INTERNET

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

To search the parliamentary database, go to:
http://parlinfo.aph.gov.au
PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

Wednesday, 17 December 2014

Members in attendance: Senators Bushby, Conroy, Fawcett and 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 2014.
WITNESSES

ALTHAUS, Mr Chris, Chief Executive Officer, Australian Mobile Telecommunications Association........ 31
COLVIN, Mr Andrew, Commissioner, Australian Federal Police ......................................................... 1
DAWSON, Mr Christopher, Chief Executive Officer, Australian Crime Commission ..................... 1
ELSEGOOD, Mr Michael John, Member, Communications Alliance .................................................. 31
FROELICH, Mr Peter, Industry Member, Communications Alliance .................................................... 31
HARMER, Ms Anna, Acting First Assistant Secretary, Attorney-General's Department ..................... 1
HARTLAND, Ms Kerri, Acting Director-General, Australian Security Intelligence Organisation .......... 1
JONES, Ms Katherine Ellen, Deputy Secretary, National Security and Criminal Justice Group, Attorney-
General's Department .......................................................................................................................... 1
LEE, Mr Simon, Acting Director, Attorney-General's Department ......................................................... 1
McMULLAN, Ms Kathryn, National Manager, Australian Crime Commission .................................... 1
MORRIS, Mr Tim, Assistant Commissioner, National Manager High Tech Crime Operations, Australian
Federal Police ...................................................................................................................................... 1
PHELAN, Mr Michael, Deputy Commissioner National Security, Australian Federal Police ............. 1
STANTON, Mr John Leslie, Chief Executive Officer, Communications Alliance .............................. 31
CHAIR (Mr Tehan): Before we start, on behalf of the committee I would like to make a short statement. The attack on the Lindt cafe in Sydney marks a despicable attack on Australians at home. Tragically, two innocent people have lost their lives: Katrina Dawson and Tori Johnson. The impact on their families and their friends will be deep and everlasting. Our thoughts are with them. To the hostages who escaped this harrowing ordeal, we extend our sympathy and support. We would also like to acknowledge the professionalism of our law enforcement and intelligence agencies—in particular, the New South Wales police. Under pressure, they displayed their dedication and commitment when it mattered most.

Threats of terrorism or terrorist acts will not change this nation. They will only strengthen our resolve. The values that we hold dear as Australians are the best way to defeat this evil. As the Prime Minister has already stated, we will continue to be a free, open and generous society. Australians will continue to open their hearts to every community that makes up our wonderful multicultural nation. As a mark of respect to the two Australians who have lost their lives, I ask everyone to stand and observe a minute's silence.

One minute's silence was observed—

CHAIR: I thank you all very much. I now welcome representatives of the Attorney-General's Department, ASIO, the AFP and the Australian Crime Commission. 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 that may be regarded as contempt of parliament. 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. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Ms Jones: We want to thank you for the opportunity to appear before the committee today. And noting the events of the last two days we are naturally deeply saddened by those events and grateful for the efforts of all of the law enforcement agencies.

As this committee has heard before, telecommunications data provides critical support to security and law enforcement agencies in the performance of their functions. The bill before the committee has been developed against the background of the challenges posed by the increasing importance of data combined with variable and changing retention practices across the telecommunications industry. In developing this bill, the department and the government have been guided by this committee's assessment in its report of the inquiry into potential reforms of Australia's national security legislation in 2013: that a data retention regime would raise fundamental privacy issues and should not be enacted unless those privacy and civil liberties concerns are sufficiently addressed. The development of the bill has also been guided by specific recommendations of this committee in 2013 in relation to data retention. And I note that those recommendations are recommendations 3, 4, 5, 42 and 43 made by this committee.

In a democratic society, law enforcement and national security measures must be designed to protect and promote our fundamental rights and freedoms, including the rights to privacy, freedom of expression, and life. Accordingly, the bill contains robust measures to protect privacy, including measures that the Office of the
Australian Information Commissioner recommended during the drafting process. The bill has also been informed by privacy impact assessments prepared by the former privacy Commissioner, Mr Malcolm Crompton, in 2011 and by the Australian Government Solicitor this year. The data retention bill contains three schedules, and I will very briefly outline those before I hand over to other colleagues.

Regarding schedule 1—data retention—Australia’s law enforcement and national security agencies are facing interrelated challenges. As this committee identified in 2013, agencies have been losing access to critical telecommunications data as a result of changing practices in certain parts of the Australian telecommunications industry. Increasingly inconsistent retention of records that are critical to law enforcement and security investigations are degrading agencies' investigative capabilities. At the same time, access to telecommunications data becomes increasingly important to the work our agencies do. These challenges are exacerbated in the current operational environment, where agencies are facing a dangerous combination of increased risk and declining capability. As such, the government decided to establish a limited data-retention regime in order to create a consistent record-keeping standard for information that is critical for investigations.

This reflects approaches in other industries where inadequate commercial record keeping undermined national security and law-enforcement investigations, including in the banking and finance industries. The bill will also supplement industry's existing data-retention obligations, such as the requirement for service providers to keep certain building records for six years under the Telecommunications Consumer Protections Code.

I want to emphasise a few limitations of the proposed scheme. This scheme does not apply to all communication services in Australia. There are significant exceptions for services where the investigative benefit would be outweighed by privacy or regulatory impact. Nor does the scheme apply to all types of communication telecommunications data. The bill and the government's proposed dataset are strictly limited. In particular, the bill would not require service providers to keep the content of any communications or to record a person's web-browsing history. The bill also carefully limits the volume and the detail of location records that industry would be required to keep. Service providers will generally be required to keep records for two years. The advice of our agencies, which is consistent with international reviews, is that a two-year retention period is necessary for complex and serious national security law-enforcement and anti-corruption investigations.

The bill will allow service providers up to two years to fully comply, ensuring that companies have the time they need to develop efficient solutions. The government has also announced that it will make a reasonable contribution to industry's up-front capital costs. The security of retained data is a very important issue. As this committee would appreciate, various parts of the Australian government work very closely with the telecommunications industry to protect their networks and information from an array of threats. This cooperation will continue.

More broadly, Australian law currently requires service providers to adopt risk based approaches to protect personal information under the Privacy Act. The government has also announced that it will introduce sector-wide telecommunications sector security reforms recommended by this committee. These reforms will be finalised before data retention is fully implemented.

Schedule 2 of the act relates to limits on access. At present, any agency or body that enforces a criminal law or a law imposing a pecuniary penalty or that protects the public revenue is permitted to access telecommunications data and the content of stored communications, such as emails and voicemail messages. In the last financial year, more than 80 agencies and bodies accessed telecommunications data under the act. The government has accepted the PJCIS 2013 recommendation and will significantly limit access to telecommunications data and stored communications.

Schedule 2 of the bill limits access to telecommunications data to ASIO and 18 criminal law-enforcement agencies that parliament has previously expressly approved to access this information. The bill will also permit the Attorney-General to declare additional agencies, subject to strict criteria, including privacy controls and parliamentary disallowance. This power recognises that there are a limited number of other agencies that play important roles in which data access may be appropriate and provides a transparent mechanism for agencies to be authorised to access this sensitive information.

Schedule 3 relates to oversight. At present, agencies are only permitted to access telecommunications data on a case-by-case basis where and to the extent that it is necessary to do so as part of a legitimate investigation. Additionally, once agencies have accessed data, it is a criminal offence for officials to use or disclose that information, except where and to the extent that it is necessary to do so for a legitimate purpose. The Inspector-General of Intelligence and Security inspects and reports on ASIO's access to and use of and disclosure of telecommunications data. In her most recent annual report the IGIS did not identify any concerns with ASIO's access to telecommunications data and concluded that there was a high rate of compliance in this area.
By comparison, presently there is no oversight regime for Commonwealth, state and territory enforcement agencies accessing telecommunications data. To address this issue, the bill introduces comprehensive oversight by the Commonwealth Ombudsman, which has been developed in consultation with the ombudsman's office. This schedule also significantly enhances the oversight of agencies accessing the content of stored communications.

In conclusion, the data retention bill is intended to address the serious and growing challenge to the ability of Commonwealth, state and territory governments to safeguard national security and uphold the rule of law. The department acknowledges the committee's previous comments that data retention raises privacy issues, which must be addressed. The bill contains a range of significant and important measures to protect privacy. We welcome this inquiry as an important opportunity to further explore these issues.

