is that our customers have a right to privacy. It is something that is enshrined by international human rights law and this is enacted through national laws. Respecting the right to privacy is one of our highest priorities. It is integral to the Vodafone code of conduct, which we all follow at our organisations. However, in every country in which we operate we abide by the laws of those countries which require us to disclose information about our customers to law enforcement agencies and other government authorities. We acknowledge that these laws are designed to protect national security and public safety.

We therefore have to balance our responsibility to respect our customers' right to privacy against our legal obligation to respond to the authorities' lawful demands, recognising our broader responsibilities as corporate citizens to protect the public and to prevent harm. We have a proud history of doing so. That is of course the issue we are here to discuss today. You may be aware that in June last year Vodafone Group released a law enforcement disclosure report, which we have included in the submission. It provides a global country-by-country analysis of law enforcement requirements that we hope the committee finds useful.

In starting to discuss what is proposed in legislation today, the assessment of that report and our own assessment is that Australia's current regime for law enforcement and access to telecommunications data strikes one of the better balances internationally between the need for effective law enforcement and the need for privacy protection and also, importantly, independent oversight of the operations of the investigative regime. From our point of view, our paramount focus must be to ensure that our law-abiding customers have a right to privacy.

There has been a fair amount of ambiguity about the policy intent of the proposed regime for mandatory data retention. At times the justifications have been that we need to establish a mandatory data regime to consolidate and standardise current arrangements. As you are aware, the metadata for traditional telephony has been something that telecommunications companies have been providing to companies for many years. Agencies have said that they want to protect current law enforcement activities because there are concerns that communications providers are starting to stop retaining that data. In our view, while we do not see a significant risk of a loss in the current metadata capabilities for law enforcement agencies, we do see policy merits in a more standardised set of arrangements to give certainty for agencies, industry and citizens. So the policy intent of the overall framework we do think is an appropriate and worthwhile activity.

On other occasions, though, the argument for the new regime is that technologies and methods of communication are changing and so we need a mandatory data retention scheme to allow governments to extend their metadata investigative capabilities. We understand that, as technology changes, regulations need to change to take into account different ways that consumers undertake communications, but our concern and our interest is that the proposed mandatory data requirements go well beyond traditional telephony billing information, which has been the less technical term for the old-style metadata that has been available up until now. A number of facets of the new requirements go well beyond the data retention activities that we would undertake as telecommunications companies for our normal commercial and billing purposes. So this represents a significant change from what we currently provide. This is really the nub of the policy focus that we think the committee needs to look at: those expanded data retention requirements into the new technologies.

As government policy has developed over the last six to 12 months, the details of important improvements to the proposed regime have been introduced. Firstly, we welcome the government's commitment to make a contribution to the capital costs of the new requirements. We agree with the rest of the industry that the cost of setting up this new capability should be paid for by government and that these government contributions should be provided in a competitively neutral way. We also welcome the proposal to reduce the number of agencies that can access the metadata information that has been proposed. As in the discussion the committee just had before with the Privacy Commissioner, we would also like the committee to consider whether there should be offence
thresholds for which data can be accessed. Under the interception powers there is a threshold about the seriousness of the offence for which you can then get a warrant. We think the committee should consider whether there should be a threshold for access in particular to the new metadata. I understand but I am new to the idea that the Attorney-General's Department has introduced, which is that there may be restrictions on that, but we do think that is worthy of some focus of the committee to see whether that is worthwhile particularly for the more sensitive new aspects of the data retention measures.

We also welcome the increased oversight by the Ombudsman that has been proposed by this regime. We think that that new role is welcome, but we would also like to see the Ombudsman clearly have a role in reporting their findings from their ongoing annual investigations. Certainly the metadata debate has raised a great deal of public interest about when and how this information is used by the security and law enforcement agencies. It is not to say that should interfere with investigations. Rather, I think the public does need to understand when and how the information is used and whether there is independent oversight of those arrangements being carried out appropriately and consistent with legislation.

I would like to turn to two broad concerns that Vodafone has with the legislation in its current form. Of most concern, as we flagged in our submission, is the proposed duration of the metadata retention. In particular, we are concerned about the length of time proposed for the storage of the IP identifier metadata. This is the data that is essentially analogous to a telephone phone number, where a customer, when they access the internet, gets assigned an IP identifier so that they can carry out access to the internet. We agree with many other stakeholders that the data storage requirement should be no more than six months, particularly for this IP identifier metadata—and we offer some comments about why we think that is appropriate.

Firstly, the proposed two-year requirement is at the upper bounds of the storage requirements being contemplated around the world. We note the European Commission's evaluation report on this which found that most data requested by law enforcement agencies is less than six months old—and you would certainly be aware of that. That is consistent with our experience in Australia. At Vodafone, our experience is that, generally speaking, around three-quarters of information is less than six months old and around 85 per cent is less than 12 months old. So it sounds like it is consistent across telecommunications providers.

We think that the time lapse will be even shorter for IP identifier information. This is because IP identifiers are not like static customer telephone numbers. Each time you set up a data session, you are generally assigned an IP identifier for that session. It is a dynamically allocated number. It would usually be used, we believe, when a particular rogue website is under an interception order—for example, a terrorist site or a paedophile site—and agencies will notice that there is an IP identifier that has accessed the site. At that point, the agencies will ask the telecommunications companies who had that IP identifier assigned to it. So the idea that you would be looking at a website of two years ago and then asked two years later, 'Who was that particular IP identifier?,' we think is much rarer than the circumstance where an investigation might find a telephone number when they have raided an office and they want to understand who had that telephone number, because telephone numbers are obviously assigned for a longer duration.

Secondly, IP information is much more sensitive data than traditional telephony metadata. Traditional metadata is generally account information and phone numbers, and often that information is in the White Pages and so on. The feedback we are getting from consumers is that kind of information is less sensitive than IP identifier information.

The other area of concern—and I think this has been raised in the discussions this afternoon—is that we do think that it is important that there is certainty about the data retention obligations. As it stands, the current proposal is a regulation based list of metadata requirements. Along with other stakeholders, we think that there needs to be significant oversight of that. Certainly, the minimum would be that if any changes are made there needs to be a requirement of consultation with industry, relevant agencies, such as the Privacy Commissioner, and that that be subject to parliamentary oversight, and, also, that when those considerations are made there is also due consideration for the amount of time the new arrangements can be put in place. That concludes my opening statement.

Mr RUDDOCK: You suggested that the measures we are now enacting go well beyond—and you kept on asserting 'well beyond'—the extent to which existing data provision requirements operate. What are those elements that are well beyond what is now retained, for instance by Telstra?

Mr Lobb: It is the metadata identifier information. That is the new measure. Currently, as other industry players will say, that the capability to marry IP identifiers with account holders is a capability that is certainly in its infancy, and it is generally something that telecommunications companies do not have the capability to do it at the moment.
Mr RUDDOCK: I suppose I would ask myself this question in relation to metadata and new capability: if it becomes known to terrorists that you can communicate and that information will not be kept, then that is the only source they would use. What you are really saying is that, if there is a metadata element that is not now covered but is in fact new, but it would give them cover, we should not go after it.

Mr Lobb: Not at all. What I am saying is that that is a new capability and will be a new requirement. We do perfectly accept that that is a new communication capability and does warrant consideration for metadata requirements. What we are saying is that that is sensitive information—

Mr RUDDOCK: So, if we think it is justified you would be prepared to accept it?

Mr Lobb: I think we accept that people are undoubtedly communicating via IP means and, given so, it warrants consideration.

Mr RUDDOCK: I have struggled in these hearings with people who assert privacy, because we are told that everything has to be proportionate. I try to have some understanding of what proportionality means, and I find it very difficult, conceptually. I was interested in a quote I had not seen before from the Office of the High Commissioner for Human Rights suggesting that where you have to weight up other rights—for instance, the right to life—all that has to be shown to justify the waiver of privacy is that there is 'some chance' of achieving that goal. I noticed somewhere else—perhaps I should take it up when we come to it—that there was a reference to a 'just in case' test. I do not think it is a 'just in case' test; it is a 'some chance' test.

Now, we go to this period of two years and your suggestion that most of the requests are for relatively short periods. But even if you have one major terrorist organisation that you did not become aware of—they are not registered and they are not out there—that you become aware of at some point in time, wouldn't you want to be able to go back beyond six months to see who had been in touch with them and might be getting the information about how they could carry out a terrorist act? Wouldn't that meet a 'some chance' test?

Mr Lobb: I think this is the key issue that we need to discuss and assess. I think that, generally, threat to life investigations would be much more immediate than that. It would be within days and weeks. But, you are right, there are conceivably longer periods than that and we have to weigh up the various rights and interests and activities. And I suppose what we are putting forward is that when we talk about IP identifier metadata the chances of that being used in those situations is less than with traditional telephony and also that IP identifier information is substantially more sensitive information and may warrant a different consideration to more traditional account-holding and billing information that has been available to date.

Mr RUDDOCK: I understand that for a local government there are all sorts of other issues that relate to money, although we had some people talk to us about the extent to which people's savings might be denuded by fraud, that they are proper investigations to undertake. But I am dealing with right to life. Once you have established that there is some chance of a terrorist act, then the information has to be kept. You cannot say, 'We'll only keep it for terrorist investigations.' You have to have access to the information per se, don't you?

Mr Lobb: Yes, and I think the length of time that is stored is a judgement that needs to be part of the considerations of this committee.

Mr BYRNE: You have an offshoot in the United Kingdom.

Mr Lobb: A very important one.

Mr BYRNE: Yes, indeed—Vodafone. How are they going with the 12-month data retention regime over in the United Kingdom?

Mr Lobb: I must say I am not sure of the status of the requirements, but I think 12 months is a fairly typical amount of time in Europe. I know that the European Commission has made some assessments that require that to be looked at in more detail. But I am sorry, I do not know—

Mr BYRNE: Do you know what the cost would have been to Vodafone UK to enable them to keep the dataset that the government required?

Mr Lobb: No, I do not.

Mr BYRNE: Is it possible that you could take that on notice? Do you have a fairly close relationship with Vodafone UK?

Mr Lobb: Yes, I can take that on notice, and we can provide some experience, where regimes have been set up, about what the requirements have been. They will be very similar to Australia's—

Mr BYRNE: Yes, they are very similar.
Mr Lobb: in the sense that we have always held the traditional telephony metadata—billing records, account holders—for certainly longer than two years. And that is for both business reasons and regulatory reasons. So, that is established. The difference with IP traffic and data flows is that the way that is billed is not necessarily about where the customer has gone. And because the IP identifiers are dynamically allocated, it is a very complex and very data-rich database where we have to marry identifiers with accounts. So, that capability is one that has needed to be developed universally.

Mr BYRNE: And just in terms of Vodafone UK, is that doing relatively well over there?

Mr Lobb: The organisation?

Mr BYRNE: Yes.

Mr Lobb: Yes, it is doing very well. Obviously it is one of the largest telcos in the world. Regarding the status of the—

Mr BYRNE: So, how long have they been subjected to the European data directive? It would have been 2006 when you started being required to keep the data for a 12-month period.

Mr Lobb: I do not know the status of the United Kingdom. I had better get back to you, but I think there might be elements that are still a work in progress.

Mr BYRNE: But would they be a group that you would consult with in the implementation of your data retention regime, should that come into law?

Mr Lobb: Yes.

Mr BYRNE: And do you have a rough costing as to how much that would be?

Mr Lobb: Not at this stage. We provided assessments to the PWC. I do not know whether you are privy to that commercial-in-confidence information.

Mr BYRNE: No, they have not been brought to our attention.

Mr Lobb: When we made those assessments it was not as clear what the requirements were as it is now. That said, the requirements are pretty much the same. The key challenge is going to be marrying the identifier to the account and doing it over many, many data sessions. Our estimate is petabytes of data, which is a significant amount. And setting the capability up to do that and then storing it and protecting it is not without its costs.

Mr BYRNE: But you would be importing some of that expertise, software from—

Mr Lobb: We would certainly talk to them about it. I think technically we do understand what we would need to do.

Mr BYRNE: How many times has Vodafone been consulted since data retention was raised?

Mr Lobb: We have had a number of meetings with the Attorney-General's Department about our capabilities and what we think about the metadata list. I think it is fair to say that the list is consistent with the European requirements. There was obviously some ambiguity about whether URL addresses were part of that, but that is now clear. There has been ongoing discussion about whether we have to log every single event. There are ways we can reduce the amount of data we need to store and that might reduce costs. There will be discussions about that. There does need to be some flexibility about delivery. Obviously we have a long history of working with the law enforcement agencies about what works for them, and that discussion will be ongoing.

Mr BYRNE: You mentioned as part of that conversation that URLs were actually being contemplated by the agencies. When would that have been, in terms of your consultation?

Mr Lobb: It would have been when the Attorney-General announced that there were going to be consultations. I cannot remember the exact date. It was the end of last year.

Mr BYRNE: So the Attorney-General's Department basically suggested to you that URLs might constitute a data set?

Mr Lobb: No. I think it was more about what data you need to keep and also what would be required to bring it back to an account holder—did it need to be the full address or could it just be the IP identifier? It was more a technical discussion rather than a policy discussion.

Mr DREYFUS: I want to ask you some questions similar to those that Telstra dealt with this morning. Vodafone is the third largest telecommunications provider, after Telstra and Optus, in Australia?

Mr Lobb: Yes.

Mr DREYFUS: Vodafone at present keeps data for its business purposes?

Mr Lobb: That is right.
Mr DREYFUS: And also in compliance with the Australian Consumer Code administered by the Department of Communications?

Mr Lobb: Yes. And obviously for law enforcement purposes—if, under the Interception Act, we are required to provide reasonable assistance, we would do it for warrants and so on.

Mr DREYFUS: Of course. And you, along with the other telecommunications providers, receive thousands of requests from Australian law enforcement agencies every year and comply with those request to the extent that you are able?

Mr Lobb: Yes.