Mr Colvin: Chair, with your indulgence, I would also like to make an opening statement. Before I do, I thank you for your comments. On behalf of all law enforcement in this country, I am sure, I thank you very much for your recognition of the efforts of the police officers, particularly those very brave police officers who executed the resolution of that matter in the early hours of yesterday morning. I would also like to express my condolences to the victims and their families of the tragic events that unfolded in Martin Place on Monday and into Tuesday morning. I place on the record my and the AFP's regard and thanks for the dedicated police who worked tirelessly and professionally to resolve that situation. Those events highlight the complex environment that police around this country work in every day to protect the public. While I understand and accept that there is a great deal of interest in the matters that unfolded over the last 48 hours, I need to say that the matter is led by the New South Wales police and we will need to be circumspect and careful about what we say and how we answer questions. There is a critical incident investigation that is currently underway, along with a criminal investigation, and the committee will understand that we will need to be careful given that those investigations are currently underway.

In relation to the matters before the committee today, thank you for the opportunity to appear here. The AFP strongly supports the changes to the legislation proposed in the data retention bill. The bill does not propose new powers for law enforcement, nor is the AFP seeking any extension of the investigation powers we already have. The Telecommunications (Interception and Access) Act was crafted a long time ago. Globalisation and increasing diversity of telecommunications service providers and technological advances mean the legislation is not as effective as it once was. Telecommunications data is a critical component of investigations and has been successfully used to support numerous investigations into serious criminality from many, many years. Industry already captures much of this data, but, as more services become available, providers are keeping fewer records for shorter periods of time. Current retention rates vary widely and provide opportunities for criminals to remain anonymous based upon retention practices.

The AFP considers that the data retention bill goes a long way to addressing that continuing loss of capability. The proposed dataset reflects the minimum crucial categories of data necessary to support investigations into serious criminal activity, including, of course, terrorism, corruption and the protection of our children. 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. Telecommunications data plays a key role in these investigations in supporting warrant applications, identifying criminal networks, establishing evidential trails and developing briefs of evidence. When the AFP are dealing with serious threats to national security and other serious crime, we cannot afford to rely on luck to see if the provider that the criminal has chosen to use has retained that data. I also do not think the public would consider that an acceptable outcome for serious criminal investigations.

Looking at AFP investigations commenced between July and September of this year, 2014, 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. Of course, we are happy to put more detail on the record through the course of the hearing.

Telecommunications data played an important role in the investigation and prosecution of suspects in Australia's two largest counterterrorism investigations, operations Neath and Pendennis. If this data was not available, law enforcement may not have prevented those planned terrorist acts. Also—and this is a critical point—the AFP deals regularly with the providers. Where it is known that the company will have already disposed of information required, the AFP will not submit a request. As such, the figures that you have just heard, as well as figures that we will put on the record throughout the course of this hearing, do not represent the entirety of investigations or the leads that may have been pursued had we been confident that data had been retained.
I would also like to provide the committee with a clear example of how the variation in retention of data affects serious investigations. In 2013, the AFP commenced an operation called [inaudible]. The operation related to the compromise of a UK based website in 2011. It involved 552 Australian based internet protocol addresses. Each IP address, which you will hear a lot about today, I am sure, represents a potential offender both online and in the offline world. Of the 552 IP addresses, 89—which represent 16 per cent of those addresses—were discounted immediately as they resolved internet service providers that were known not to retain data for the period of time in question.

Further analysis revealed 244 addresses were likely to have been linked to criminal offending and were the subject of further requests to the ISPs for telecommunications data. Of those 244 requests, another 67 were unable to be progressed further, primarily because the data had no longer been retained. Data was available for only 177 IPs, resulting in the identification of 139 people or subscribers of interest who were then referred to the AFP and other state and territory counterparts for investigation.

It is of great concern to the AFP that the persons behind 156 of those IP addresses were able to preserve their anonymity due to the fact that the data had not been retained. If those ISPs faced the consistent obligation to retain data for two years, as proposed under this bill, it is quite possible that additional persons of interest, some of whom appeared to be involved in serious offending, could have been identified and properly investigated.

The AFP understands the importance of individual privacy and we support this as a fundamental right in Australia. We also support the important protections on privacy provided under Australian law. However, the AFP does not support the right to anonymity when it relates to unlawful activity. The proposed scheme has robust oversight mechanisms with the ombudsman conducting annual inspections of stored communications and telecommunications data, and reporting accordingly.

The AFP supports these mechanisms to ensure that the public can have confidence that these powers are being used in a targeted, transparent and accountable manner. The safeguards ensure the AFP only accesses information in a highly targeted way. It is critical that there is a level playing field so that the AFP and other law enforcement agencies can be confident that all providers will retain that limited subset of extremely highly valuable telecommunications data for the two years proposed.

I would like to extend an invitation to the committee to attend AFP headquarters at a time to suit the committee—perhaps in January—so that we can provide further operational briefings to demonstrate the central role that telecommunications data plays in all of our investigations. If the committee is agreeable, of course, Chair, we will work with you and the secretariat for a time when that may occur. I would like to thank the committee for inviting the AFP today. As you know, Chair, I may have to step out. But it is critically important that I am here today because, from a law enforcement perspective, this issue of great importance. Thank you.

Ms Hartland: If I could just add a few comments by way of opening statement. I would just like to support the comments made by the department and the commissioner, and make a brief opening statement from ASIO’s perspective. In doing so, I too am very conscious of the recent events in Sydney and the need to not add to public speculation about that event which remains under investigation, as the commissioner has said, by New South Wales Police and New South Wales Coroner. ASIO works and will continue to work very closely with the AFP and New South Wales Police in any investigations and inquiries that take place. I would, however, like to reflect publicly that our thoughts are with the innocent victims of this horrendous act, particularly with the families of the two hostages who lost their lives and the police officer who suffered injuries during the emergency action undertaken by police.

Today’s hearing is to provide context into ASIO’s clear and stated requirement for the retention of telecommunications data. ASIO’s role is to identify threats, investigate them and provide advice that reduces the risk to Australia, its people and its interests. The committee’s work in reviewing this bill is important to Australia’s national security. ASIO has consistently made the case for such legislation over the past decade because of the value of communication data to security investigations. This is because the mandatory data retention scheme that the bill will provide ASIO with has key capabilities to enable us to perform our statutory function.

It is not a hypothetical discussion: Australia is a terrorist target. Recent events have once again demonstrated that Australia is not immune from acts of terror. The Australian government and private interests are also the subject of malicious cyberattacks. We have seen an increase in the scale and sophistication of such attacks by hostile foreign nations.

Communications data has been critical to the disruption of terrorist attacks in Australia, and I would like to talk you through some of the cases that demonstrate this that Commissioner Colvin has already touched on. The
committee will recall the disruption in 2005 and 2006 of terrorist activity in Melbourne and Sydney and Operation Pendennis under which 22 men were arrested with 18 convicted of terrorism offences. They were plotting mass casualty attacks.

Communications data was vital in uncovering who was involved in that plot and enabling other investigative tools to be used that ultimately disrupted and prevented harm to the community. In particularly, communications data was used to identify a covert phone network.

What do I mean by a covert phone network? The individuals had the regular mobile phones that they used but they also had other mobile phones subscribed in false names. These falsely subscribed phones were changed very often and were the means used to progress the terrorist activities. Without going into the sensitive technical detail of how that was done, communications data was key to identifying all of the phones that were being churned through. It meant ASIO and police could target more intrusive methods including telecommunications interception at the plotters and gather key content showing the intentions and plans of the men as well as the activities they engaged in to progress the plot.

Without that retained communications data, ASIO would not have been able to identify the covert phone network and been blind to vital pieces of information. Communications data was also used by ASIO to identify new people of interest and leads to further investigations. For example, it showed us who called whom and when.

Another case, Operation Neath, in 2009 involved the arrests of Melbourne based individuals who were plotting an armed assault against Holsworthy army base in Sydney. Five men were arrested and three convicted of terrorism offences. Communications data was used in that operation to identify connections between individuals, who had called whom and when and how often; analyse connections to individuals in other security investigations; generate leads to overseas based investigations and extremists; and identify attempts by the plotters to hide their communications from ASIO and police. Without retained communications data, ASIO would not have been able to identify all the communications relevant to that plot and would likely not have understood the network of people who were involved.

In both cases, the consequences of not having communications data available to support ASIO and police would have been disastrous. There is more detail on these cases in our submission, including details that remain operationally sensitive that show the value of those tools in our investigations which we are happy to talk through further in closed hearings.

I want to talk briefly around the retention period and also locational information. Public debate about the retention bill has focused on the retention period and locational information. A two-year retention period is a compromise from ASIO’s perspective. We have said repeatedly that we would prefer a longer period to match the long-term strategic nature of serious national security threats we face.