Mr DREYFUS: Does the data retention requirement that this bill would impose on Vodafone, along with every other telecommunications provider, call on you to store data that you currently do not keep?

Mr Lobb: Yes, that is right. That relates to the IP metadata. And certainly the duration of the storage of the data would be shorter. Generally we store data for billing purposes—

Mr DREYFUS: You said you now keep that data that you use for billing purposes for two years and longer.

Mr Lobb: Yes. Telephony we store for more than two years—call records and account details. For metadata, we do store some marrying of accounts to IP identifiers but not at the capability that is being contemplated here. Again, we do that for systems purposes or for billing purposes, but nothing as robust as is being contemplated.

Mr DREYFUS: And there will be a capital expenditure imposed on you to create the capability that Vodafone Australia does not presently have?

Mr Lobb: That is right, yes.

Mr DREYFUS: In lay terms, that is to build a system that will enable Vodafone to store, in particular, IP identifier numbers, which you do not presently retain?

Mr Lobb: Yes.

Mr DREYFUS: And that is because you do not have a business purpose for retaining those ever-changing IP identifier numbers?

Mr Lobb: That is right. There would be three costs from that. We would need to establish a capability to connect the IP identifier to the account. Then there would be the costs of storage. Another significant cost would be from having the ability to retrieve the data from the very substantial database.

Mr DREYFUS: And you have provided estimates of those costs on a commercial-in-confidence basis to PricewaterhouseCoopers?

Mr Lobb: Yes.

Mr RUDDOCK: Just on the same matter—I am very ignorant of these matters—Skype is a telephone you use on a computer. You are using IP identifiers. Does that mean somebody can have the equivalent of Skype on the IP identifier?

Mr Lobb: That is right. Skype is what is known as an over-the-top service. It goes over the top of the underlying IP—

Mr RUDDOCK: So traditionally we have access to telephone calls. You are saying that an IP identifier is something new. In fact, it is a substitution for a telephone.

Mr Lobb: That is right. As flagged, there is no doubt that technology is changing. We recognise that the new technologies require—

Mr RUDDOCK: I just wanted to satisfy myself that my understanding was not too far in error.

Mr Lobb: No, that is exactly right.

Mr DREYFUS: Just to go on with that, the IP identifier number changes during the course—to take Mr Ruddock's example—of a Skype call.

Mr Lobb: The phone number you might have in a Skype account is assigned by Skype, and that will not change. The underlying IP identifiers will change each time a call is made.

Mr DREYFUS: Yes, and that is the issue about matching it to account holders.

Mr Lobb: That is right. In might be better to understand it in fixed terms. You would have a fixed DSL provider leased out to a telco and then a customer would establish a Skype account with potentially a phone...
number in it. That component is managed by Skype. The IP identifier, the data stream, is managed by the broadband service provider. That is what we were talking about with the different IP identifiers.

Mr DREYFUS: To what extent is Vodafone a broadband service provider?

Mr Lobb: Around the world, we are a major fixed provider. In Australia, we are considering when we may enter the market.

Mr DREYFUS: You have provided, as I understand it, on an in-confidence basis the details about the age of data requests received by Vodafone in 2012, 2013 and 2014. To what extent can you put any of that on the record?

Mr Lobb: I did, just before. Around three-quarters are less than six months old. Around 85 per cent are less than 12 months old. As you can see from that information, it is fairly static. It has not changed over time. From information in other discussions, that sounds consistent with other industry players around the world.

Mr RUDDOCK: But 15 per cent is beyond that?

Mr Lobb: Yes.

Mr DREYFUS: And that is all data requests?

Mr Lobb: Yes.

Mr DREYFUS: Is there a distinction or difference that you can draw between requests for telephony data and requests for, say, IP identifiers or other data forms?

Mr Lobb: Certainly telephony metadata has been very useful in investigations. Given that we retain it for two years, I think a case could be made that telephony data could be held for a longer period. Certainly our view is that IP identifier metadata would be of most use more immediately than telephony metadata. That is because it is ever-changing. I think it is going to be potentially useful in regard to IP telephony. I think there are other ways of overseeing that. But when you are talking about an 'under surveillance' website, an agency will be looking at a dodgy website, an IP identifier accesses the website and the agency wants to find out who that person is, it is unlikely that that will be in two years hence. It is much more likely to be an immediate event.

Mr RUDDOCK: But not always?

Mr Lobb: Then the issue is proportionality and assessments of other issues.

Mr DREYFUS: Is Vodafone Australia proposing to reduce the data that it currently keeps in the foreseeable future, absent this legislation?

Mr Lobb: No. With respect to traditional telephony, we will continue to retain the call event: who was it, where did it go to? That will continue. We generally deliver itemised billing for calls and we do not have an intention to change those arrangements. So at this stage they will continue to be part of our data retention.

Mr DREYFUS: Are you able to explain to the committee what are the commercial-in-confidence or commercial sensitivities about public revelation of the cost? And I ask that question in the context of the Commonwealth of Australia using taxpayers' money to pay for this scheme.

Mr Lobb: I think there are potentially two. One is that we have not done detailed assessments of what the costs are, so we are reluctant to put forward a number when it could be incorrect. Obviously, as you know, the estimates have been hundreds of millions of dollars. I think that estimate was much more when content was potentially part of the scheme. That is where the substantial storage requirements would be, certainly less so with just IP identifiers. Another is that it might reveal differences in capability of our networks. Those would be the main two. But certainly we would be happy for you to see, in confidence, our assessments if the Attorney-General's Department thinks that is appropriate.

Mr DREYFUS: It is more if this committee thinks it is appropriate.

Mr Lobb: I would expect you would trump that, so yes, that is right.

Mr DREYFUS: Through the chair, we would accept that offer. Thank you.

Mr Lobb: As I said, it was an estimate and we have not done a full—

Mr DREYFUS: It will be taken exactly in that light. Thank you.

Mr NIKOLIC: Just a point of clarification: if I understand what you said, new technology data retention is for six months and, for old technology such as telephony, two years. Is that right?

Mr Lobb: That would be the way things would end up, with a six-month requirement. As I said, we will continue to hold the telephony data for two years.
Mr NIKOLIC: My question relates to how you settled on six months. It seems sort of arbitrary for the new stuff. Is that a cost issue? What drives the decision making to six months?

Mr Lobb: It is really customer feedback about their concern about the amount of data that we would be storing. Certainly, for billing purposes, if we were to ever have a capability we would not keep it for six months. We would keep it for less than that.

Mr NIKOLIC: But customer feedback on the old technology, telephony is not—

Mr Lobb: No, this is on the new technology. Certainly, as debates continue, the feedback from customers is: 'We're uncomfortable with IP identifier information being stored for significant periods of time.'

Mr NIKOLIC: Thank you. Thanks, Chair.

Senator FAWCETT: While on the same topic, can I clarify that one of the concerns you have expressed was that you felt that the usage of IP identifier information would be far more immediate and that you did not think it would stretch back as far and that was one of the reasons you thought six months was appropriate.

Mr Lobb: That is why we think it is reasonable that it is a shorter period, married against the fact that it is substantially more sensitive information in the consumer's mind.

Senator FAWCETT: Sure. I am conscious of the things we can and cannot talk about in briefs we have received, but one of the things I can highlight in the public space was that the Queensland task force Argos in 2006 started a paedophile operation, and 2010 was when they finally had the global bust all around the world. It is in the public space. I can say that is indicative of the length of time of a number of operations that use IP data. Given that information is available to indicate the length of time, does that change your position that six months is appropriate?

Mr Lobb: I am obviously not an operational expert, so I am not privy to that. I think it would be best to discuss that with the agencies. What I would say is that if you are surveilling a website, if you are getting information about what is happening at that website, and an IP address identifier comes to that site, it would be best for the investigation to identify who that person is quickly rather than a year or two years hence. In our view, practically, the six months allows the agencies to determine who has accessed those websites.

Senator BUSHBY: Mr Lobb, you indicated that the six months was a period which you put forward based on feedback from your customers. To any extent, did you then temper that with the desirability of law enforcement and security agencies being able to access that information, or is it purely formulated on the basis of feedback from your customers?

Mr Lobb: The six months is consistent with the Communications Alliance and the Australian Mobile Telecommunications Association recommendation. That was put forward as an industry consensus view. Certainly that is the judgement of Vodafone and others in the industry.

Senator BUSHBY: Following on from Senator Fawcett's questions, you indicated that it would be ideal to act quite quickly. I am quite sure that the law enforcement and security agencies, when they get wind that a crime may have been committed and that the identifier is available, would be acting very quickly to find out who is behind that. It is quite possible that our law enforcement agencies might get notified—and a good example is a child exploitation ring, where they work very hard to try and keep all that under wraps. Somewhere in the world they might crack into it somehow. Having done that, they will have all of these identifiers. They will contact Australian agencies and say, 'These are identifiers that we have in Australia.' But they may be, and are likely to be, historical. It is only then that our law enforcement agencies have the ability to go back and have a look and try and work out who the people are who are behind that. In that sense, the evidence that we have received from law enforcement and security agencies is that they would love to go back many, many years, but two years is where they have settled as the appropriate place to be able to capture most of those more egregious types of activities and to be able to get behind those people. We have had a lot of evidence here that, certainly when the law enforcement and security agencies identify a person of interest—criminal activity, terrorism, whatever it might be—there are other mechanisms that they have available to them which they can then employ, usually more intrusive. The metadata is good for helping identify who the persons of interest are when they get wind that something has gone on. They have a small crack and this allows them to open it up and find out who is behind it. In that sense six months is not necessarily sufficient.

Mr Lobb: I think that is something that will need to be discussed with the agencies. What I would say is that, certainly with a traditional telephone number, going back to beyond 12 months would be more likely because it is a static number that would endure through a number of years. In a situation where you retained the IP identifier detail 18 months ago and then you say, 'There is an IP identifier here. We want to know who that is. Do they marry?' that would occur substantially less frequently. So what we are saying is that, weighing up against that
factor, we think it would be less often, and also as this is substantially more sensitive information, a shorter period would be appropriate.

Senator BUSHBY: But the sensitivity is only highly relevant to the extent that it is accessed.

Mr Lobb: That's right.

Senator BUSHBY: For the law enforcement and security agencies, there is a pretty clearly defined set of circumstances under which they can access that information.

Mr Lobb: Yes.

Senator BUSHBY: There are issues, and I think the committee will work through those in terms of the security of information that is stored by providers and how you maximise that security. But it comes back to my question: it is only sensitive if it is accessed and how is that a problem for your customers?

Mr Lobb: It is the fact that it is every single customer's IP identifier as opposed to a small subset. For example, an arrangement could be put in place whereby, if there are websites that are being identified, you could regularly provide a list of the IP identifiers for those websites within the six-month period to enable agencies to have a list for future investigation. I think you are right. It is about accessing the information and protecting it appropriately. Where the bad people are accessing the bad websites is where the operational focus should be. What we are talking about here is the requirement to retain a substantial amount of data on everyone's metadata information. So the proportionality is: is there a way of avoiding that but also ensuring that very important investigations are effective? This is a new capability, and so what we are talking about is an enhancement. What we are not talking about is the traditional use of metadata, which from established practice is less sensitive information. At this stage, we do not have plans to alter the way that is being stored and retained—

Senator BUSHBY: The traditional metadata?

Mr Lobb: For the traditional metadata.

Senator BUSHBY: This probably does not apply so much to Vodafone but I will ask you the question anyway. The evidence that we have received from the law enforcement and security agencies is that their main concern is that changing business practices and models means that providers are less likely to retain a lot of the information that in the past they had and were able to access as required. Does changing business models mean that Vodafone is changing what it stores?

Mr Lobb: I should flag that there is the traditional 'maintain a status quo', and I think there are legitimate policy requirements about establishing that and making sure that it remains effective. At this stage, we do not think there is a risk for traditional metadata, but undoubtedly technology—

Senator BUSHBY: For Vodafone?

Mr Lobb: And also the industry, Undoubtedly, technology is changing. IP communications are going to become more and more significant. Switch based telephony will, over the next decade or so, become less and less. Undoubtedly, we do need to manage the technological change. To be clear, what is being proposed is an extension of metadata capability, and it is more sensitive information. As we move into the IP realm, we are saying, 'Let's be cautious about the amount of time that it should be stored.'

Senator BUSHBY: When you say it is 'an extension', you are not saying that the law enforcement and security agencies aren't already accessing that data where it is available?

Mr Lobb: Under the legislation, if there is a reasonable request, we are required to comply.

Senator BUSHBY: And you have it?

Mr Lobb: If we have it.

Senator BUSHBY: That is the issue as we understand it.

Mr Lobb: That's right.

Senator BUSHBY: It is about how we ensure that there is consistency and data available—

Mr Lobb: Undoubtedly, this will be a discussion that will be continuing, but the key issue is protection of consumers' privacy as the technology changes. That is why we are flagging what we are flagging today.

Senator BUSHBY: I understand that Vodafone and other providers provide a business in which people who are involved in criminal activities, people who are planning terrorist type activities, make use of your services.

Mr Lobb: Yes.
Senator BUSHBY: So, in a sense, you are innocently involved, but what you do is accumulate data which is of immense importance to law enforcement and security agencies. So you are the meat-in-the-sandwich in that respect but—

Mr Lobb: Yes. We recognise that we play a very important role for law enforcement agencies. We have a very good working relationship with them—high levels of trust—and we also have a very proud record of being involved in some very challenging investigations. We are not saying that that is not an important activity. We were just saying it has to be measured against the fact that, for the 99.99 per cent of customers, we want to make sure that we can say to them that we are protecting their privacy and that the information that we have stored is protected and used appropriately.

Senator BUSHBY: Whatever data you do end up storing, are you confident that you can store that securely?

Mr Lobb: We will establish that, consistent with our security standards. They are the standards that are well established internationally. You are probably aware the Attorney-General's Department is working up a compliance framework in this area, and we will meet those requirements. Consistent also, I think, with the Privacy Commissioner's comments, this will be data that we would treat very much as data consistent with our privacy requirements, and I think the Privacy Commissioner's role in that regard is very important.