We have provided the committee with a classified breakdown of the age of ASIO’s communications requests using 12 months as a benchmark, but I can say in this hearing that 12 months is not a sufficient period of time. Around 10 per cent of the requests are for periods of 12 months or more, leading into periods of up to two years and beyond. Those cases relate to—10 per cent may seem small number—our most serious and complex cases. Typically, these relate to activities of hostile foreign nationals or nations engaged in spying and influence operations against Australia. It absolutely needs to be two years from our perspective.

The bill will not require providers to retain all the location information—the regular connections mobiles make to cell towers, for example. What the bill does require is for providers to retain the location information when communications occur. For example, what cell tower did the mobile connect to when they made a call? This does not amount to tracking as some people have suggested. If ASIO has a requirement to monitor individuals, other capabilities can be deployed—for example, tracking devices under warrant.

The cell tower locations that will be required to be retained by the data retention bill will only ever provide agencies with the vicinity of the mobile phone. This information provides useful intelligence, including when correlated with other intelligence over time, and there are some operational examples of that in our classified submission.

Finally and very briefly, if you accept ASIO’s role in protecting Australia and you accept that we need 21st century tools to do it, all that remains is to consider the checks and balances that must apply. ASIO is already subject to many accountability and oversight mechanisms spanning legislation, ministerial accountability, parliamentary review and independent oversight. These have been tested and evolved over time. ASIO also has rigorous internal policies and controls which the people of ASIO operate within day to day.

The reality of the assurances that these mechanisms provide to government, parliament and the community is often ignored in public debates on national security issues. It is important to note that these already consider...
individual rights, such as privacy, proportionality and minimising intrusion as well as the collective community right to feel safe and secure. The data retention bill will continue this present system of checks and balances. In ASIO's view, the bill will be an important modernisation of the TIA Act to prevent further degradation of the intelligence and law enforcement capability.

CHAIR: Thanks Chief Commissioner, Ms Hartland and Ms Jones. Can I say once again to the Chief Commissioner and Ms Hartland: you can hear from the emotion in your voices that it has been a very trying 48 hours for you and, once again on behalf of the committee, our feelings go out to you and your officers for all the work that you have done and your dedication to the cause. The fact that you are here today prepared to give evidence to us, shows your willingness to do what is right for this nation. So, on behalf of the committee, thank you both very, very much. Mr Dawson, I invite you to make an opening statement.

Mr Dawson: I would like to make a couple of remarks in opening, consistent with those of fellow colleagues who have already spoken. Telecommunications data is an effective and efficient tool used by law enforcement and national security agencies to identify and investigate crime, including serious and organised criminal activity, and to reveal the true extent of a criminal network. The Australian Crime Commission and its Commonwealth, state and territory enforcement partners support mandatory telecommunications data retention and provisions that standardise the length of time of data retained for all telecommunications service providers operating in Australia. Access to this information is not a new power for law enforcement and security agencies; it is an attempt to get consistency in the storage provisions for data that law enforcement and security agencies already collect and already use.

The ACC investigates serious and organised crime. Inherent in this crime type are complex communication webs which are often only able to be discovered through retrospective analysis of criminality which span at times many years. Telecommunications data is an essential resource within the ACC and the state and territory partners in discovering, understanding and responding to serious and organised crime and volume crime. It is a foundation of, and one of the least intrusive sources of information for, other investigative techniques. Such data enables agencies to establish the time, general location and persons involved in communication activity. It is critical for determining the parties involved in serious and organised crime activities as well as for eliminating innocent parties from our investigations. Currently, retention of communications data by service providers is variable and it may be hours, days or weeks depending on which provider. The difference in what is retained in the absence of standard retention periods does affect the ability to detect and understand serious and organised crime.

The Australian Crime Commission board members agencies have compiled 10 case studies which I would like to table to the committee today. These case studies demonstrate why it is not confined to one particular level of intoxication. Person A drove the taxi to a vacant reserve. While there, person A met another taxi driver—who we called person B. It was alleged that they both sexually assaulted the victim.

After the sexual assault, person A dropped the victim home after 11 pm. Telecommunications data established that person A called person B within five minutes of collecting the victim. At that time the other taxi driver was elsewhere, dropping off another fare. Person A and person B then both drove separately to the reserve. There were another three calls between the two parties between 10 and 11 pm, and a further three calls went unanswered.

The GPS in each of those taxis did support that both offenders attended the reserve. Telecommunications data confirmed that persons A and B had spoken on numerous occasions in the 24 hours prior to person A picking up the victim. In the 24 hours following the offence persons A and B exchanged several telephone calls, with additional calls going unanswered. Evidence of phone calls between the offenders indicated that their meeting at the reserve was not coincidental. Persons A and B were charged with sexual penetration without consent. In 2012 person A was convicted and sentenced to six years imprisonment. Person B was acquitted at trial.

The important point is that deploying other capabilities such as telephone interception would not have been effective in this sexual assault case, as the crime had already been committed. It was only the availability of telecommunications data that had been retained that enabled police to identify the time line and understand the offence. I would like to table these case studies.

CHAIR: Thanks, Mr Dawson. I might start. Chief Commissioner, you talked about the use of data retention and the fact that it is not as effective as it once was. In 92 per cent of counterterrorism cases it has been used. If it
could not be used, or if it was of diminishing use when it came to counterterrorism, what sort of impact is that going to have on your ability to deal with terrorism?

Mr Colvin: The issue that we are dealing with is an increasing diminishment of the capability. So, as more providers are coming online we are able to access less information. So my first concern would be that, while it has been used in 92 per cent of counterterrorism cases, that figure may well—our fear is that it will—start to go down as more providers come online and have legitimately changed their business models to make it such that they do not retain this data.

The effect it would have on us in terms of our ability to investigate terrorism—of course, our focus is to prevent terrorism—I could not overestimate. It would have grave implications for law enforcement's ability in this country to investigate, deter and disrupt potential terrorist acts.

Mr RUDDOCK: I have a question that relates to one of the concerns I have about the coverage that we are likely to get under the bill as proposed. In this provisions that I was reading, internet cafes were to be exempted. I do not understand why we would be exempting particular locations such as internet cafes using wifi. That is what it says. It would be just another place that people would say, 'I can go there and nobody will be able to monitor my movements and understand where I have been.'

Mr Colvin: I might ask the department to answer that in the first instance. Then perhaps we could give some operational context once that is done.

Ms Harmer: The bill is intended to provide an appropriately targeted data retention regime to ensure that we keep a range of useful data. Naturally, a wide range of data could potentially be useful to our law enforcement and security agencies but the bill is intended to provide a proportionate response to that challenge and excludes a number of categories of providers that are subject to specific definitions in the Telecommunications Act framework. There are a couple of exclusions. One is 'immediate circle', which covers such things as corporate networks and close—

Mr RUDDOCK: No, I understood in terms of network, but I am talking about wifi services in cafes.

Ms Harmer: That relates back to the provision of services within what is known as a 'same area'. That particular section is excluded because of an assessment that, while that data is useful, the compliance burden and impost upon the providers of those same-area services is a significant one, and the intention of the regime is to provide a targeted response around a range of data that is useful. Naturally, agencies have a range of tools at their disposal to access communications and identify the behaviours and communications of suspects, but there is a particular exclusion there which relates back to a particular compliance burden for the providers of those services.

Mr RUDDOCK: I would like to have some understanding of what that compliance burden might be. It beggars belief. If people who go to internet cafes were told that it is not possible that their communications would be monitored in the same way as any other form of communication, that is where they would naturally go to.

Ms Harmer: As the committee is probably aware, there is obviously a large range of wi-fi providers, including free wi-fi at cafes, takeaway services and various public venues. In excluding those, that is not to say that relevant data is not captured at some point. Obviously the service that is provided by a cafe or a community service is provided by a telecommunications provider. So some data is available; it is simply that the burden is placed not on the provider of that free wi-fi service but, rather, on the telecommunications providers who are providing that communications mechanism.

Mr RUDDOCK: I am very troubled by it and I would like some explanation about the nature of the burden. That brings me to my next question, which goes to the time of two years. I know that the committee I was previously a party to suggested two years, but I really want to open up a question. If information is kept for two years, what are the significant costs that would suggest that you should say, 'We'll wipe it all after two years'? If the information is already kept, are there significant costs in keeping it for longer periods if the keeping of that information is going to be valuable? I would like to get an idea about the potential costs if we were to extend it beyond two years.

Ms Harmer: The first bit of information I can provide in relation to the two-year retention period is that there is no obligation in the bill to destroy that information after two years. The bill would create—

Mr RUDDOCK: I understand that. That may mean that it is not a bad thing to have an obligation that they keep it for longer—say, five years.

Ms Harmer: Indeed, and there are some contexts in which providers do keep that information for longer. For example, there is already an obligation under consumer protection codes to keep some billing information for six years, and of course the providers are entitled to keep information for such time as it is required for their own...
legitimate business purposes. Industry may provide you with some advice about the particular costs that are associated with an extended retention period. They have provided some feedback in consultations that there is a cost associated with a longer retention period. But they may be better placed to advise the committee because their individual circumstances, their network configurations, affect the way in which they implement data retention obligations and, therefore, the proportionate aspect of the cost that is attributable to implementation and then ongoing storage as an incremental burden upon that.

Mr Colvin: From a law enforcement perspective and, I would imagine, also from a security perspective, the longer the data is kept the better because there will be investigations where we would ordinarily have sought information that goes back beyond two years. This is about trying to create a minimum standard that is level across the industry. As the department has already said, there are internet providers now who routinely hold this information for up to seven years and perhaps longer, depending on the way their systems are configured. From a policing perspective, that would be beneficial to us. But this is about creating a minimum standard. The costs will depend on how industry have established and set up their systems—and they will each be different, depending on how new they are the market, I am sure. But this is about providing that balance. Two years is a time frame that law enforcement and security agencies have accepted. That is appropriate in the circumstances, but I can see instances where we will still claw back further than two years if the data is held. If data is not held under this regime then it is not available to us.

Ms Hartland: As the commissioner has said, there are some investigations which we are involved in, particularly in terms of espionage but also in terms of terrorism, which go over decades. We understand that need to find a compromise. If I could add to that by way of example: last year we saw an internet provider who had been keeping information on IP addresses for a number of years. They changed their regime and business model, quite legitimately, to keep data for only three months. That sort of change makes it very, very difficult.

Mr Ruddock: Just to make it clear: if we agree to this legislation, we have established the principle that information should be kept. Once we have established the principle, we then go to the question: what should be the length of time? It appears to me that the only relevant factor is potential cost. The utility of that information, if it is going to impose a very significant cost, we may weigh up. I want to be very clear: you are arguing that five years would probably be a better period in terms of law enforcement and security purposes. Having established the principle, we should try and get some further information on costs—and you cannot provide that.

Mr Colvin: That is right. It is not a question that we can answer.

Mr Dreyfus: I think these questions might be addressed to the Attorney-General's Department. Could I set a bit of context here as to what this bill is about. This bill—and if you can confirm—is not dealing in any way with the powers that there presently are for ASIO, the Australian Federal Police or other police forces to access telecommunications information. Is that right?

Ms Harmer: The only amendment to the access arrangements is to reduce the number of agencies who can access the data, but the access thresholds are not changed.

Mr Dreyfus: Understood—for a particular kind of data.

Ms Harmer: That is correct.

Mr Dreyfus: At the moment we have got powers for police and ASIO to conduct surveillance of telephone conversations and full content on warrant. Is that right?

Ms Harmer: Yes.

Mr Dreyfus: And there are powers for ASIO and the police to obtain a warrant to access full content for internet communications?

Ms Harmer: In the same power, yes.

Mr Dreyfus: There are powers to obtain under a stored communications warrant anything that companies have kept, including all content. So that kind of access and surveillance is all under warrant?

Ms Harmer: Yes.

Mr Dreyfus: In addition, there are existing powers which are known, I think, by all of you as authorisations, which enable police forces, ASIO and a range of other law enforcement agencies, including the Australian Competition Commission and ASIC, to seek telecommunications data from providers without warrant?

Ms Harmer: In accordance with an authorisation; that is correct.

Mr Dreyfus: I think for the last reported year some 330,000 authorisation requests were sent to service providers, telecommunications providers.
Ms Harmer: That is correct.

Mr DREYFUS: This bill does not seek to change any of those powers other than, as you have pointed to, Ms Harmer, the tightening or the lessening of the number of agencies that will be able to obtain data that is being required to be stored.

Ms Harmer: That is correct.

Mr DREYFUS: So this bill is about forcing telecommunications companies to keep personal telecommunications data of potentially all Australians?

Ms Harmer: This bill creates a consistent obligation to retain a range of telecommunications data, a large of amount of which is already kept by a number of providers, and creates consistency around that set of data. Yes, the bill is about creating a retention obligation around a limited set of telecommunications data.

Mr DREYFUS: At the moment we have a set of powers that operate on the world as we find it or the data as it exists, and there is a degree of inconsistency between companies as to the data they keep. What this bill seeks to do is not only require data to be kept for two years but also require it be kept in a particular way, in a consistent way.

Ms Harmer: In terms of the last aspect of your question, there is no particular regulation in the bill about how the data is kept. The obligation is around the retention of the set of data. No particular obligations are placed around how. I may have misunderstood the last aspect of your clarification.

Mr DREYFUS: I am quite happy to spend some time on this because it is a quite important aspect of this bill. As I understand the bill, it is seeking to force telecommunications companies to keep a range of personal data—we will get to what that range is—for two years. They are given up to two years, I think Ms Jones you put it, to fully comply. If this bill were to become law, from the date on which it becomes law telecommunications companies would have another two years within which to comply.

Ms Harmer: Yes, with one minor clarification: the two years is comprised of two components. There would be six months after royal assent—that would be when the obligations commenced—and then there would be an 18-month period. Combining the six months with the 18 months gives a period of two years to support implementation.

Mr DREYFUS: Sure, that is helpful; thank you very much. The bill talks about 18 months but you are correctly pointing out that it is intended there be a six-month period between assent and commencement and then 18 months for compliance, giving two years.

Ms Harmer: Yes.

Mr DREYFUS: We are certainly not going to see an instant change in the landscape on this bill becoming law. Far from it. It has a lead time for implementation.

Ms Harmer: There are a couple of clarifications I would add to that. First of all, the 18-month phase is one that is attributable to the development of implementation plans. They are an optional tool for industry to stage implementation. For those implementation plans, the obligations would commence on commencement of the legislation, but the 18 months gives providers the opportunity to stage their implementation under an approved plan. Subject to approval of the plan, this provides the staged implementation, which is intended to achieve progressive compliance throughout that 18 months.

The other clarification I would provide is that there are a number of transitional provisions that ensure that in the interim, between royal assent and commencement and then following commencement, there is no degradation in current retention practices and it obliges providers not to reduce the period for which they currently keep the items that are specified in the dataset.

Mr DREYFUS: Can you explain to us, across the landscape of telecommunications providers, who is keeping what? You just referred to the intention of this bill, which is to impose an obligation—while they are working up their implementation plans—on telecommunications providers not to lessen the period that they keep data.

Ms Harmer: As I think both the commissioner and other agencies have said, there is currently significant variability across industry in the retention periods, across individual items and across individual providers. It is the agencies who are engaging with the providers on a day-to-day basis and who see that variability in their operational activities.

Mr Colvin: I could answer that and perhaps, in session, we could talk about specifics a little more. What we are seeing is, as the industry is changing and as technology advances, those companies that are in the industry under old technology have largely configured their systems in a way that retains this data. As new companies are
coming on board, new internet service providers—right down to local community type providers, ma and pa businesses, that are quite small and can have very small customer bases—the need for them to set up an infrastructure that Telstra might have, for instance, is very different. The need for them to bill you or me on the way that we make phone calls has changed considerably. They care less about how many phone calls I make and how long they are. They care more about how much material is being sent down the line and how much data is being used, and they will bill me for that data. It is less relevant how many calls were made and what that call might have been.

As more companies are coming on board, this is the degradation that we are very concerned about. It is not just a matter of the consistency; it is that if we do nothing now, each and every day as more companies are coming on board in an industry and a marketplace that is very competitive, the ability of law enforcement and security agencies to access it is degrading.

Ms Hartland: We have seen some companies alter those time periods from years down to months for certain sorts of data, and the variability is great. Companies are keeping some of this data and certain sorts of data for up to seven years; others are keeping them for three months. So you are quite right in saying that this is not about looking at additional powers and additional powers of access. It is not about that; it is about having a consistency of a regime so that we can work with the companies and know that they have that data that we require for our operations.

Mr DREYFUS: Just on that, there is a requirement for billing records to be kept under a quite separate consumer protection regime?

Ms Jones: That is correct.

Mr DREYFUS: Can someone explain to us what that consumer protection regime is?

Ms Harmer: That is a consumer protection regime that is oversighted by the Australian Communications and Media Authority and it places particular obligations under that code for the retention of a limited set of billing records and to oblige providers to deal with their customers in a particular way in a way that is honest, open, fair and transparent, and is consistent with their privacy. That is a limited set of information that is around consumer protection in relation to their acquisition of telecommunications services.

Mr DREYFUS: It is billing records only?

Ms Harmer: Yes.