If it is okay, I might just comment on the roles of the Ombudsman and of the Privacy Commissioner, just thinking about the discussion today. Undoubtedly, there are our obligations—privacy obligations and data retention obligations—and the Privacy Commissioner can play that role. But it not must not be overlooked that we see the role of the Ombudsman as ensuring that the law enforcement agencies' activities are consistent with the legislation; and we think it is important that the Ombudsman play a role in telling the public that they can trust what the law enforcement agencies are doing. I think that is a very important role, particularly as we expand that function.

One other comment I would make is that, at the moment, Australia is a good reporter of law enforcement numbers and activities. The Attorney-General's Department provides a report about that. We also have an ACMA report, where the industry self-reports to the ACMA, and the number for that same data is up to three times the Attorney-General's Department number. One is about 300,000 and the other is about 800,000 for the same information.

Mr DREYFUS: (inaudible)

Mr Lobb: That is because we get asked by the ACMA, 'How many requests did you have,' but the law enforcement agencies often have a single request that goes out to a number of operators. So, when you give it all to the ACMA, it is often multiples of the same event. We think that is inaccurate and that what should be looked at is a reporting framework that says, 'Here are the activities,' so we are being transparent about that and the customers understand the context in which the data is being used. We would like to see a bit more oversight, where an independent person could say, 'We're confident that this regime is working well.' I think that is a very valuable component of this.

Mr DREYFUS: This is something that has troubled a number of members of the committee. From your point of view, the ACMA number is a—

Mr Lobb: Misleading.

Mr DREYFUS: better reflection?

Mr Lobb: No, we think the Attorney-General's Department—

Mr DREYFUS: Worse than the Attorney-General's Department?

Mr Lobb: is the accurate number.

Mr DREYFUS: Okay.

Mr Lobb: And we think the ACMA report is unnecessary.

Mr DREYFUS: Because the Attorney-General's Department is reflecting a request from an agency in respect of a particular event or subscriber that might go to more than one company?

Mr Lobb: That is right.

Mr DREYFUS: But it is, nevertheless, more useful to think of it as a single request for the purposes of that investigation.

Mr Lobb: That is right. At the moment, if an agency comes across a phone number and wants to know who it is but does not know which provider it is, it usually will ask the three main ones and, potentially, a number of others. So the self-reported number is misleading. In fact, when the Vodafone Group put their report out, The
Guardian newspaper went to the ACMA because it looked like there were an enormous number of metadata requests and we had to explain that there was probably a more accurate number. I think that confusion is something that is minor in the scheme of things, but it is certainly something worth looking at.

Mr DREYFUS: That is helpful, Mr Lobb. In relation to the establishment of this capability, which came out of Senator Bushby's questions, on the last page of your actual submission, not the attachment—in the last couple of sentences, actually—you said:

- Generally, different IP-identifier numbers are allocated each time a customer accesses the internet or sends an online message and so each time a customer accesses the internet. It is our assessment of is that it will take some years to firmly establish a standard industry capability to store this data. In particular, before we introduced the capability we would need to be confident that we could protect every customer’s privacy.

This bill, as I understand its framework, envisages that the absolute compliance requirement—that is, the requirement to store from now on—commences two years after the bill commences. That is because the operative provisions do not commence until six months after the bill receives royal assent and then there is another 18 months bound up in the introduction of the data implementation plants. I am sure I have not done it justice, Mr Lobb. My question is: on the basis that this is a framework which allows two years for telecommunications providers to comply with the retention requirement, is that long enough, given that you have said it will take some years to firmly establish a standard industry capability?

Mr Lobb: We think that that two-year period will establish a capability. During that period of establishing it, there is going to be a discussion about the evidentiary quality of that information and that is the unknown.

Mr DREYFUS: Can you help us with what that term means—'evidentiary quality'?

Mr Lobb: Okay. Because it is a marrying of two pieces of data and the significant number of events in any one day, there may well be a discussion about what is the confidence that the marrying has occurred accurately. All technical things can be resolved. I suppose I am prefacing that certainly there will be a bedding down period.

Mr DREYFUS: So that you can adduce it as evidence in court for the purposes of the crossbench?

Mr Lobb: Potentially and if somebody flags with the department in passing that until we know what the requirement is and then how the law enforcement agencies are going to use it, that is going to be an ongoing discussion over that period of two years.

Mr DREYFUS: It might be that the agencies want to use it to give them a lead.

Mr Lobb: That is right.

Mr DREYFUS: It might be that they want to use it to eliminate a suspect and it might be they want to use it to adduce evidence in court with it and they are all different.

Mr Lobb: For the first two, I think the two-year period is reasonable. We liken this issue to ONA evidence. The legal process needs to have growing confidence about its accuracy for evidentiary purposes. That would be an implementation issue and I do not think it is insurmountable. That is why we flagged it. It will take some time to bed it down because it is a new complex capability.

Mr DREYFUS: Thank you, Mr Lobb.

Mr RUDDOCK: Maybe I should ask this question of the Attorney-General's Department but I will ask you just to help me. Given some of the news reports which suggest that people are claiming they are still getting rid of data, even though there is a bill there, because they believe the privacy obligations have primacy, I assume the legislation will ensure that the privacy obligations will not mean that we cannot use, that we cannot acquire the data for up to two years.

Mr Lobb: I do not believe so. That would be a drafting issue.

Mr CLARE: Thank you for the data you provided the committee on the age of requests. That is a combination of telephony metadata and internet metadata, I think.

Mr Lobb: No, that is the metadata requests to date. So that would be on telephony.

Mr CLARE: Is that telephony only?

Mr Lobb: Yes.

Mr CLARE: Are you able to provide the same data for IP?

Mr Lobb: We do not have that capability.

Mr CLARE: You do not have that capability at the moment.
Mr Lobb: We have some limited—for systems issues over very short lengths of time we might do it. In a really serious event we might be able to do it but we certainly do not store it in any way the same way we do for telephony. Obviously our systems have to marry up the two to enable the call to work. So, in that very immediate time, we might have that capability, but that data is telephony traditionally.

Mr CLARE: It is telephony only.

Mr Lobb: Yes.

Mr CLARE: You said in evidence that you hold telephony data for two years.

Mr Lobb: Yes.

Mr CLARE: Does that include SMS?

Mr Lobb: Yes, it does. There are some components of the new requirements that we would have to introduce into our capability. There is another table that I have provided in confidence where there are some limitations on our SMS capability, consistent with the proposed requirements. But, generally, in that metadata and those numbers, SMS was included.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.
BYRNES, Ms Bronwyn, Lawyer, Australian Human Rights Commission

TRIGGS, Professor Gillian, President, Australian Human Rights Commission

[15:51]

CHAIR: I now welcome representatives of the Australian Human Rights Commission. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Prof. Triggs: Thank you, Chair, I would like to make some introductory remarks. I thank you for the opportunity to appear before the committee this afternoon. I have had the advantage in the last three hours of listening to the presentations, the questions and the answers, and they have in fact informed some of the things that I would like to say to you very briefly. I obviously do not want to repeat our submission to you, but I am very happy to answer questions in relation to that submission.

Can I begin by saying that the Australian Human Rights Commission recognises the importance of ensuring that our police and security agencies have appropriate tools to investigate criminal activity as well as to protect national security, and modernising our laws to reflect contemporary technical advances is obviously a sensible, justified and legitimate objective, by reference to this bill. We then, in short, support the passage of the bill, but we do suggest that some amendments be made to it. In particular, we strongly support the bill's proposal to confine the number of agencies that can access retained telecommunications data, and there are other aspects of the bill that we think are extremely useful. But, if I may, I would like to concentrate on three particular matters that do concern us.

I am sure you are aware that our entire mandate is based on a human rights standard—in particular, the International Covenant on Civil and Political rights, which is part of our schedule and the mandate under which we operate. At least for this presentation, we are looking in particular at articles 17 and 19 of that covenant, which deal with the right to privacy and also the right to freedom of expression. The point has been made many times—and, in particular, by Mr Ruddock—about the importance of the proportionality test under that law. It is actually a test that applies both at international law and domestic law, but the part of the test that has been left out by most speakers is that it must be proportionate to the legitimate aim. I would like to suggest to you that it is the element of the legitimate aim that allows some answer to the kinds of questions that have been put about the difficulty of adopting a proportionality test.

The commission has also considered, as part of our background to making a submission, the experience of the data retention schemes in Europe and the United Kingdom as, of course, comparable legal institutions—and, in particular, the landmark judgement of the Court of Justice in the European Union on the EU's data retention directive, which underlies some of the thinking about what is an appropriate or best practice response to data retention.

So the first of the aspects that I would like to suggest to you are important concerns the retention period; you have been discussing that at some length. The two-year retention period is at the upper end of retention periods implemented in comparable jurisdictions. The majority of the European Union countries, including the United Kingdom, have a one-year period, and I think you are aware of the evidence from the EU that shows that only two per cent of requested data is over one year old. The commission has suggested an initial retention period of a year—maybe a compromise is 18 months—but it should be trialled for three years of the scheme's operation.

But I, having had the benefit of the discussion today, do believe that this concept is a very crude tool to deal with the problem that you are faced with, and that is that really you need some form of sliding scale which can take into account the seriousness of the matter. The question that arises from Mr Ruddock is: how you deal with the minor chance when the risk is loss of life and serious terrorism? I understand that the Australian Federal Police would like five years and not two years, 18 months or whatever turns out to be a political compromise. It seems to me that it would be far better to face the reality of the problem and create a structure that addresses that problem than to take a compromised period of time—let us say two years if it were to pass—that is not really addressing the issue, which is not one of statistics but is a matter of balancing the dimensions of the risk against the time needed to deal with that dimension. So I would suggest that some fresh thinking is required to really address this problem, and I am happy to come back to that.

The second point is that we recommend that the committee review the circumstances in which the retained telecommunications data can be accessed. In line with EU jurisprudence, the commission considers that access to
and use of the retained telecommunications data should be restricted to the prevention, detection and prosecution of defined and sufficiently serious crimes.

The third point, and the final major point, that I would like to make is that we believe that the process of supervision that has been adopted in the bill is ex post facto; it is after the fact. Before I develop that point, may I say that of course the Australian Human Rights Commission will be part of that ex post facto process, because we will highly likely receive communications, inquiries and complaints from the Australian community that their fundamental human rights have been breached, and we will need to consider those complaints and ultimately to make reports to parliament. So that will be part of the process. In other words, the way in which this is actually working in practice will be a matter that would be of considerable concern to the public, who will doubtless come to the Australian Human Rights Commission.

Our key concern here is that all of the safeguards, or the major safeguards, are after the fact. We suggest that some form of administrative—possibly judicial but for practical purposes administrative—body be developed in advance of the access or collection process so that there is some form of control. I know that there is great reluctance to look at a warrant process—which currently exists, of course, in relation to content—but I would like to challenge or ask you to think about the accuracy of the submissions and the Attorney-General’s explanatory memorandum in making a distinction between content and metadata. A great deal can be learned from metadata. Indeed, in many cases, more can be learned from metadata than can be learned from content, especially as many people are extremely cautious about content but forget that it is the metadata that can actually lead law enforcement agencies to a paedophile ring, to a terrorist group or to serious criminals. So I would suggest that the rationale for a distinction between the two is extremely weak and should be challenged. If it is accepted that a warrant is necessary for content, I think it at least has to be further explored why it is not necessary to have a warrant at the beginning of the process.

Again, I am conscious of the concerns that the warrant process can be time consuming, expensive and difficult to establish, and that is very important when we are dealing with critical questions of life and serious criminal offences. So we would suggest that, rather than going necessarily through a warrant process, some more nuanced process of administrative authorisation be adopted which is simpler, clearer and cleaner. That would help to deal with a problem that has again been pointed out—if it is only two per cent where you have got a really serious matter, you want it for four years, five years or sometimes longer. That is the practical reality that the law enforcement agencies will tell us about. And you are not going to solve that problem by having an 18-month or two-year retention period—or one year if that were to be accepted. But if you had an up-front administrative process that allowed the police criminal investigation authorities to come to that administrative body to say, 'We now have some evidence with a serious risk that we need longer to retain that data,' then that could be properly considered and extended for the period necessary in the circumstances. But it would mean that you would not be retaining data in relation to Australian citizens for a sort of catch-all purpose.

So I think the summary of our position at the commission is that this is a rather blunt or crude instrument to deal with a problem that is a very sophisticated one and one where considerably greater lengths of time may be necessary. But it is very hard in the first year, or 18 months or two years to know which is going to be that two per cent where you need it for longer. So you need a process at the beginning in order to be able to make these judgements, rather than ex post facto, by which case, of course, the damage is done—and it is going to be done on past performance, leading to damage to a lot of Australians who will be very concerned about their rights to freedom of speech and privacy at least, along with other concerns in relation to civil and criminal penalties.

A final point I want to make is a matter that has come up relatively recently—so we are perhaps all novices in this area—and that concerns the Council of Europe's Convention on Cybercrime. This is a convention of 2001, and Australia is a party to it. There is an obligation to allow access to what is stated to be specific criminal conduct. It does not say what specific criminal conduct is, but that is not relevant for the moment. There is a core obligation under that convention to allow access, and that is being used as a reason for permitting access in a way that can breach human rights. That is our concern. What I want to draw to your attention, if I may, is that article 15 of that convention specifically provides that the obligation to allow access for the purposes of specific criminal activity is subject to human rights protections and, in particular, is subject to the International Covenant on Civil and Political Rights. We would be very happy to provide some further information on that, as indeed I am sure are each of the other witnesses before this committee.

In summary, we agree that the passage of the bill should go forward. We would like to see some changes, and I think one of the most important is to consider how you deal with this problem of very serious, life endangering threats to the Australian community, and do it in a way that the law enforcement agencies are requesting but
equally protect the rights of the overwhelming majority of Australians whose privacy and rights to freedom of expression should be protected.