Mr DREYFUS: That is a legislated requirement?

Ms Harmer: It is delegated legislation. I think it is a code that the Communications Alliance developed.

Mr DREYFUS: It is for six years?

Ms Harmer: Yes.

Mr DREYFUS: Just to go back to what Commissioner Colvin was talking about. Do all companies have billing records?

Ms Harmer: If they are providing a service which is paid for. The obligation is to keep billing records because it is consumer protection. So if they are providing a chargeable service then the obligation is to keep those billing records.

Mr DREYFUS: Perhaps I can get Commissioner Colvin on this. I am not inquiring into investigative methods and I am not wanting to compromise anything at all: there would be some companies for whom billing records, I assume, would be quite thin if they have some kind of bulk-charging arrangement—certainly a non-itemised charging arrangement.

Mr Colvin: I might ask Deputy Commissioner Phelan to answer that.

Mr Phelan: Mr Dreyfus, you are quite right. Depending on the circumstances of the business, it might very well be that all they want to know is how much data passed over, say, your system that you own between me and the ISP. That is all they are after and that may very well meet the minimum requirements under the protocol. It will not though, however, potentially tell me what IP address was allocated to your computer when you accessed that data which is the equivalent of a phone number that we are after—that unique identifier that picks up the service provider and the user. That is the sort of metadata that we are obviously after to keep.

The important thing that I want to get across is that it is not just the mums and dads or even those ISPs that are owned by criminals that we are after, or even the bigger telecommunications, companies. At the moment they do keep data on who you call, how long you called and where you called to and from because they need it for billing...
because that is how they bill is at the moment. They are doing it over the copper wires et cetera as they have done for many, many years—decades.

When they move to using the internet for the transfer of the data—in other words, the calls—even the large telecommunications company will not care less who you call; it will all be about how much data passed across their lines for the purposes of billing. We want to be able to still have that same access to information about who was being called and where you called from, so that we can have that unique identifier from a person to a service. That is all we are trying to preserve—the similar requirements that we have now.

Mr DREYFUS: To take the example of a smaller and newer telecommunications provider coming into the market who is billing on some data measurement basis—bulk only—they will not have any systems that presently, as I understand the example you are giving, capture the data that they will, if this bill becomes law, be forced to keep. So is the intent of this bill to require such a telecommunications provider to create a system under which that data can be kept?

Mr Phelan: I will let the department talk about the specifics of that, but certainly we would want that information, yes.

Mr DREYFUS: I understand you want it. I am interested in the mechanism that this bill uses to get to that situation where it will be available to you.

Ms Harmer: The mechanism that the bill uses is to prescribe that particular items of data must be kept. Those items of data are ones that are retained in the telecommunications industry but not necessarily consistently. Not all providers retain all elements, but they are all retained somewhere in the industry, and it is to ensure that those particularly prescribed classes are kept. Does that—

Mr DREYFUS: To take this example, I think the reference was made to mum and dad operations, but let's say not just mum and dad operations but something smaller than Telstra comes into the industry as a new company with a business model that has the simplest of simple billing systems—one that certainly does not require them to keep any data. Would this bill require them to set up a system that would enable the keeping of data as prescribed?

Ms Harmer: The information that is required to be retained is information that is typically used and required by a telecommunications network for the provision of the services themselves. They are key items of data that are required in order to know how to deliver a communication and to have it reach its destination. So the bill will require the retention of defined items of data. Those items of data, though, are ones that are typically required in the provision of the communications service itself. They are not things that are extraneous to the delivery of communications services.

Mr DREYFUS: Understood. So we are talking about data which is required to make the system operate.

Ms Harmer: So they would typically have it anyway.

Mr DREYFUS: So they exist, albeit fleetingly. They exist.

Ms Harmer: That is correct.

Mr DREYFUS: But what this bill does, if it becomes law, is to force the companies concerned not just to observe and use that data but to keep it for the prescribed period.

Ms Harmer: That is correct.

Mr DREYFUS: The government, at this point, has not settled the dataset—that is, the personal telecommunications data that companies are going to be forced to keep.

Ms Harmer: The government has published a draft dataset for the purposes of consultation, of consideration by this committee and of further refinement. I think that, as the government has indicated, it has already been the subject of some consultation with industry, but it is correct that that dataset is currently the subject of further consultation.

Mr DREYFUS: And that draft dataset circulated with the bill was not in fact any more specific than that which was circulated at the time of the 2012-13 inquiry?

Ms Harmer: It certainly builds on work that was done around the time of the committee's previous inquiry, but it is correct that the broad categories of data that we are looking at are ones that we have been considering for some time and that, indeed, draw on extensive international experience in the key data points that are required to support investigations.
Mr DREYFUS: The committee was provided last night with a document—a report—described as the first report of the Data Retention Implementation Working Group, which is a working group that, we have been advised, met for the first time on 19 November 2014.

Ms Harmer: Yes.

Mr DREYFUS: Its members are the secretary of your department; the Director-General of ASIO; Commissioner Colvin, the Commissioner of the AFP; the Secretary of the Department of Communications; the Chief Executive Officer of the Australian Crime Commission; some representatives of Telstra and Optus; and the Chief Executive Officer of the Communications Alliance. I have just read to you from the letter there from the Attorney-General.

Ms Harmer: Yes.

Mr DREYFUS: I have had the opportunity in the few hours since late last night, when this was delivered to me, and now to have a look at this first report of the data retention implementation working group. It makes a number of recommendations to change that draft dataset that was circulated. Is that a fair description of it? I am not wanting to go to the changes they suggest.

Ms Harmer: That is correct. It makes a number of recommendations in relation to the dataset, a small number in relation to changes to the dataset, a number in relation to the addition of additional explanatory material that industry considers would assist, and one recommendation in relation to the process for any changes to the dataset in future.

Mr DREYFUS: And just to get this clear: the structure that this bill uses is not setting out in the bill the data that companies are going to be forced to keep but rather allowing for the dataset to be prescribed by regulations.

Ms Harmer: That is correct, with one clarification: the bill does not prescribe the detail of the data that is to be retained but does place a limitation on the types of data that may be prescribed by regulations by prescribing certain classes within which that data must fall before it can be the subject of regulations.

Mr DREYFUS: At recent Senate estimates the Attorney-General, Senator Brandis, indicated that a settled dataset in the form of regulations would only be circulated in—his words—'the early part of next year'. Are you able to say when this will be, precisely? I ask because at the moment we have a draft dataset and now a report of a working group which recommends some changes to that dataset. We have the Attorney-General saying that the settled dataset would be available in the early part of next year. And for the purposes of this committee's inquiry I am interested in knowing when that might be, and also for the public who are interested in this process and getting a grip on what it is that companies are to be forced to keep. When will that be known?

Ms Harmer: The dataset, as I mentioned, has been considered by the implementation working group, which has recently provided a report to government, which has been shared with this committee to assist its consideration of the bill. So, that is one mechanism through which the dataset has recently been reviewed, and potentially it might be refined. As the Attorney I think also indicated in the estimates hearings, the dataset has of course also been referred to this committee for consideration. So, we certainly envisage that the refinement of the dataset would indeed be assisted by the findings of this committee and any observations that this committee might make as well. So, while I could not provide a precise timing for it, the refinement of the dataset will be influenced by the implementation working group's report and also by any observations that this committee might make.

Mr DREYFUS: So, is it the government's intention not to determine a dataset before this committee concludes its deliberations?

Ms Harmer: The government's intention has been to provide a draft dataset for the purposes of consultation so that it is possible indeed for the dataset to be commented on and refined through this consultation process and indeed this committee.

Mr DREYFUS: Well, are we to comment on the government's draft dataset? Or are we to comment on the recommendations of the data retention implementation working group? Or both? Or something different again?

Ms Harmer: The government has published a proposed dataset, which is naturally before the committee. I think the government envisages that the committee might be assisted by the implementation working group, which has had the opportunity to bring together both government agency and industry representatives to provide a collective view and some agreement on key features and issues which perhaps might assist the committee in reaching its own view as to the appropriateness of the dataset.

Mr DREYFUS: Perhaps this is a rhetorical question, but how is this intelligence committee to scrutinise the scheme unless the government has a settled idea, a settled definition, of the dataset that it wants to force companies to keep?
Ms Harmer: I think the government would consider the draft dataset to be a fairly advanced document which has been informed by extensive consultation between agencies, industry and relevant government departments. And while it is a draft dataset it is certainly one that is advanced and has been informed by extensive consultation, and we would consider it to be an advanced document for the committee's consideration.

Mr Dreyfus: Is there a draft regulation at present? Is a draft regulation in some form in existence, or has a draft regulation been circulated to the industry working group?