Mr NIKOLIC: Thank you, Professor Triggs, for your testimony and also for your support of the bill. You may have noted my interest in the data retention period earlier on, so perhaps I can commence there. I note your comments about security agencies desiring up to five years or as long as possible. But I note that the AFP Commissioner, in his evidence to the committee last December, talk very specifically about the period required. He said: 'The AFP firmly believes that the two-year retention period proposed in the bill is a reasonable and appropriate time frame and that long-term complex investigations have demonstrated the critical importance of access to this historical telecommunications data.'

We earlier heard from my colleague of a case study, and there are many others that we have heard which I guess are the backbone of that comment that the commissioner made. You say we should perhaps trial a one-year period. One of the things I have heard in recent times is that victims of some crimes, including sexual crimes, often do not report immediately; they report well after the actual crime has taken place. So I am just struggling to understand, given what the commissioner has said and given the case studies we have seen and the evidence that I think we have seen on the public record, why we would not want to give victims the benefits of the police commissioner's experience that two years is what is required.

Prof. Triggs: Of course, we greatly respect the views of the Australian Federal Police and the commissioner's views in particular. He has put his mind to it. That is obviously important opinion and evidence to be taken into account. However, at least we feel that the committee should be aware that the majority of European countries believe that a year is sufficient. That is relevant evidence; it is not determinative. But it is important in a global environment that we have similar approaches, particularly with jurisdictions that are comparable to our own.

My view, frankly, is that, while we could have a best practice of a year, 18 months or whatever the compromise is, the key question is to allow flexibility so that it will be possible for the law enforcement agencies and other agencies to come to some form of administrative body operating on an efficient basis that should be able to approve an extension of that data retention requirement in relation to certain kinds of matters. But I would have thought that, after a year or 18 months, there would be a greater level of knowledge for the law enforcement agencies to be able to say, 'Now we want an extension and we've got a reason for doing it.' So you have the sort of supervisory role beforehand rather than later.

Mr NIKOLIC: Doesn't the obverse apply as well—that, if you start off with a two-year period, you gain knowledge over the same period that potentially you might require a shorter period? Why wouldn't we err on the side of the victims here? Why wouldn't we err on the side of not telling criminals, 'If you can get away with it for one year, the chances are that we're not going to be able to follow up the data relevant to you beyond a 12-month period?'

Prof. Triggs: As you put it in those slightly emotive terms, what you are really doing is saying that the interests of 23 million Australians on the other side of the equation must be subject to intrusion in the interests of those victims. Many in the community, and we, would say that the more serious the offence, the greater the right to interfere in the rights of the other 23 million. That is the balance that constantly has to be made as a subjective judgement: the more serious the offence, the greater the intrusion.

I feel that the debate about the period is missing the core point. That is my concern. Frankly, I would not argue too strongly for a year. That happens to be best practice in Europe. If that does not impress the committee, that is appropriate. We would listen to the views of our own Federal Police officers; that is very credible and important evidence. Make it two years, but there are costs involved in two years, and that is another consideration, and there will be further intrusions into ordinary Australians' lives.

That is why I come back again to saying that, rather than being overly concerned with the question of exactly how long this is going to be, if there were some flexible administrative process to begin with then it would be possible to say: 'We want it to go for longer. We've got some evidence that we'd now like to consolidate by having further retention in relation to certain areas, for example, or in relation to certain suspicions—hopefully reasonable—in relation to criminal activity.'

Mr NIKOLIC: Thanks. Could I move to your recommendation 5—and I am mindful of how much time we have—which would effectively require some form of warrant process for each request. I guess my concern is that in the early stages of any investigation, when metadata is most useful—agility and the capacity of law enforcement agencies to access information and to understand the links between people or networks of concern are perhaps most valuable in the early stages of any investigation—applying a warrant process, which you have in the content side or the post-access side of the equation, to the pre-access side in my view adds red tape,
complexity and time and ties police officers up at the early stages of the investigation with another process. What evidence does the commission have that the current access to metadata by these agencies gives rise to your rationale that we must have some sort of warrant process prior to access of metadata?

Prof. Triggs: We are conscious of the concerns about red tape. Red tape is going to be the thing that interferes with the ability of proper criminal processes and investigation. The difficulty is that we are not convinced by the logic that there is a substantive difference for the purposes of law enforcement between content and metadata—in other words, anecdotally. We cannot say more than that; but I think it is something the committee should look at. It is unconvincing to suggest that you should have a warrant for content but no warrant for metadata, especially when there appears anecdotally to be evidence that metadata can be even more intrusive than the content itself. Indeed, it is arguable that now the ready access to content in some respects is already having a chilling effect on the willingness of people to commit their thoughts to the communications that are currently available. It is already clearly having an impact on the willingness of people to be frank in their communications. You might say, 'Well, that will be a reason for not having a warrant in relation to content,' which takes us away from the current debate.

Mr NIKOLIC: I'm not saying that.

Prof. Triggs: I know you're not. I think the key point is that, as we intrude on human rights for Australians, we have to be very alert to how we balance and particularly supervise those intrusions, and that is why we suggest that some form of preliminary administrative management of this will be a far more effective safeguard of those rights than to rely on ex post facto our protections when the damage is done.

Mr NIKOLIC: Why then have you taken a different view to that of the UN Human Rights Council? I refer to a report by Frank La Rue, the UN Special Rapporteur, who has distinguished between 'the surveillance of communications' which must only occur under the supervision of an independent judicial authority, like our warrant process, versus 'The provision of communications data to the State', which must be 'sufficiently regulated to ensure that individuals' human rights and 'should be monitored by an independent authority, such as a court or oversight mechanism.'

By any definition, the Ombudsman, the Privacy Commissioner and the Joint Committee on Intelligence and Security would constitute, in my view, a fairly effective oversight mechanism. By your own admission, there is nothing that gives rise to concerns that access to metadata in the past has been abused, and nor are we seeking to change the system. We are simply trying to standardise the period by which data is retained. Given that the UN Special Rapporteur on the Human Rights Council distinguishes between pre and post facto, why do you argue that both need that warrant or judicial process?

Prof. Triggs: I will ask my colleague, if I may, who is the senior legal adviser with the commission.

Ms Byrnes: The human rights committee has also recently questioned the distinction between content and metadata. They say that metadata gives an insight into an individual's behaviour, social relationships, private preferences and identity that can go beyond that conveyed by the content of a private communication. So our thinking is that, if a warrant is required for content of a communication and metadata provides an even greater picture than the content of the communications then a warrant would also be justified for that.

Mr NIKOLIC: The Special Rapporteur, as I read the report, distinguishes between the surveillance of communications—that is, entering content of communications versus the provision of communications data by the private sector to the states for the purposes, for example, that the AFP Police Commissioner and others have said they need it to determine pattern of life, to determine pattern of connectivity between individuals and networks of concern to try and respond in an agile way to the threats that are confronting our country from resurgent terrorism and paedophile networks and so on. You have taken a different definition to the metadata.

Ms Byrnes: Yes. The commission was also influenced by the European Union data retention directive decision, which also set out the permissible limits at human rights law for data retention, and one of the reasons why it found that the EU data retention directive was a disproportionate interference with the right to privacy is that it did not have access to an administrative or judicial body. The commission was also relying on that judgement when it suggested that a warrant for metadata might also be something the committee should consider.

Mr NIKOLIC: But your recommendation is not underpinned by a fear or evidence that people accessing metadata previously have behaved in ways—within Australia—that have raised concerns in your mind that they are mistreating that information at the metadata level, rather than the content levels?

Ms Byrnes: No. The commission has just looked at the EU data retention directive and European Union jurisprudence on this topic, as well as the Human Rights Committee.

Mr NIKOLIC: As I read that UN Special Rapporteur's report, I wonder if the bill is inconsistent with that, given the oversight mechanisms in place. But I appreciate your evidence, and thank you so much.
Prof. Triggs: We have relied, as Ms Byrnes has said, reasonably heavily on the very considered judgement of the European Court of Justice, and that is a very powerful decision. It tries to achieve that balance of proportionality and it is certainly a judgement that influences our own suggestions to this committee.

Mr NIKOLIC: Thank you, Professor Triggs.

Senator FAWCETT: Professor Triggs, thanks for your evidence. I want to come back to this concept of the sliding scale—

Prof. Triggs: Yes.

Senator FAWCETT: to understand the mechanics of it and your thinking. I understand that what you have proposed is that, rather than having a set limit, if a significant risk is identified—let us go back to Task Force Argos, which identified a paedophile ring involving children in Australia who were being abused—in such cases we should extend the period of retention. Is that correct?

Prof. Triggs: Yes, that is an example—and it is a very good one, because, as was pointed out, it can take four, five, six years.

Senator FAWCETT: I am just trying to understand how you would see this working. Advice is provided to the police that a paedophile ring has been operating for some months and children are at risk, so the police decide they need to act. They go to your authority and they say, 'We would like to extend the data collection period by a year,' four years, whatever, on a sliding scale—let us make it four years. Who does the authority give them permission to retain data on? I come back to the comment that Hetty Johnston made about this case. She said: Offenders don't fit any kind of stereotype: they are police officers and priests and teachers and charity workers and media people …

There were nurses and others arrested in this case. So we have already reached our six-month point; we are applying for a longer period. Who is actually captured by this longer period? According to this case, it would have to be everyone in Australia.

Prof. Triggs: That is a good example of the difficulty of managing this problem. One might say that that is such a serious offence that it is worth intruding on the rights of others in order to ensure that you can capture those cases. Now, reasonable minds will differ about that. What we are talking about is a period of time. I am suggesting to you that, whatever compromise is reached at the political level, on the assumption this bill goes through, best practice in Europe is a year, but that is not nearly enough; two years may not be.

I am suggesting that, if we had an up-front administrative oversight body, we would have some capacity for that oversight body to take into account the accumulating evidence of the police or other law enforcement agency. They might say: 'All right. The act now says two years; we can accept that. We needed the two years.' But, at the end of the two years, they might say, 'Well, we've got some information here, but it's nowhere near enough to really get to the heart and the full extent of this circle of people we want to know more about.' So we would go to that administrative body and say we want these people under some level of supervision for another year or another two years, and report back to that body—something of that nature.

Senator FAWCETT: But that decision would then apply to every telco, every internet provider, for everyone in Australia who uses their services. At any given time we have espionage cases that ASIO are dealing with, we have paedophile rings, we have drug cases and we have terrorism cases that the various agencies are dealing with. All of those would meet the threshold of serious cases, in which case the sliding scale would be constantly at the five- or 10-year point. That is why I am struggling to understand how your concept would work. Once you have reached the six-month point or the 12-month point, the data is deleted. If you subsequently decide you have information that there is definitely a terrorist threat or something running, you cannot recreate the data; it is gone—even if this authority says it thinks two years or four years appropriate. So I think there is a problem with the mechanics of what you are suggesting.

Prof. Triggs: I think that it needs further thought, and that is essentially what I am saying to you. Whatever you reach as a final result if this legislation passes—whether it is 18 months or two years—I do not think that addresses the problem in an adequate way. Certainly it allows retention for a longer period than would currently be the case, as we have just been hearing from Vodafone. But I think we need a more nuanced approach to how we collect that data for longer periods where it is necessary for serious crimes. It is about the seriousness of the crime and the need for access to that material—the way we need to protect national security and to protect people against criminal offences. I do not think a blanket rule that applies to everything, without some pre-existing supervisory capacity, will ultimately help solve the problem. Indeed, I suspect that we will have thousands upon thousands of complaints and issues going to the Privacy Commission being considered by the Ombudsman and by the Australian Human Rights Commission. So, if one is thinking about red tape and things that are going to tangle...
us all up, it would be far better to have a more sophisticated, more nuanced approach. The technical issues are going to be complex—I am not underestimating it. What I am saying is that I think a rather different frame of reference needs to be thought about here, and an up-front capacity to supervise before you get to the situation where the damage is already done.

**Senator FAWCETT:** But isn't this process that we are part of now an up-front process of supervision? We are dealing with concurrent multiple serious threats, which means we have already passed your threshold for extending time. The community clearly is giving us feedback. Other jurisdictions are indicating that two years is probably about as far as people are happy to go. So this is the up-front process where we are saying there are multiple serious threats that require the retention of data. We cannot isolate and say that pocket of data is what we need to retain for four years because everyone is potentially a suspect when it comes to drugs, espionage or paedophilia, so this is the process. I am struggling to see how another process could be any more robust than the process we are currently going through.

**Prof. Triggs:** The bill will become an act, and your role will be over—apart from, presumably, looking at other amendments to that. So you will have created a process which sets, say, a two-year limit—and that perhaps is the one the community can accept in the circumstances. I am saying that, assuming that passes, it will be helpful to have the additional role of some form of administrative authority that could supervise the access to this data and ultimately extend the period in certain contexts so that you are actually able to deal with the problem of the seriousness of the legitimate aim, if you like, and that would be justified as a matter of proportionality. But the key point I would like to make is that it is European practice, it is the Court of Justice view and it is the commission's view that some form of front-end administrative supervision would be a helpful way of preventing the damage at the end, where I think we are going to see a lot of problems arising in the future.

**Mr BYRNE:** Have you looked at the system the United Kingdom currently has in place?

**Prof. Triggs:** We have looked at it as a comparative exercise.

**Mr BYRNE:** Therefore, what would you say about the single point of contact that is utilised by the agencies and the law enforcement agencies to broker the requests for information with the CSPs, which is your front-end point of contact?

**Prof. Triggs:** I will ask my colleague to answer that question.

**Ms Byrnes:** We have looked at the United Kingdom very briefly in the 2011 European Commission report on the implementation of the data retention directive. The UK does not have a warrant system, but there are other countries in the European Union that do have requests to a judicial officer or senior official, so there is some precedent for having an administrative oversight of a data retention scheme.

**Mr BYRNE:** I am saying the Brits have it. I am saying: could you have a look at it, because it came in with the rushed legislation that was pushed through the British parliament? One of the things that was attached to that was a single point of contact. I am saying you are arguing about front-end administration but there is already one there in the United Kingdom system. Could you have a look at that and report back to the committee and see if that satisfies the concerns that you have? My understanding is that that system has in fact been implemented in the United Kingdom as one of the safeguards to get the stuff through the parliament.

**Prof. Triggs:** We would be very happy to look at that in more detail and come back to you with some information about it and how it has worked.

**Mr BYRNE:** Thanks.

**Senator FAWCETT:** You mentioned restricting access for the data. I wanted to get your sense of organisations like ASIC, who presented first this morning. They currently have access to metadata as part of their role against white-collar crime. They have presented a fairly cogent case to the committee, saying why they should be included in the bill as an agency. Would you support groups like ASIC being included in the bill as being given access to the data?

**Ms Byrnes:** We have not considered the specific question of whether ASIC should be allowed access to data in the retention scheme, but we certainly think it should be refined to bodies who are investigating sufficiently serious crime. So there might be cases where ASIC could meet that definition.

**Mr RUDDOCK:** ASIC gave us evidence that I found very compelling. It related to insider trading and substantial losses to seniors' investments in superannuation where they may at a time when they could never make it up lose all of the provisions they have made for their retirement. As I said, I found it very compelling, and I was hoping you might make the case against it so that I could better understand what the alternative is.
Prof. Triggs: I think the point that we are making is that, where it is a serious outcome, however you define it, that warrants the increased level of access or intrusion of the right. You have mentioned the loss of life. It is perhaps an obvious case that the paedophile ring is another one. This is an interesting one about older people who have lost their savings through insider trading or financial advice that goes wrong. That is a very serious matter, particularly with an ageing Australian population. So, again, it is a subjective judgement ultimately—a political one—but one might say that is a serious matter and should very well balance the intrusion on human rights. But I shall try to think of some anti-arguments.

Mr RUDDOCK: It is nice to know the Human Rights Commission is not arguing against it.

Prof. Triggs: No.

Mr RUDDOCK: I then take you to my next question, which goes to what happens now in relation to the requests to access metadata. My understanding with both law enforcement agencies and security agencies is that, while they do not require warrants, they do have a procedure where senior officers are involved in assessing the material to make a decision as to whether or not they should request that particular data. Is that what you mean by an administrative process?

Ms Byrnes: I think we are requiring some form of independent oversight—something that is external to the agency.

Mr RUDDOCK: So, when we are looking at some agencies that have 60,000 or 70,000 requests, do you have any idea of what the costs of establishing such review arrangements for all of the various agencies might be?

Ms Byrnes: No, I certainly do not have those kinds of figures to hand, but we would be advocating—

Mr RUDDOCK: It might dwarf the retention costs that the providers are suggesting ought to influence this.

Ms Byrnes: Our recommendation is for some kind of independent oversight, but that could be by email or by telephone—something that could be very efficiently run.

Mr RUDDOCK: You do not think it is efficient oversight to have the latter review by the Ombudsman or the Inspector General of Intelligence and Security?

Ms Byrnes: The difficulty with that monitoring system is that it is after the fact.

Mr RUDDOCK: I understand that. But it does give you an indication of whether you are making flawed decisions under the arrangements that we have in place.

Ms Byrnes: After the fact, yes.

Mr RUDDOCK: As I understand it, there is already review of those matters by the Inspector General of Intelligence and Security and no matters have been drawn to notice.

Ms Byrnes: That is true.

Mr RUDDOCK: My principal concern is that your evidence that suggests that metadata is in some way comparable with content. As I understand it, the major purpose for which metadata is sought is to give agencies some idea about where to look. It is in fact about intelligence when they have not been able to get material that would produce a warrant and enable a very thorough investigation. So this is about looking to see who may have been talking to whom and then coming in later with a warrant to see whether or not a fuller inquiry should be pursued. In a sense I am very worried about—particularly in relation to security agencies—they not getting access to the first step, which is the intelligence material that may tell you where it is useful to look.

Prof. Triggs: I think that is a perfectly proper concern; but, as a matter of logic, if you protect content with a warrant, why would you not protect even more powerful information, which is metadata?

Mr NIKOLIC: How is that more powerful?

Prof. Triggs: Because the pattern of behaviour can reveal all sorts of things about a person's life that would not necessarily be revealed in the content of a particular email or text. That is why it is so important. That is why the law enforcement agencies and so on need it. You can develop patterns of relations. You can triangulate information: where they are going, how often they are doing it. You can learn a great deal more from that information than you can in relation to individual content or a series of emails.

Mr NIKOLIC: With respect, the reason why there is a warrant process for content is because it is far more intrusive and revealing. It is the content of information between people. The metadata—if you like, who talks to whom when—is that first cup for the AFP and agencies, as I understand it, to understand the patterns of contact between people of concern. Only when those patterns reveal a need to go further into those people—something comes out of the metadata to say two, three or more people of concern are talking to each other—is a warrant...
applied for that much more intrusive content that they then look into. So I am not sure that is entirely right. I might have that wrong—

**Prof. Triggs:** Let me give you an example. Let us say somebody has a sexual orientation that means they like to go to particular clubs or they meet with certain friends. They make phone calls consistently to particular people as part of their network and do so in a totally legal way. To examine that metadata would tell a great deal about that person and the whole of the social network with which they operate, and it would expose them to an intrusion into their privacy in ways that they may find exceptional.

**Mr NIKOLIC:** How does someone's sexual preference fit the criminal intent of the metadata purpose in this bill?

**Prof. Triggs:** The point I am making is that, when you acquire information of that kind, you are intruding into the lives of ordinary Australians. So that is a very powerful tool to understand not only the personal life of one individual but to link that individual and link their behaviour with many others. For most Australians their linking through metadata will be totally legal, completely inoffensive and no threat to the Australian people.

**Mr RUDDOCK:** Who would be finding out about that? A police officer who is investigating a serious criminal issue who says, 'This person's behaviour is not of concern.' It in fact ensures that a person, when examined, is free from any blame.

**Prof. Triggs:** You would certainly hope so.

**Mr RUDDOCK:** I do not care how many police officers find out who is talking to me, who is visiting me and so on. I am behaving properly.

**Prof. Triggs:** But many Australians would find that an intrusion into their personal lives and their social networks that they would object to.

**Mr NIKOLIC:** The examination is targeted.

**Senator BUSHBY:** But the reality is that the examination would only occur if that person were either a primary person of interest which led to an examination of their metadata to look at their networks or, alternatively, if they came up as one of the people on those networks. I believe that examination looking at that metadata could be used to say that this pattern suggest that this person is involved in this conspiracy that we are looking at or this pattern suggests that this person is just coincidentally relevant to this person. Then you move on. As I understand it, that person's metadata would only be examined if they were that very tiny percentage of people who were associated with a person of interest or a criminal or terrorist issue that arose and they were trying to work that one through.

**Prof. Triggs:** That may be the case as a matter of practice. We will see how many of these matters come before, for example, the Australian Human Rights Commission where people feel that in fact that information has been misused.

**Mr NIKOLIC:** How many of those issues have come to you till now? Apart from restricting the number of agencies, we are not changing the metadata process. We are simply trying to standardise the time the metadata is retained for. As the process has been going over many years, how many people have you had to investigate up till now?

**Prof. Triggs:** I would be very pleased to come back to this committee in the next few days with some illustration. As you know, we get 21,000 inquiries or complaints a year, but I am afraid I am not able to say how many of those concern access to data of this kind. I will certainly find out. We certainly do get a significant number of claims that data has been breached and privacy has been raised. That may be of value to you in thinking about how real or abstract this problem is. But I should also say that what we have just been saying is very much a matter of concern to the European Court of Justice in considering this matter. So we are presenting this to you not as though we are experts on this question but as we are looking at the jurisprudence that has been developed in best-practice nations with comparable legal systems, and it does at least need to be taken into consideration.

**Senator BUSHBY:** Thank you. I think that information will be very useful. One question I was going to ask you was related to that. Given that the proposed bill does not actually impact on access arrangements except to the extent that it actually tightens them up a little bit and provides additional oversight—it does not expand access arrangements—if the bill does not go ahead, would your recommendation that that type of regime be put in place stand regardless given that the authority to access metadata currently exists anyway?

**Ms Byrnes:** Yes, that is right.
Prof. Triggs: Yes, we would accept that. If it does not go through, I think I would like to see a more nuanced approach to assessing this information in order to get to the core of the problem rather than running the risk of intruding in the lives of so many millions of Australians. That is our primary concern.

Senator BUSHBY: You have mentioned on a number of occasions intruding in millions of Australians' lives. For clarification—I am not challenging you necessarily; I am just trying to understand it—how in your view does the retention of the data in an inert, hopefully secure way, only ever accessed for very clear, legislatively controlled purposes, and only for very, very small percentage of the people whose data is retained, intrude on millions of Australians' lives?

Prof. Triggs: The key point is that the data is a matter of personal privacy. When that is being collected and then made available to agencies that—

Senator BUSHBY: Is it the data being made available or is of the retention, or both? You are nodding—I am not sure what the answer is.

Ms Byrnes: It is both, even the collection itself.

Senator BUSHBY: So, in your view, the retention of that data in an inert way, 99.99 per cent of it never, ever looked at or touched, is an intrusion—

Ms Byrnes: Into the right to privacy.

Prof. Triggs: And there is a considerable body of jurisprudence that supports that view.

Senator BUSHBY: So that is an intrusion. Am I right in concluding that it is a fairly small one if it is never—

Prof. Triggs: Exactly, it is a small one, and that is where this balancing comes in.

Senator BUSHBY: And then you need to balance that against the benefits that the law enforcement and security agencies consider exist in that data being retained so that they can then make use of that for serious criminal investigations and terrorism investigations.

Prof. Triggs: And that is why we support the passage of the bill. That is our core position—we support it—but we are simply raising for the committee's interest—

Senator BUSHBY: Yes, a consideration that we need to look at.

Prof. Triggs: Our job is to help. This is not necessarily—

Senator BUSHBY: I am not trying to be combative today.

Prof. Triggs: No, thank you very much. I am mightily relieved, I have to say! But we do look at the jurisprudence, we look at what is going on in Europe, we look at what best practice is and we look at the views of many people, not all of them. The rapporteur's is an important view—this is all evidence for you to take into account. We are simply putting this on the table, but we would love to give you a bit more information, if we may, about the convention and about our own data in terms of levels of complaints and concerns within the Australian community. As you may know, we do settle about 70 per cent of these matters, so they never go out into the public arena; they are confidential. But we can certainly talk about the data.

Senator BUSHBY: I think that deals with the issue of access. Regarding your sliding scale or the time for which the data is retained, you made a suggestion which Senator Fawcett went through with you a few minutes ago. I still do not quite understand how it might work given the evidence that we have received from the law enforcement and security agencies. My understanding is that generally what will happen is that they will get a snippet of information. They will be informed through their own surveillance or their monitoring of individuals in a terrorism situation that something is afoot. They may be informed by an international law enforcement agency that they have come across some activity in Australia involving certain persons. They then look at these people, and one of the tools that they use to commence that investigation is to examine metadata. The metadata they look at is not the metadata from that day on; it is the metadata from that day backwards, which they use to try and piece together a picture of what those people might have been doing and who they might have been talking to and try and establish whether there is a conspiracy et cetera. That is why the time line for how far back you go is relevant. We have heard evidence that 90 per cent of relevant stuff happens within one year, but there is 10 per cent that extends further. That 10 per cent might be more important, it might be more egregious and it might not be, but there is probably a mix.

Your sliding scale suggests that you look forward and I do not really understand how that will work. As I understand it, once a person becomes a person of interest and they start accumulating the evidence against them, that is when the warrants—the more intrusive elements of their investigation—come into play, because they have some evidence. But looking back on the metadata is actually part of putting together the jigsaw puzzle to work out
who might be involved in these activities. It might be to identify who is behind an IP address that somebody in a law enforcement agency in another country said was accessing a child exploitation site. Going backwards is where it is important; it is not going forward where they get most of the benefit. How would what you are suggesting work with that, or could it?

Prof. Triggs: Ms Byrnes, please interrupt me, but let us assume that the law is passed to provide a two-year retention period and the law enforcement agent comes to some form of administrative body and says, 'The two years have given us the beginnings of some worrying indications of a serious criminal matter,' however defined. 'We can keep an eye on these people, but we would like to be sure that the data in relation to these kinds of people or these kinds of activities is held for more than two years, because we don't want it to drop off at the end.' So, if you move forward in time, your two years keep dropping data off the end. They may very well come to the agency and say, 'We really need to keep not only the existing data but for the next year or so we'd like to just consolidate this because we think this ring is more extensive in another country,' or, 'We want to know more about it. We want clearer evidence. If you want a conviction, we need better evidence.' They will be compelling reasons for saying we will require the retention of that data for three years or four years, but we have to do it very secretly, very quietly and confidentially, in order to get to the outcome. That is the kind of flexibility that I think probably needs to be built into the system.

Senator BUSHBY: I think that is a constructive suggestion. I guess it comes back to Senator Fawcett's line of questioning about which data you keep. If you become aware that one person might be involved in criminal activities, you might look at their metadata and identify another five people who match up somehow, using the techniques that they use. There may well be more, but you do not know which metadata to keep to identify that issue.

Prof. Triggs: That is right.

Senator BUSHBY: I imagine that, once you have those five people, there are other powers that the law enforcement agencies have to retain the data for purposes of prosecution and so on down the track.

Prof. Triggs: Yes.

Senator BUSHBY: It is more about what else might be out there linked to what we know that metadata would be useful for to find those linkages.