Ms Harmer: The substance of the draft regulation would have effectively been the draft dataset. So the regulation would prescribe a dataset; that dataset is embodied in that document that is now before the committee.

Mr Dreyfus: So it is embodied in the draft dataset plus the recommendations for change to the dataset that the working group has produced.

Ms Harmer: Yes.

Mr Dreyfus: Well, I would go back again to this question: when is it that the government will be determining the dataset?

Ms Harmer: The government has proposed a draft dataset in the document that it has published through the department's website and referred to this committee, and is receiving feedback on that through the IWG process and through this committee.

Mr Dreyfus: That is not an answer to my question, Ms Harmer, and I will ask it again: when is the government proposing to determine a dataset that companies are to be forced to keep?

Ms Harmer: The draft dataset that has been—

Mr Dreyfus: Is a draft; yes.

Ms Harmer: The draft dataset that has been provided to the committee is the government's proposal for a dataset.

Mr Dreyfus: Is the government proposing to take any account of the recommendations for change to the dataset which have been made by the data retention implementation working group?

Ms Harmer: The government formed that implementation working group to refine the dataset; yes.

Mr Dreyfus: Is the government intending to indicate to this committee what it proposes to do with those recommendations?

Chair: The government has done that through what it has given us by close of business yesterday. The government has made that quite clear. But, as it has done with previous hearings, the government is also seeking our contribution. With the two previous piece of legislation that we have looked at, all of the bipartisan recommendations which were put forward were accepted by the government. The sense of cooperation and the bipartisan nature of this committee, and the way it has worked, is why the government has gone down this path.

Mr Dreyfus: It appears that we cannot advance that for the moment, Ms Harmer. Is your answer that you do not know when the government is going to make up its mind?

Chair: No; do not try and verbal Ms Harmer. She has given a very good and detailed answer about the process. I do not think that we should be trying to verbal the witness.

Mr Dreyfus: Well, I certainly was not trying to verbal you, Ms Harmer, and I take great exception to the chair suggesting that I was. But I am going to have to leave it there: at the moment it seems that we have a draft document and we have a report with recommendations, the status of which is not clear. Is that right?

Ms Jones: If I could answer that question, Mr Dreyfus: a report has been provided to this committee to assist it in its deliberations. Obviously, we will take note of any recommendations or advice that come from this committee and then, ultimately, government will make a decision that will be reflected in the bill.

Mr Dreyfus: All I was getting to was the question of when the government might be going to reach that point. And I am assuming that it will not be before the presently-intended conclusion of this committee process.

Ms Jones: The timing will be influenced by the timing of the deliberations of this committee.

Mr Dreyfus: But it will not be before the end of this committee's deliberations, which presently is intended to be a report at the end of February.
Ms Harmer: The government has sought the views of the committee on the dataset, so we would not anticipate finalising a dataset prior to receiving the views of this committee on an issue which has been referred to it for consideration.

Mr DREYFUS: And what should the public do? In making submissions to this committee, what should the public be commenting on?

Ms Harmer: The draft dataset which has been published on the Attorney-General's Department website; and which has also been published on this committee's website to provide views to this committee.

Mr DREYFUS: And what should the public make of the recommendations made by the data retention implementation working group, chaired by the secretary of the Attorney-General's Department?

Ms Harmer: The working group has been convened to provide advice to this committee on what is a very technical issue, and on which the government considered the committee might be assisted by deliberations of government agencies and industry, collectively. So, naturally, I will leave it to the committee how it treats the Attorney's transmission of the implementation working group, but it presents a series of views which have been provided to this committee, as would other submissions from industry, agencies and members of the public.

CHAIR: Before the public hearing started, we agreed in our private hearing that we will make this public so that it will be available for the public.

Mr DREYFUS: If I could move on to a bit of detail about the draft dataset, the committee secretariat has noted for us that the dataset is quite similar to that which has been used, albeit for much shorter periods, in some countries in the European Union, except for the addition of aggregate volumes of uploads and downloads. Would you explain why those two types of data have been added to the dataset in use in some European countries.

Ms Harmer: As I said earlier and as a number of the agencies have confirmed, all elements of the dataset have been included on the basis of a review of elements that are of assistance to law enforcement and security agencies in the performance of their functions. So the dataset that has been developed is one that reflects the critical and base pieces of telecommunications data that those agencies consider to be useful. We have been guided by international experience, but, ultimately, we engage closely with Australian agencies on the information that they require in support of their investigations and have developed the dataset on that basis.

Mr DREYFUS: Are you able to be more specific as to why those two types of data—aggregate volumes of uploads and downloads—not used in the EU have been added? Could I suggest one possibility: volume data would be especially useful in targeting torrenting activity, wouldn't it?

Mr Phelan: First of all, working out whether or not the line is active is most important of all—whether there is any volume passing over it or not and the amount of volume is important. Torrenting is certainly not something that we have been looking at, but certainly the amount of volume also determines, when we want to put an internet intercept off, how much capability we will have to dedicate to it. For planning purposes as well that is extremely important to us. Like anything else, we have to know how many lines to put off, our monitoring capability, our monitoring capacity and so on. That is one component of it, but the most important is to know in the first place whether or not the line is active and if any volume passes between an account at all. That is from the AFP's perspective, anyway.

Ms Hartland: To add to that, everything that the deputy commissioner has said is relevant from ASIO's perspective. Also—and I am happy to talk further about this in a closed hearing—in terms of looking at facilitation, networks who might be central, that sort of download information can be quite important in investigations. But to get into that any further I would probably like to take that behind closed doors.

Mr DREYFUS: Okay, thank you.

Mr NIKOLIC: New South Wales Commissioner Scipione has said:

There's not a terrorism investigation since 9/11 that hasn't relied on metadata. So why hasn't this bill been an imperative as strongly in legislative terms in the past?

Mr Phelan: Firstly, the data is available now, so we have been using it in current investigations. It is there because, as we said, communications companies are keeping it for billing purposes, and some of them are keeping it depending on what their business model is. But what we want to do is to seek to retain that ability going forward. I can confidently say that that information will not be available in five years time if we do not have a data retention regime in this country.

Mr NIKOLIC: So the imperative to standardise the length of time they keep the data is a relatively new issue that has confronted you.
Mr Phelan: No, the length of time is not relatively new. The big telcos keep it according to their business models. Some others do not keep it at all. Some keep it for a very short period of time.

We want standardisation. Also, we do not want the crooks to shop. We do not want them to go to the providers who they know keep the data—and it will not take long to work out who keeps the data and who does not keep the data. We do not want them to sit there and say, 'That's the best network to go if you are a criminal, because we know that they are not going to keep the IP addresses if it is dynamic. They are not going to keep it for any length of time. They might keep it for three months, because that is what their business model says, but beyond that that is fine. Why we do not go to one of the big ones at the moment is because they keep it for—for however long they keep it—'a long period of time'. We do not want that to happen. We want a consistent model, so that we have a level playing field and the people we are trying to combat against also have a level playing field.

Senator BUSHBY: Is there any evidence that that is occurring at this point?

Mr Phelan: Absolutely.

Senator BUSHBY: That they are shopping?

Mr Phelan: Absolutely.

Mr NIKOLIC: So if I understand the tactical risk, you might identify an individual that constitutes a terrorist threat or a threat relating to serious crime and you might then be seeking to do pattern of life analysis about that individual—looking back at who they have spoken to and what the other potential links might be. But telecommunications company X might keep that data for 12 months, two years or whatever the time may be but other people within that network with another provider might only keep it for six months. So you get an incomplete picture of those links that you are trying to establish. Is that the tactical risk that you are describing?

Mr Phelan: That is right. If I picked any major investigation that we do at the moment and I gave you a massive link chart here of all of the links between the ISPs, the SIM cards, those in real names, those in fake names, the numbers of the phones put in et cetera, we would be able to do a big link diagram but in a component of it there would be gaps because I would not be able to go any further because there would not be any information if it went to one provider as opposed to another. If I were to draw that exact same chart in five years' time it would be significantly smaller because there would be less and less data. If there is less and less data there are fewer links—and it is the links that are absolutely vital to any criminal investigation. The worst thing is your unknowns.

We have had terror investigations in the past, such as Operation Neath, which we have referred to before, where, but for the use and exploitation of metadata—so not the content which we got later on under warrant but the exploitation of metadata—we would not have been able to get the links to actually identify the offenders who were going to perpetrate those acts. That was a terrorist incident but, as Mr Dawson said, it happens with every single serious and organised crime investigation that we are doing around the country.