Prof. Triggs: That is right. I fully appreciate that I do not have all the answers to these technical questions. But I guess what I am saying is that, if you are going to deal with the seriousness of the issue and the need to have evidence that may be required over a longer period, that should be part of your considerations. There needs to be flexibility built into it. Again, that body would then learn as we go with this massive range of data. The advance of technology is such that what we are talking about today is, I understand, going to be very different in five years from now.

Senator BUSHBY: No doubt.

Prof. Triggs: So we do need a flexible capacity. But also, dealing with your question, wouldn't it be useful to have a small administrative body that could follow this through, follow the data and technology changes, and tweak it and make suggestions so that they are meeting the proper needs of our agencies in protecting Australia and obviously whether it needs to be protected? Maybe if this bill goes through there will be a capacity to develop these other safeguards as we go along, which would be encouraging.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. We would appreciate the additional material that we have discussed. If the committee has any further questions, the secretariat will write to you. Thank you very much.

Prof. Triggs: Thank you.
CLARK, Ms Narelle, Deputy Chief Executive Officer, Australian Communications Consumer Action Network

PAVLIDIS, Ms Katerina, Grants and Research Officer, Australian Communications Consumer Action Network

Chair: I now welcome representatives of the Australian Communications Consumer Action Network. Although the committee does not require you to give evidence under oath, I remind witnesses that this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Ms Clark: Yes, and I will try and keep them as brief as possible, considering the time.

Chair: Great—thank you.

Ms Clark: In fact, I am quite happy to have ceded some time to the Human Rights Commission because that was indeed very interesting. I think we would like to lend our support to all of that submission. It was very well argued and put a very similar position to our own in many respects. Once again, thank you for the opportunity to present today.

To open, we welcome the effort to reform the Telecommunications (Interception and Access) Act and consider it timely, as the previous inquiry conducted by this committee exposed a significant number of agencies able to access data on individuals and exposed variability across the different telecommunications providers and inconsistency between the providers as to what data was retained and what access was being given to a range of agencies or not. I think the previous inquiry exposed the extent to which data is potentially not being retained that is perhaps being claimed to be the case today, and this bill does indeed bring about changes to the existing regime. So we welcome efforts to standardise the data held and restrict access to a named group of agencies. However, we caution the committee to further ensure that this access be for serious offences, as defined under the Telecommunications (Interception and Access) Act.

We remain concerned also that there has been insufficient engagement with consumer representatives in the examination and information being brought to this review. From my understanding, the PricewaterhouseCoopers work and the working group has not had any consumer involvement in it whatsoever. If we refer back to the report provided by the Attorney-General's Department, just recently tendered to the committee, Report 1 of the Data Retention Implementation Working Group, it outlines that there were very small number of parties involved with the review of this effort and the review of the dataset involved. It includes the Secretary of the Department of Communications, a number of law enforcement agencies—and of course we support them and we support their work throughout this process—and senior executives of Telstra and Optus and the CEO of Communications Alliance, which is an industry body. So there has been no consumer participation in the review of the specifics of any potential dataset to be defined throughout this process.

We already see many consumers going without to pay their phone and internet bills, and so we are very concerned about the level of cost that may be associated with this system. I think you have heard plenty of evidence, and we have heard more today, about the costs associated with this particular scheme. Costs outlined in previous inquiries have shown significant costs, of the order of potentially hundreds of millions of dollars across the sector, and iiNet stated that it would result in an approximate cost of between $5 and $10 per service per subscriber. We do not think that consumers are prepared to wear these costs, so we are very concerned that this will cause a distortion within the marketplace and make things very, very difficult for consumers.

We are also concerned that this cost containment will not be guaranteed, given that the dataset will be defined in regulation rather than in legislation. If that the dataset is defined within legislation, there should be greater clarity over what precisely will be retained, by whom, where and what the processes are to access that data. If it is defined by a regulation, consumers have no guaranteed participatory processes, and the powers of the Attorney-General to extend that through legislative instrument rather than through legislation mean that these costs could potentially blow out.

Our recommendations go to both of these issues and we request that the dataset be set out within legislation. We also request that the powers of the Attorney-General be further contained so that changes to the list of agencies that are able to access this data or changes to the regulation defining the dataset must be made through
legislative changes rather than through a legislative instrument or through regulatory changes, which we may or may not be able to access.

Now, I do not think we really have the time today to go through the lack of clarity in the dataset. There are some aspects within the legislation at this point in time that I find extremely troubling, particularly as somebody who has spent many years as an engineer building these sorts of systems in my telecommunications professional life. We are talking about communication, yet communication is something that is not clearly defined here. I can make a communication by writing something down and passing it to my colleague, or I can do it through the means of guided electromagnetic energy, or I can do it by flags on a hill. There are a number of different ways by which I can do this. In a telecommunications network, communication happens at all sorts of different layers of a system. And a consumer may not be a party to any of those individual layers of the communication. So, very, very rich amounts of data can be collected and gathered.

One example I think, which is not clear within here, is the case of a consumer with a wi-fi enabled handset. If an internet service provider is providing a wireless internet service provider network, then they will be covered under this act, because they are captured under schedule 5 of the Broadcasting Services Act. Yet if another type of party provides a wireless network, they will not be covered. So, there are all sorts of systems and services that will be in or will not be in, by whom and by where. There is a distinct lack of clarity here.

Mr RUDDOCK: Could you just elaborate on that? I am not sure I understand 'in' and 'out', and I might want to ask some of the other agencies about whether your understanding is in fact accurate.

Ms Clark: Perhaps I could just check: which aspect of that do you want me to clarify?

Mr RUDDOCK: You have said that some wi-fi providers are in and some are out. The only thing I know about wi-fi is that you try to find out at a hotel whether you can get wi-fi—that is about the only thing I know!

Ms Clark: That would be a good example. The hotel wi-fi service would not be included. Yet Telstra's commercial wi-fi service, which it provides at coffee shops and which it used to provide at airline lounges—but I do not believe it does anymore—would be included, because Telstra is a telecommunications services provider under the act. Yet a hotel wi-fi provider or a shopping wi-fi provider would not be included—or potentially would not be included. If I am wrong, that is—

Mr RUDDOCK: Well, I do not know. The only ones I heard that missed out—and I am told I misunderstood it—were internet cafe providers. I was not aware that anybody else had been left out, and I was keen to get them in, but my colleague says that I misunderstand it all.

Ms Clark: Then I would suggest that there is a lack of clarity, both in the bill and in the definitions that run between the various acts.

Mr RUDDOCK: So, when I am questioning them I would be asserting that hotel providers, internet cafes—which we were told were left out—and shopping centre providers are not in, but Telstra is.

Ms Clark: That is my understanding of it, yes.

Mr RUDDOCK: Thank you.

Ms Clark: I was going to spend the time going through some of the recommendations that we have made within our submission. I am happy to cede that time, if you want to go through any of our recommendations.

CHAIR: I think they are all there for members to read, or have probably been read. There are a number of them—14, I think. So, is there anything else you would like to add, Narelle?

Ms Clark: There is one final thing and that runs to the experience that consumers have had with data breaches in the telecommunications sector over the last few years. I think one of the other people who appeared before you today did refer to hacks by unknown agents on Sony. We have had a very significant history within this country of telecommunications service providers' data being exposed in the public domain. We assert that consumers are very concerned about this level of data breach and that these breaches are not necessarily well managed or well notified to the customer base. With this particular type of system where there is a significant amount of data—and we also contend that metadata is rich data—it will be very attractive to players. Thank you for your time.

Mr RUDDOCK: I have never had a constituent come to me and complain about telcos having breached their metadata.

Ms Clark: We have certainly had consumers come to us concerned about data breaches.

Mr RUDDOCK: I am a member of parliament and, in 40 years, I have never had somebody come to me to complain, so I am trying to get into my mind to what extent it is a reported problem.
Ms Clark: I can only refer to the Office of the Australian Information Privacy Commissioner, who received a record number of data breach complaints against government agencies and private companies over the last few years. That is probably the best data for me to refer to at this stage.

Mr RUDDOCK: We had him before us and he was not adducing that sort of evidence in the context of this inquiry.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.
AYNSLEY, Ms Brenda, President, Australian Computer Society

CHALMERS, Mr Athol, Manager, Federal and State Government Relations, Australian Computer Society

[17:02]

CHAIR: Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. 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. Do you wish to make some introductory remarks before we proceed to questions?

Ms Aynsley: Yes, please. I want to thank you for the opportunity to appear today before the committee to give evidence in support of our submission. Firstly, by way of background, the ACS was formed in 1966, so we are approaching our 50th anniversary next year. ACS is Australia’s peak body for ICT professionals. We have almost 22,000 members nationally and a core function of the ACS is the assessment and certification of our members as technologists and professionals. To retain professional status ACS require certified members to undertake annual ongoing professional development activities. ACS also conducts research-based advocacy on behalf of members on public policy issues relating to the digital economy and the impact of ICT on productivity growth and standards of living in the Australian economy. As a vendor neutral organisation, with no direct commercial interests in particular technology products or services, the ACS is able to provide a genuinely balanced view with a focus on good public policy outcomes.

ACS is also a member of the International Federation for Information Processing, which represents IT societies from 56 countries and regions, covering all five continents, with a total membership of over half a million.

Currently, I have the privilege of being the Chair of the International Professional Practice Partnership, which is a subcommittee of IFIP, which is leading international efforts to define minimum standards of professionalism in ICT and to establish supporting infrastructure amongst stakeholders and partners in government, industry, education and community.

The ACS supports initiatives that will assist Australia’s law enforcement and security agencies to more effectively address serious criminal behaviour and other activities that threaten Australia’s national security. As noted in our submission, in the 35 years since the original Telecommunications (Interception and Access) Act 1979 was enacted, communications technology has advanced significantly, which makes the role of our agencies even more challenging. The internet is a core part of our daily lives. The power, the capability, functionality and range of communications of ISIS are increasing dramatically. Social media and other communication mediums abound and we have a population which has high digital literacy and 24/7 access to communications devices and platforms. The ACS acknowledges that there is a need to ensure our law enforcement and security agencies have the tools to operate effectively in this digitally-powered environment.

To this end, the ACS supports the intent of the bill and will happily leave to others the arguments relating to the bill’s details, which we have seen evidence of this afternoon while we have been here. The principal issue that this bill raises for the ACS is the implications of the bill at an operational level. A mandatory data retention scheme will require telecommunications companies, internet service providers and the various law enforcement agencies to build systems to capture, store, retrieve and analyse the metadata. These will be software based systems built and, to a large extent, operated by ICT practitioners. The very sensitive nature of this data means that we need to trust that these practitioners will operate with the highest standards of ethics and professionalism.

We need to be confident that important privacy and security principles are not breached. Breaches will heighten concerns which already exist in the community about this legislation and will therefore potentially undermine the government’s efforts to provide agencies with the tools they need to fulfil their roles. We have heard this afternoon and I am sure you have heard on many occasions on which you have sat of the fear, uncertainty and doubts that exist in the minds of those who have appeared before you and those who have reported on your work. So for the very same reasons that there are well-established processes, systems and standards in place to ensure the highest levels of professionalism and ethics amongst our doctors, lawyers and engineers so, too, do we now need to start regarding elements of ICT practice in the same way. Information and communications technology is now pervasive. It underpins virtually all of our businesses, our transport systems, our energy systems, our critical infrastructure, important health products and so on. It sits at the core of most products and services we now consume. So as a society we now need to be thinking of key parts of ICT practice in a different way.

Breaches of professionalism standards by ICT practitioners in today’s digital world can have very serious consequences for individuals, businesses and governments. This is the core issue for the ACS as the peak body for
the ICT profession and whose principal objective is the advancement of Australian ICT resources. Those who have yet to engage with ACS are aware of the need for professionalism in their work. We are also working to raise awareness of this issue both domestically and internationally through our peer societies around the world.

I am happy to expand on our work in this area if the committee so desires and I want to thank you for the opportunity to appear today.

CHAIR: Thanks very much. Any questions? I have one question. In your submission, at ‘3.2.2—Content is Undefined,’ you say:

The Bill specifically excludes ‘content’ from the scheme but ‘content’ is undefined.

You then give an example, which the Parliamentary Joint Committee on Human Rights uses, which is metatags by website developers. Do you have an example of a definition of content that you think would be applicable?

Ms Aynsley: I have been party to the discussions on defining content since the seventies. I do not have a problem with the accepted definition in use today. ACS does not have a view; my own view is that I am happy to accept the current definition of content, but metadata is not content in that sense.

CHAIR: Would you just expand on that. If we were to do something in this area, what is the definition of content that currently exists?

Ms Aynsley: The definition of content that currently exists is the one which the Human Rights Commission was talking about earlier—a warrant and authority process that is required before one can examine content. At the moment, there is no suggestion for having this for non-content, this metadata, and yet metadata, I am sure you have heard, in and of itself includes some content that is personally identifiable and that is able to be linked, though not in all cases, as we heard from the representative of Vodafone today. An IP address today is my IP address, but in a dynamic world it might be somebody else's address tomorrow when they connect their modem to the internet. So metadata can be content; we just need a clear definition from the committee on what is content, what is metadata and what the distinction is.

CHAIR: So you are really not saying that content is undefined; you saying that metadata is undefined.

Ms Aynsley: Exactly. There is a certain lack of clarity around what is meant by metadata and where it ends.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.
FONG, Mr George, President, Internet Society of Australia  
PATTON, Mr Laurie, Chief Executive Officer, Internet Society of Australia  
RAICHE, Ms Holly, Chair, Policy Committee, Internet Society of Australia

[17:13]

CHAIR: I welcome the representatives. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is serious and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Patton: Firstly, we would like to thank the committee for the opportunity to present the views of our members in relation to this very important legislation. The Internet Society of Australia, also known as ISOC-AU, is the Australian chapter of the worldwide Internet Society. Our mission is to promote internet developments for the benefit of the whole community, including business, educational, professional and private internet users. As such, we are the umbrella organisation representing the interests of everyone who uses the internet. Many of the organisations that have already appeared here are very closely allied with us and work very closely in that relationship.