I can talk about what the AFP does. We have done around 25,000 requests for metadata. That is a small proportion of what the state police are doing. If you think we get contracted by not having access to it, imagine what the state police would be able to do in investigating homicides, kidnappings, extortions, armed robberies and all those sorts of things—not just drug trafficking, child exploitation material and NCT matters. It would be devastating for law enforcement. It would send us back to the Dark Ages.

Mr NIKOLIC: On the dataset point, if I understand the way the bill and the regs work, there are seven categories of data that industry is obliged to retain and they are specifically set out in the legislation, but the regulations then provide that greater technical specificity relating to those things that are set out but only within those seven categories. I am interested in your response to criticism that, by virtue of the regulations, this somehow creates a carte blanche situation about what may or may not be accessed in the future. Could you talk a little bit more about how that structure works?

Ms Harmer: The structure you have outlined is correct. The bill prescribes certain classes that may be the subject of regulations to set out the detail of the data elements to be retained. There are six categories in the bill. They are broad categories: information about the subscriber of accounts; information about the source of the communication; the destination of a communication; date, time and duration of a communication; the type of communication or relevant service used; and the local of equipment used in connection with a communication. What that does in the bill is to clearly limit the classes of information that may be kept and then the regulations may be used to prescribe in greater detail the range of identifiers that would need to be kept for those particular classes of information. Then the regulations may be used to prescribe in greater detail the range of identifiers that would need to be kept to support those particular classes of information.
Mr RUDDOCK: On that same matter, are there certain practices in relation to these matters. Putting everything into legislation creates a degree of inflexibility, when you might need to make minor modifications at a later point in time. I assume that that is the reason that some of this detail is in regulations rather than in the act.

Ms Harmer: There are a couple of reasons why regulations have been used in this particular instance. That is one of them. Obviously, regulations provide some flexibility to modify in circumstances where there may be changing practices within the industry. The industry have directly indicated that they foresee significant developments in telecommunications services—not just in the medium and long term, but even in the short term. It is a quickly evolving environment.

Another key factor is, of course, that the matters to be prescribed are quite technical. They are at a level of detail that is typically more commonly in regulation rather than in primary legislation. It is quite lengthy and quite detailed. For that reason, as well, they are included in the regulations.

Mr RUDDOCK: There have been some suggestions in submissions made to us that we ought to require everything to be in the act. I want to know what difficulties that would create if this committee said: 'For more abundant caution we think everything should be in the act. Then it has to be a new bill that will vary it and the parliament will have greater control and oversight. People will be more confident because the parliament is going to have greater oversight.' Why shouldn't we do that?

Ms Harmer: There are a number of different approaches, as the committee will be familiar with. All could be in legislation; all detail could be in regulations. Alternatively, what we have here is what might be described as a hybrid model, under which the key criteria or threshold issues are described in the legislation, with the detail being left to regulation. That provides a degree of flexibility in the event that changes are required, while still providing the opportunity for parliamentary consideration of regulations that are made under that act.

Ms Hartland: From an operational perspective, one of the things that we are seeking is to ensure that this can be as technology-neutral as possible because of the rapid change that is occurring in technology. As the committee is aware it is very rapid, so it is about getting that balance. If you are too prescriptive then technology is going to take over within a very short amount of time, but then you need to be able to provide clarity from an industry perspective.

We have certainly looked at this in terms of the outcome we are trying to achieve—not how it is achieved by the companies themselves. So we are trying to be prescriptive to a point, but not overly prescriptive so that it defeats the purpose of being technology neutral.

Mr CLARE: Just to the point that Mr Ruddock has raised, there is a question of whether the data set goes into the bill or into the regulation. I think the Joint Standing Committee on the Scrutiny of Bills made the point that they think it is an inappropriate delegation of authority to go from the legislation to the regulation. What you are saying is that there is nothing that would stop the dataset being in the legislation if it was the view of the government that it should be embedded in the bill rather than the regulation. Is that right?

Ms Harmer: There is no legal requirement that would preclude such information being included on the face of the bill.

Mr CLARE: My second question—and final question on this point—is that the same committee recommended a number of other alternatives, such as procedures through the House of Representatives and the Senate that the regulation might be tabled in, or merely just rest in the House for a set period of time. Does the Attorney-General's Department have a view on some of the recommendations made by that committee in that respect?

Ms Harmer: I should say that the Attorney-General has not yet responded to the Scrutiny of Bills Committee report. Naturally we are aware of it, and have considered the issues raised in there. I anticipate that we will respond in due course during the consideration of this bill. The only thing I could say in relation to the range of alternatives is that—as I said in response to the previous question—we have considered, and are aware, that there are a number of possible alternative approaches to prescribing the detailed range of information that was proposed in the dataset—from the act to regulations and the hybrid model, which we have had a look at.

One thing I would draw the committee's attention to is a recommendation in the implementation working group's report about a procedural aspect of how any regulation changes might be dealt with. The implementation working group has suggested ensuring that, around commencement of any changes, there is a period for any changes to be considered by industry and to be properly considered by the parliament up until the expiry of the disallowance period. We will respond to that report. We are certainly aware of the issue and the possible alternatives.

Mr CLARE: But the response to that report may be after we table our report, I suspect.
Ms Harmer: I would anticipate it would be prior to that. Naturally I could not commit the Attorney to it. It is the Attorney's response to that report. But we would certainly anticipate responding to that in the near future and prior to this committee's conclusion.

Mr NIKOLIC: If I understand the submissions we have heard this morning, you are about speed and agility. You are talking about an adaptive enemy that has adapted since 2001. If I understand what you are saying, your ability, then, to adapt to future changes it might make is more easily accomplished by having the technical specificity in the regulations rather than enshrined in legislative change, which would need to be amended over time. You can take that as a comment.

I will move on to my next question, which is about some of the criticisms around non-warranted access to metadata. Some see it as exceptional and troubling. Indeed, some of the public commentary in the submissions I have seen almost tries to invest in the metadata the same sort of privacy sensitivity as you would find in the content of some of the data that is produced. So I am wondering to what extent you consider non-warranted access to metadata exceptional. Where else in law enforcement do we already find non-warranted access to records and information which would reasonably attract similar sorts of privacy concerns?

Ms Harmer: Agencies can probably comment from an operational perspective on their practices for the range of information that they access. But, while there are warrants for access to some types of information and tools, warrants are typically reserved for those tools that are most intrusive. The committee has already commented today on telecommunications interception warrants, but there are a range of other warrants for more intrusive steps—search warrants et cetera. However, access under alternative mechanisms is certainly by no means unprecedented. Indeed, it is common through 'notice to produce' authorisation processes et cetera to access more routine ranges of information that are less intrusive. Telecommunications data, as we said, is a basic data point. It is typically used at the beginning of investigations to commence inquiries, to identify inquiries and to pursue those. It is a relatively less intrusive range of information. It is also often required to progress investigations quickly and to provide the information that is then required to support something like an interception warrant. So it then supports warranted access to other tools.

Ms Hartland: I will just add to that. As Ms Harmer said, metadata is often used as our first point in an investigation. So we see it as the least intrusive stage. It is as much to rule people in as to rule people out of investigations so that we do not then need, in many cases, to go to another higher level of intrusion. But I would not want the committee to think that there are no checks and balances for the data we collect. ASIO officers have to collect information using the most effective means. It has to be proportionate to the gravity of the situation. It has to take into account the level of intrusiveness. That is done under the Attorney-General's guidelines and in accordance with our own codes of conduct. As the level of intrusion increases, the level of delegation of an individual signing off on it goes higher. So it is proportionate, if you like, to that level of intrusion.

If there was a warranted regime for the sort of metadata that we are talking about here it would have a grave impact on our operational response and agility in these areas and would impose a sort of overlay and consequential delay in being able to assess and respond to emerging security threats that we think is beyond the level of intrusiveness that is involved.

Mr Phelan: It is the same with us in terms that I do not want anybody to be under the illusion—I think I have used the words 'willy nilly' with the committee before. We are very careful about the authorisations and the type of information we want and when we want it. The authorisations in the AFP are up to commissioned officer level, so only a commissioned officer can authorise the access to the communications data. We do not do it all the time; we do it when we need it because we actually have to pay for it as well, as it is at the moment. It is not free.

It is a point worth making that to move to full warranted application to do so is a very long and onerous process, and rightfully so, for intrusive actions. Whether we are doing telephone intercepts or whether we are using the metadata to form the basis of information to do a search warrant on someone's house, all those authorities have to be done in some form judicially. So we believe that it is most appropriate that we have the checks and balances in place. The AFP last year—and again recall that it is only a small percentage of what all law enforcement agencies do across the country—had 25,000 odd authorisations for 56,000 actual pieces of data or different services. If we were to get a warrant for each one of those, and it is roughly eight hours an application to put a search warrant together—that is how onerous they are to do these days—you are talking about 200 people taking a year to put that together. That is 20 per cent of my investigative capacity in the AFP.