Our members hold a wide range of views about the way in which Australia can best benefit the internet. However, all of us believe in the fundamentally positive role that the internet is playing and the need for an open, accessible and trustworthy internet. Globally, the Internet Society coordinates the development of internet policy and technical standards. This includes advising the United Nations and internet management organisations such as ICANN, the Internet Corporation for Assigned Names and Numbers. The Internet Society is responsible for the Internet Engineering Task Force. The mission of the task force is to make the internet work better by producing high-quality, relevant technical documents that influence the way people design, use and manage the internet. So, it is our conclusion that the Internet Society is well placed to offer independent technical and policy advice to the committee and to the government. In a moment I will hand over to my colleagues, who will happily expand on our submission, but please let me begin by restating the position outlined in our submission very briefly.

The Internet Society of Australia contends that the data retention legislation as it is currently drafted simply will not achieve the government's stated aims, while constituting a serious threat to existing civil rights protections. We understand the government's concern to find effective measures to deal with national security. However, we argue that the bill is deeply flawed, its coverage is unclear and it does not reflect the complexity and diversity of internet communications. It will add significant costs to service providers, which will undoubtedly be passed on to consumers, and will seriously hamper competition. Significantly, it will not reach some offshore communications services widely used by many Australians, potentially providing a loophole capable of exploitation by precisely the groups and individuals the government seeks to target for surveillance. The bill represents a challenge to the right of Australians to the protection of private information. This has the potential to reduce the confidence that Australians have in their internet use.

In conclusion, there are three areas in the bill that are drafted very broadly and that we believe should be redrafted: the definition of the data that is to be retained, the agencies and the organisations that will have access to the data, and the grounds on which access to that data will be granted. As I have indicated, we represent and have among our members people with considerable technical and policy expertise. We would like to offer that expertise to the committee and, through the committee, to the government, and we would, respectfully, ask the committee to encourage the government to take up our offer. Thank you.

CHAIR: Thanks very much.

Mr RUDDOCK: You made that offer already.

Mr Patton: Yes.

Mr RUDDOCK: To the government.

Mr Patton: Yes, to the Attorney-General's staff.

Mr RUDDOCK: I do not know whether anybody else wants to have a go, but I have only one other question.

CHAIR: Okay.

Mr RUDDOCK: Is offshore operations the only loophole that you actually identified? I do not know whether I would want to publish it; I do not know that I would necessarily want to draw attention to all the people of concern. But those loopholes—
Mr Patton: Which is why we are offering to work with the committee and with the government. I do not think we really necessarily need to highlight the inadequacies.

Mr RUDDOCK: Well, I would be interested in identifying the areas that you think the legislation does not cover.

CHAIR: We could take that in confidence—in writing, in confidence.

Ms Raiche: May I talk in confidence?

CHAIR: No; this is a public hearing.

Ms Raiche: All right; I will give a brief overview. And I think my first comment is that given many of the technologies that exist now that are not well accommodated by 1997 legislation, there are going to be some loopholes. Now, the loopholes are already in our submission and therefore are public anyway. Some of the problems are simply about drafting, and they can be easily corrected—for example, the drafting about the service providers covered. The way it is written now, it looks as if it is only carriers as infrastructure owners and ISPs, and that leaves all providers of telephony that do not also provide internet access not covered by the bill. That is not intentional. If you read the Attorney-General's submission, they do not believe that is what they have come up with—but they have. I do not understand that. Bad drafting.

Another is an 'immediate circle'. Really, this is an answer to your question to ACCAN, which is: 'Who is covered?' The explanation in the Attorney-General's explanatory memorandum is that it will be difficult to unpick the commercial relationships that underpin what is conceptually an immediate circle as defined in the Telecommunications Act. Parliament House is an immediate circle. The Commonwealth Bank and all of its branches is an immediate circle. Libraries and universities are immediate circles as defined in the Telecommunications Act. In that situation, they are provided generally by a service provider under contract with a particular firm. So those are in one sense commercial agreements that you do not unpick. Another aspect of that definition which is involved in the term 'supply to the public', which is section 44 of the Telecommunications Act, is the reason that some of the cafes are just plain not covered. So in some cases we are dealing with definitions in the Telecommunications Act that mean some areas are not covered. If you read the Attorney-General's submission, they are relaxed about some of that. They understand the difficulty in covering some of this, but I think some of the drafting could be better so as to close some of those loopholes. I would be completely happy to go through and say, 'Clean up some of this wording.'

Mr NIKOLIC: I have a follow-up on that—and I will just ask for the bill to be brought to me. The data retention bill refers to 'carrier' but it is then further defined in the act as a 'carrier' within the meaning of the Telecommunications Act, the 'carriage service provider'.

Ms Raiche: I will explain why there is a difficulty. Under section 5 of the telecommunications——

Mr NIKOLIC: Sorry, I can't hear you.

Ms Raiche: I have a soft voice until I actually lecture. Under section 5 of the Telecommunications (Interception and Access) Act, the definition of 'carrier' is said to include 'carriage service provider'. Okay, that is a choice that the drafters have made, but then when you come to section 187A where this is the bill, then the bill is said to cover 'carries' and 'internet service providers'. If they had just said 'carrier', you could say, 'Okay, that definition covers carries and carriage service providers,' but, because they have said carrier and ISP as defined under the Broadcasting Services Act, the way a lawyer would read that and the way a court would read that is: 'Why haven't you used the term 'carriage service provider'?' That term is what is in the Attorney-General's submission, but it is not used here. It is the way it has been drafted; they have not used the very definition that is in the act, which I do not understand. I read this and I do not understand this drafting.

Mr RUDDOCK: There are other examples where you can give us in writing where it is undesirable that we in fact publish them to draw to others' attention that these may be the loopholes they could avail themselves of.

Ms Raiche: My pleasure.

Mr Fong: For the benefit of Mr Ruddock, prior to this you were talking to my colleague Narelle Clark about the uncertainty about Wi-Fi cafes, internet cafes, and things. The Attorney-General's submission on page 24 reads:

Second, data retention obligations will not apply to services that are provided only to a single place, or to places in the same area, such as free Wi-Fi access provided in restaurants, libraries or a campus. This exception reflects an assessment that the law enforcement and national security benefit of imposing data retention obligations on these services would be outweighed by the privacy and compliance burden.

The submission goes on to say:
However, some key non-content data relating to the communications made from internet cafes will be retained by the internet service providers, supplying those services to the internet cafes. This will assist with any authorisation requests issued by agencies seeking to advance their investigations.

My role in the Internet Society on this particular issue, in the task force we have set up, is primarily technical. One of the things I also look at—as a service provider myself in a private capacity—is the fact that the legislation contemplates a situation where, if other people are providing those services, as a service provider I do not have to collect the metadata in relation to that. Now, the problem with that is the wi-fi: is the cafe providing the wi-fi access or is the service provider itself providing the wi-fi access? If it is the latter, then it is likely that it is responsible for picking up the metadata. If the cafe owner is operating it, then the service provider has no obligation to collect the data; and of course the cafe is not a service provider, so the data is effectively not collectable.

That is a fairly well defined example, the cafe—small, quite isolated. But, when you get into the position of looking at supermarkets and university campuses and things like that, we are talking about much larger entities where effectively you are running, in the case of a university campus, almost a small city. We would regard that as something of a loophole that should be looked at quite closely.

The prospect of a number of different providers as well, at a much more serious level, could result in that data not being collected. I can give you the example of corporate services. Many people are aware of the fact that corporates run their own mail service, and it is possible, the way the legislation is drafted, that internet service providers provide the connection but are not actually providing the service at the end, which means that that internet service provider or carrier does not have to collect the data. This is a predicament that I face as a small provider. Again, there is the same problem. There is no obligation to collect the data from the corporate exchange server that might be at the end of that, so the service provider sits back and says, 'I don't have to collect that data.'

The variables in terms of those types of scenarios are quite significant, and we believe that, in the old, traditional legal sense, you could drive a coach and horse through a number of those scenarios, which would cause some issues, especially when it comes to public wi-fi access. That sort of technical issue, I think, can be resolved in the legislation, but there needs to be some technical consultation with people like us to work out what those issues are.

Another example is the collection of logs. One of the things that our little operation does—and we are a very small operation—is have mail logs. In the case of the mail logs, 90 per cent of any email that is sent to our system is rejected as spam, and the reason it is rejected is that there are what are known as real-time black-hole lists around the world. Those black-hole lists are fairly simple; they are lists of IP numbers that are updated hourly. So, if a piece of mail comes to our server and they knock on the door and say, 'We'd like to deliver the mail,' the first thing our servers do is check them against the database: is this person a spammer? And we will know by the IP number. If that piece of mail is from a known spam source according to our database, the mail is rejected and it never reaches our system, but the metadata with regard to the actual instance of that negotiation is kept. Now, 90 per cent of our mail logs contain information about spam. Some of that metadata includes URLs because the spam providers will very often say, 'If you want to check why that has been rejected,' and actually put a URL in the header. Under the legislation, that URL is not required. In fact, the legislation specifically says, 'We are not collecting URLs.'

So, if an enforcement agency came to my office and said, 'We need to see your metadata,' part of the problem is that I would have to separate that data out from the logs, and that is not an insignificant technical task, given the amount of metadata that is generated—five to six lines a second in some cases, at peak hours during mail services. So there are some technical issues there that we think need to be looked at very seriously because they have practical implications for whether the law can be enforced in a practical way. As my colleague Laurie has indicated, the Internet Society is very keen on being able to perhaps provide some of the technical assistance in that process.

Mr RUDDOCK: In terms of the timing, what you are referring to are amendments to the legislation, not the subordinate regulatory arrangements. You could not fix it through regulations, could you? Are you talking about amendments to the legislation or matters that we could deal with through regulations? Regulations are going to come later. In terms of whether we want to get the legislation through in, say, two weeks time, when the parliament is back—

Mr Fong: I think we are looking at the big picture here. I think that within the bill itself there are some fundamentals that have been set up that are possibly going to be difficult to fix by regulation. Some of those fundamental processes need to be addressed first before we can then move on to regulation to say, 'Yes, we can do that.' Again, an example of that is what data is captured; who is a service provider and who is not; and, if that
service provider is providing a service that just happens to pass the packets through, who on the other end is caught.

Mr RUDDOCK: I suppose I am looking at where the government is. The government wants to get this through when we come back, and it wants us to report on it. I am anxious that we should look at the issues you are raising, but I do not necessarily want to see the whole legislative package derailed. So are there any matters that you could look at through further amendment?

Ms Raiche: Yes.

Mr Patton: I think some of the things that we are talking about are certainly in that category, but I think there are some fundamental parts of the bill that are beyond being sorted out by regulation.

Ms Raiche: Let me first answer your question in terms of just the coverage of a carriage service provider. We have a two-sentence correction to the bill, and there would be things that are in the bill now that could be changed in the bill, and those could be easily forwarded. On some of the other issues we have, yes, the bill could be amended. There would be more implications from doing it. There are some difficulties.

For example, we are talking about, I would have to say, a very badly worded section in the bill that talks about, I think, excluding providers that are based overseas, but I think the infrastructure is here. I have read that sentence about five times, and I have come up with about three meanings. It is not clear to me. I would like to redraft it once I understand it. My impression is that it will be difficult for this government to actually regulate some body that is based overseas. However, you can incorporate regulation for an entity that has a basis in Australia. You could redraft the sentence that is here to make it clear what you are after and make sure that it is possible to get the bodies that, in fact, have a presence in this country. For example, the Broadcasting Services Act has some hints on how you do that. So there are things in the bill that could clarify how you would address the issue of somebody that may be based overseas but also here, recognising that, if that is a completely foreign presence, you would have a jurisdictional issue. We realise that that is a hole which will be difficult to plug if there is not an Australian presence. So then you would look to, say, the Broadcasting Services Act, where in fact the provisions talk about cooperation with overseas agencies as the way to deal with that. So there are those sorts of things that you could do with this that would improve that.

Mr RUDDOCK: I hear these points, and now I go to the question of how you made your offer to the government. Did you speak to the minister and hear him say, 'Look, I'll have somebody talk to you'?

Mr Patton: No.

Mr RUDDOCK: Or did you put it in writing? Have the people who are drafting the legislation turned their minds to these sorts of questions you have raised? I am just trying to get how you have made your offer.

Mr Patton: The answer is that I have emailed the deputy chief of staff to Senator Brandis.

Ms Raiche: And we would be happy to follow that up.

Mr Fong: We are also in constant—

Mr RUDDOCK: Has somebody talked to you after that email?

Mr Patton: No, I have not heard back yet.

Mr RUDDOCK: How long ago was it?

Mr Patton: It would have been late last week, from memory. But we have had previous meetings.

Mr RUDDOCK: So, a week ago—late last week is a week ago!

Mr Fong: We have had contact with members of staff and some members of parliament from both sides of the House to offer our assistance on a regular basis, where we can. That has gone back probably over the last three or four months. We have spoken to Mr Turnbull's office and his chief of staff—we meet him regularly. We did in fact spend some time in August writing 10 questions, with a fair detail of explanation, as to what we were asking, and why, about the legislation. We did follow up and ask if we could address those issues and perhaps discuss them. There has been communications on both sides of the House for that. The responses have been variable. I understand it is a busy time in parliament and obviously not everybody can be seen. But at the same time we have made concerted efforts over the last three or four months to ensure that an even-handed approach to all sides of the House has been made. An offer to assist where we can has been made at that level.

Mr BYRNE: Have you approached any members of the committee? You were saying that you have been in contact—

Mr Patton: Not specifically in relation to this hearing, but we are generally in conversation. If I could just make the point that, apart from me, the organisation is staffed by volunteers. So we have spent a considerable
amount of time, particularly Ms Raiche, in writing the document. It really was very late that we got the document finished. To come back to your point, Mr Ruddock, it was really only last week that I think we came to the conclusion that the best thing we could do was to offer the technical advice from the committee—

Mr RUDDOCK: I hear that. You have written to the minister and at this point in time the people who are in the department who draft these matters and are across them may not have even turned their minds to the issues you are raising.

Mr Patton: No, and that is why we are keen to offer our services.

Mr RUDDOCK: My question is that if the government is initially keen to get this through, in two weeks' time, can these matters be dealt with by further amendment later.

CHAIR: No, we do not report until the end of February.

Mr RUDDOCK: So you are not going to get it through for next week! I am a bit disappointed.

CHAIR: We report by the end of February.

Mr RUDDOCK: I thought this legislation was urgent and pressing!

CHAIR: Unless the Chief Government Whip has taken matters that we are not aware of into his own hands!

Mr Patton: If I were the Attorney I probably would have!

Mr Patton: The essence of the point we are trying to make is that we are keen and available to assist. As far as we have been able to do so, we have been frank and honest in terms of our own opinions and concerns. Certainly, the Internet Society is not made up of just the three of us there. There is a board of 13, and other members. They have all put their hands up to say—

Mr RUDDOCK: If you had not gathering it, your submission impresses me greatly. I am fairly naive about these matters, but it does impress me greatly and I would be encouraging people to speak to you as quickly as possible. That is where I come from—

Mr Patton: Thank you very much—

Mr RUDDOCK: Maybe informally, but they seem very cogent and very appropriate to be considered by me.

Mr BYRNE: To back up what Mr Ruddock is saying, in addition to what you might give the committee if you could give a document to the chair. He can distribute that and we can make sure the documentation is passed on to the Attorney-General's Department, and the office as well. It is two measures. Along with Mr Ruddock, we are quite impressed with what we have heard and we are very keen to hear more from you.

Mr Patton: With respect, we are happy to do that, but I would have thought that as a starting point our submission is fairly detailed. I think our submission would probably prompt a two-way discussion. We are certainly happy to provide more information. We are happy to provide people to come and speak and discuss matters, but in the first instance I think it would be good if the committee could pass on to the government the suggestion that they might read our submission in preference to some of the others!

Mr CLARE: I think you can rest assured that after the evidence you have given today they would. I think it would be extremely embarrassing for the government if legislation passed the parliament and then evidence that was given to this committee before it was passed was subsequently revealed to be correct—that there were loopholes that you, Mr Fong, described that you could run horses through. So it is in the interests of good public policy that these concerns are brought to the drafters' attention. Tomorrow the Attorney-General's Department will be before us and one of the questions that I will be asking them is if they are aware of your submission, their initial thoughts on it and whether they intend to sit down with you and go through the concerns that you have identified and see if they can be addressed prior to, one, this committee reporting and, two, the bill being debated in the House.

Ms Raiche: Could I just repeat: there are things that can be fixed, but there have obviously been some policy decisions in respect of whether or not you really want to go after companies in foreign jurisdictions and how you would want to do that. I guess my point, I repeat, is that the Broadcasting Services Act does suggest a way. Immediate circle is another issue where the Attorney's submission said, 'Yes, we know this.' The examples they gave were that libraries and universities already cooperate with us, but we are not talking about just libraries and universities; we are talking about any big corporation. So it is a larger problem than was suggested in that submission. We are saying that every large corporation will have its own network, and that is a private network. It then becomes a policy choice: do you want to unravel some of those circumstances? You have in the bill allowed for the identification by the communications coordinator to name immediate circles if there is a problem, and that may be sufficient, but I would say maybe there is a test that surrounds that that could be strengthened. There are
things like that where a policy decision may have been made—I am not sure it has been made well and I am not sure the alternatives have been thought through. Those of the things that, when I was reading it, were troubling, frankly.

Mr Patton: By way of a concluding remark, if I may, I have only just recently taken on this role and the Internet Society is in the process of, I think, increasing its profile. We would hope that in a situation like this, if it were to occur a year from now, the government and the members of parliament that are particularly interested in this subject would in fact come to us long before we get to the point of going through a bill and identifying its weaknesses. We would like to be in a position to be able to provide strategic advice as well as detailed technical and legal advice, and we have the capability to provide that.

Mr RUDDOCK: Thank you very much. I found it extraordinarily helpful.

CHAIR: If there is a possibility for that confidential information, that would be—

Mr Patton: We are very big on confidentiality!

CHAIR: That would be good. Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.

Mr Patton: Thank you very much.
FLYNN, Ms Julie, Chief Executive Officer, Free TV Australia
HOLLANDS, Mr Mark, Chief Executive, The Newspaper Works
KRUGER, Ms Sarah, Senior Lawyer, Special Broadcasting Service
SCHUBERT, Ms Georgia-Kate, Head, Policy and Government Affairs, News Corp. Australia

Evidence was taken via teleconference—

[17:43]

CHAIR: I now welcome representatives of the joint media organisations. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Ms Schubert: Yes, we will make a brief opening statement. Firstly, we appreciate the opportunity to provide evidence to the Parliamentary Joint Committee on Intelligence and Security regarding the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. As we have outlined in our submission, our concerns regarding the bill are as follows.

First, there is the impact on news gathering, particularly on the confidentiality of sources and inadequate protections for whistleblowers, of large-scale surveillance and data retention. Second is the lack of definite listed agencies able to access metadata. As we recommend in our submissions, the ministerial declaration scheme available to request access to metadata must be based on demonstrated operational need and more particularly for the purpose of law enforcement and national security only. Third is a lack of requirement for a warrant to access metadata. If the committee recommends that a warrant should not be required then another formal authorisation to request and to be granted access to metadata must be developed to ensure appropriate checks and balances are fulfilled. Fourth is the interaction between the three national security bills and the chilling effect on news gathering overall.

We welcome any questions the committee may have in relation to our submission.

Mr RUDDOCK: We have had a lot of discussion today about the issue of warrants and whether there ought to be an independent agency that looks at these matters. The number of occasions in which organisations endeavour to seek access to metadata is enormously large. I do not pretend to understand all of the potential requests, but we are talking about 60,000 requests to one particular agency. If we are going to set up a system, that is going to effectively constrain, I would suspect, the number of requests that might be pursued and sought. As I understand it, metadata as distinct from content is the basis upon which security organisations—those involved in investigating terrorism issues and the like—identify the people who they may need to be able to look at and seek further information on. But it is intelligence rather than evidence that is initially sought. If you do not have access to that, you have nowhere to start your inquiries to actually find out about the matters that are of concern to you. That is how I understand it and how it is put, and I wonder whether or not that might influence the approach that you want to see taken on this matter.

Ms Flynn: I think what we would say is that our concerns are really around the parameters of this. Yes, we are concerned about the need to get a warrant to get this sort of information, but I think we might be a little more comfortable if there were more of a test of what this is about. The act can also cover not just national security issues but also intelligence. As we have seen recently in The Guardian about requests that have been made for information about people who might have been accessing information about immigration issues, I think it needs to be very clear that this kind of process is not available to government agencies who are not happy about what is being reported about them by the press.

Mr RUDDOCK: We had been having some discussion earlier. The legislation makes it clear that the only organisations that can be approved are those that are investigating serious criminal offences as defined in the Telecommunications Interception Act. I do not know that it goes to immigration matters, as you suggested, for instance. I do not know that immigration offences could be included other than perhaps people smuggling. That may be regarded as sufficiently serious to be a serious crime, but it would probably be police rather than immigration that was investigating it and seeking to get access in any event. Given that you also have agencies like the Ombudsman and the Inspector General of Intelligence and Security overseeing the use of these matters and reporting on them, surely that is a safeguard that ought to be satisfactory.
Ms Schubert: I think what is of concern to us is that it does not appear that there are the checks and balances to ensure that the access to metadata that may be occurring is actually for the purposes of law enforcement and national security. If you follow that tree down, the overseeing role of the Ombudsman is based on inspections that he or she may undertake and whether or not the agencies that have access are complying with the rules. It would seem that, without a paper trail, the overseeing function for whether or not that metadata has been accessed and authorised in an appropriate manner and for the purposes that the bill states could not be discharge to its fullest capacity.

Mr RUDDOCK: There is nothing I see that suggests that there would not be a paper trail for the agencies that are responsible for overseeing these matters.

Ms Schubert: Here is what is not clear to us. In the absence of a warrant process, the process is not clear that there would need to be an authorised application made to be able to access that data for the purposes of law enforcement and national security. It may be that we have—

Mr RUDDOCK: I suspect you probably have. My understanding when I was the Attorney was that there were procedures in the security agency to ensure at a very senior level information that was being sought was for a proper purpose in investigating either counterterrorism or national security issues. Equally, as I understand it, each of the other agencies have to have appropriate senior staff that vet it. Under this legislation that we are now considering, the range of organisations that are going to be able to get access is going to be very seriously limited. There are organisations that for law enforcement purposes—that is, councils that need to enforce their rating arrangements—have had access before that will no longer have it. There are organisations dealing with animal welfare—a very serious issue; I know our ABC runs the animal welfare issue very strongly—like the RSPCA that are no longer going to have access to metadata. So we are reaching a point where the access that has been available to Telstra, Vodafone and Optus data—which is already in place—will have a smaller group of people able to access it in the future. I do not know whether I should be defending the legislation, but those are the arrangements that have been put to us as I understand them. I am looking seriously at the arguments that you have made to see if there are issues that we should be pursuing, and I am still waiting.

Ms Flynn: What we are saying is that we are concerned with the way that this is structured. There should be significant parameters around it so that journalists in the normal course of their business are not going to be impacted, and that is not clear to us. I think it could be made clearer through the bill being much more specific about some of those things we are talking about. It is not about the sweep of things; it is about what you are able to do and how it is used, than what the accountability is for how it is used.

Senator BUSHBY: Once again, we are not here to give evidence, so I will put this in the form of a question. Are you aware of other evidence we have received in this committee through submissions and at the previous hearing that there are serious restrictions over the circumstances in which law enforcement and security agencies can access the metadata? We have gone through the procedures. There are procedures in each of the agencies that they would need to follow. You suggested that a government of the day might use metadata for purposes beyond those legally allowed. The intention, as I understand it, the evidence we have received is that the increased oversight arrangements, together with the fact that organisations like ACLEI will take an interest if that data was being used for legal purposes or outside the purpose for which it was granted would make it very unlikely that a government might use metadata for purposes beyond those legally allowed.

Ms Kruger: It is comforting to hear that the procedures [inaudible] I think my concern remains going back to the [inaudible] that those boundaries are not clear to us from the wording of the bill. I guess there are a number of [inaudible]—

Senator BUSHBY: I am sorry: I do not know about the other members of the committee but I am not getting all of that. It is difficult to—

CHAIR: You are breaking in and out a little bit. Is there a possibility you could find a spot where you are closer to the—

Senator BUSHBY: Sit a little bit closer to the—

Ms Kruger: We are moving around. Do you want me to start again? Is that better?
CHAIR: That is much better, thank you.

Ms Kruger: Shall I start again?

Senator BUSHBY: If you could, that would be appreciated, thank you.

Ms Kruger: It is very comforting to hear your comments on the sorts of internal processes that the agencies have in place, the restrictions that you envisage and the intention behind this legislation. I think in going back to the wording of the bill we still have some concerns about the lack of detail and the indeed we would like to see some of the comments you just made incorporated into the bill. Without wishing to repeat points that Judy Flynn and Georgia-Kate Schubert have made, the bill does not give an exhaustive list of the agencies who are able to access the metadata, which is something of concern to us. As we mentioned, we have already discussed the warrant issue and then the issue of course of the data that could be caught under this legislation is going to be covered under the regulation, which we have not yet seen. So I think there are still some areas where we feel a little more detail would help us and, as I say, the comments you have made are certainly comforting but we do not necessarily see those incorporated at the moment into the bill.

Senator BUSHBY: Thank you.

Mr CLARE: To follow on from that answer, I am wondering whether the representatives of media organisations have had a chance to look at the draft dataset, which has been made public, which is the proposed, for want of a better term, definition of metadata that would be accessible under this proposed regime?

Ms Schubert: I have had an opportunity to have a look at the draft dataset, so yes.

Mr CLARE: That might help address the previous comments that you have made about concern about what that metadata might be. The other question I had was whether the representatives of media organisations had a particular view about how long the data that would be retained under this proposed legislation should be retained. There have been different views expressed about whether it should be for six months, one year, two years or five years or forever. Do the representatives of media organisations have a view?

Ms Schubert: The time frame has not been our focus. I would say that the reason why it has not been our focus is that given our concerns in relation to the bill, particularly the impact on confidentiality of sources et cetera, the time frame—whether it is six months, one year or two years—is not as large a factor in that. The confidentiality-of-sources issue remains regardless of the time frame for the retention scheme.

Mr CLARE: Thank you.

Senator BUSHBY: The evidence that we have received is that the bill itself does not actually increase or open up any further opportunities for enforcement and security agencies to access the metadata. In fact, to a degree it actually limits them, and I think Mr Ruddock touched on that. So there is no additional access to the metadata. All the bill is really designed and intended to do is to maximise the likelihood that, when an agency seeks to access metadata, that data is actually there. So what is it about the bill—what does the bill seek to change—that leads you to request a higher standard or threshold before those agencies could access that data?

Ms Schubert: Our view still stands: that, given that this is a legislative requirement for telecommunications companies to retain data for the purposes of law enforcement and national security, the checks and balances should be there. If they are already there, my colleague Sarah Kruger has already mentioned that it would be useful to have those more specifically spelt out in the bill. We note that, while the access to a piece of metadata may not seem to be as intrusive on its face value, we believe that the profiling that can occur through the aggregation of that data is equally deserving of some sort of authorisation process that would need to occur and be documented, as are other processes that already exist. But again we come back to the point that, if those processes already exist, it would be useful to see those identified more specifically in the bill and that that would help the Ombudsman undertake and execute his or her role in overseeing the scheme.

Senator BUSHBY: Thank you.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you. Thanks very much.

Resolved that these proceedings be published.

Committee adjourned at 18:04