Ms Hartland: I should also say that, in ASIO's case, the IGIS has oversight and full royal commission powers to look over the way that we collect and use data. As Ms Jones pointed out earlier, and I will quote from her most recent report, she said that she 'did not identify any concerns with ASIO's access to prospective and historic telecommunications data. My officers' oversight of this particular technique decreased during this reporting period.
due primarily to changes in our inspection program and the high rate of compliance in this area.’ So there are checks and balances there and warranted activity provides another level of intrusion and another level of checks and balances over the top of that.

**Mr NIKOLIC:** In those areas where there is already a precedent for unwarranted access—be it banking, finance or health records—can anyone on the panel tell me whether there has been an upsurge of complaints or criticism that there has been a free-for-all in accessing that material, as some are suggesting might be the case for metadata access?

**Mr Dawson:** Mr Nikolic, I am not aware of any other sectors that are complaining about a civic duty that has been put upon them, and the example you just referred to in terms of the financial sector is a good example. We have notices to produce that get served on financial sectors from all police and law enforcement agencies across the country—

**Mr NIKOLIC:** Unwarranted.

**Mr Dawson:** Unwarranted. And those investigations are generally over a regime which requires those institutions to hold those records for seven years, not two. So they are a necessary way of discovering and understanding what is the nature of the allegation. If I could refer back to the data issue that was just raised, the Australian Crime Commission has only 20 authorised officers who have oversight and have the delegated authority to require such information, and it is under a regime again by numerous oversight agencies. We have got about five or six that oversee the Australian Crime Commission in one form or another. Again there have not been any instances that I have been made aware of that have complained about the nature of those requirements for a telco to produce such data.

I might just add, though, in response to your earlier question, in terms of the discrepancies and divergent nature of the carriers that we deal with, some of the larger carriers only hold data between one and four months; so they will purge those records. There are numerous other providers that are beyond the larger bigger companies; there are quite a number of subcontracted services where the smaller operators do in fact require or have a commercial arrangement for those larger carriers to hold certain data sets for them.

**Mr CLARE:** Just on this issue of warrants, in August in the *Sydney Morning Herald*, a story by Latika Bourke reported that the former head of ASIO, David Irvine, had suggested that he might be willing to accept more oversight when it comes to accessing metadata, including requiring authorities to secure a generic warrant that is not currently required. The former Independent National Security Legislation Monitor, Bret Walker, has also made public comment that he would support the idea of a generic warrant. He said that, if sensibly devised, it would be an appropriate high level of accountability here. I am interested in ASIO’s advice about what a generic warrant would mean or consist of and, in particular, how it would be different from the existing authorisation process.

**Ms Hartland:** Thank you for that question. I am aware of that article on 8 August. I think it followed a joint press conference that was given with Commissioner Colvin relating to data retention. I think it is useful to point out that the full context of Mr Irvine’s comments had not been aired in that report or in reports around that. You rightly say it was in response to the former INSLM’s comments—I think it was post him being the INSLM, if I remember correctly—about that idea of a generic warrant. It was put to the then Director-General: would this be workable? His comments were reflecting: if you could make a broad class of warrant that was not done on an investigation by investigation or a case by case basis then we could have a look at that. It is hard to envisage how you would get the thresholds around that and, indeed, whether, by making that as broad as it would need to be, it would actually provide any additional assurance or whether it would just be too broad. We have put some thought into that. I think it would be quite difficult to have a very generic warrant. As I said, it would end up being of a nature where I am not sure that it would add very much in terms of accountability because of the breadth that you would need.

**Mr RUDDOCK:** They would give you a warrant to investigate all terrorism investigations.

**Ms Hartland:** Correct.

**Mr CLARE:** We would obviously need to explore this area in a bit more detail. We have got submissions from the Law Council that recommend a warrant based process. We have got the recommendation of the Joint Parliamentary Committee on Human Rights that recommends a warrant based process. We have got a submission from the University of New South Wales that is recommending a ministerial warrant based process similar to the way processes work for the Attorney-General and ASIO at the moment. And then we have got the former head of ASIO suggesting there may be a generic warrant based process and that has been endorsed by the former National Security Legislation Monitor, Bret Walker. So I think this is deserved of some serious investigation and
consideration and advice back to the committee about how this might work and how it may be different from the existing authorisation process, particularly given that in many of the other jurisdictions overseas where we have mandatory data retention there is some additional level of judicial approval or extra approval processes before the data is collected.

Ms Hartland: Could I go back to some earlier comments. We are not seeking—and I think Commissioner Colvin said this as well—access to information which we do not currently have access to. So we are not looking to extend that. What we are looking to do is to look for a consistency of a regime and, I guess, a level playing field amongst providers.

If a warrant regime were to be anything other than an extremely broad system, I am not sure it would add very much in terms of accountability. It would significantly impede our operations, the level of agility. As I have also said, the level of intrusion we see involved in this versus warranted activities is very much different. It is as much about ruling people out as ruling people in, so we do not have to go to that extra level of intrusiveness. We do see that as a step. It is in the same way that my colleagues have said: the internal authorisations around this are to a select group of people involved in operational activity; it is not as if there is open slather.

The other thing I might add is that I know commentary is often made about us trawling through data for security purposes. We can only ever legislatively look for material, seek data, when we believe there is a nexus to security. We do not have the resources, ability, time, energy or inclination to be trawling. These are selective. We are looking at individuals of security concern. The concern expressed by some in the public—that we monitor communications of all Australians and that we are seeking to do that and that this would provide that—is erroneous.

Mr CLARE: I have a final question on what Mr Irvine might have been suggesting, in terms of a generic warrant process. Is it your understanding that this would then be some form of different level of internal approval that would happen inside the relevant law-enforcement agencies?

Ms Hartland: Yes. If I read further to what he said, he said it depends on what the warrant system was. He said:

If it was a general warrant that said ASIO can collect metadata in the pursuit of its legal functions, then I can live with that. If it's a warrant that is required for every single request for metadata that we make, the whole system would come to a halt. It's the equivalent of asking you to write a three-page letter every time you want to look up the telephone book.

Mr CLARE: So it is a warrant issued by a judicial officer, but it is of a generic nature rather than a different level of authorisation inside the organisation itself.

Mr RUDDOCK: A warrant for ASIO is really a turning point.

Ms Hartland: When we speak of warrants we speak of warrants signed by the Attorney-General.

Ms Harmer: I would like to add a couple of other comments to that discussion in relation to the authorisation process. The absence of a requirement for a warrant does not mean, as a number of other agencies have said, that there are no processes or accountability. Thresholds for access to data under an authorisation do require consideration of the extent to which the particular data being sought would assist in performance of legitimate functions, such as the enforcement of the criminal law, and do require the authorising officer to consider the impact on privacy of the person whose data is being accessed. So there are issues required to be considered, on a case-by-case basis, through the authorisation process.

There is also some guidance coming out of the United Kingdom, where there are some warrant requirements for a small subset of access to data. A recent finding by the Interception of Communications Commissioner, Sir Paul Kennedy QC, who has provided an annual report to the UK parliament, is that he has recommended that the arrangement for access through warrants, in that particular context, be repealed—because of the significant risks it entails.

Mr RUDDOCK: On this same matter, I am very concerned about the extent to which agencies dealing with terrorism investigations, for instance, are impeded by unnecessary and very complex and costly processes that limit their capacity to go after the crooks. I ask myself the question: for the 30-odd thousand that you say the police needed of authorisations to get access to metadata, what is the cost of each authorisation? What would be the average cost of getting a warrant for every one of those authorisations? What would it do to the capacity of the organisation to carry out its functions?

I just get the impression that we are being totally unrealistic, and I would like to have some objective data that just demonstrates that it would impede the effectiveness of the organisations that we are relying upon to deal with these very significant investigations.
Mr Phelan: As I said, I only did it just on the back of the envelope, but I know how long it takes for our investigators in this day and age, in 2014, to put a search warrant together. They are very complex documents now. It was a lot different when I put one together 25 or 30 years ago.

Mr Ruddock: Opportunity cost—$1,000 for each warrant?

Mr Phelan: More than that. It is going to take at least eight hours a person—56 times eight. I am talking about 200 people in addition that it would take.

Mr Ruddock: So each warrant might cost $10,000.

Mr Phelan: Easily. At least a thousand bucks—a day's worth of work for each single one. You are talking millions. It is the back of an envelope here: the additional cost or the opportunity cost to our organisation would be at least $25 million a year.

Mr Ruddock: And there would be 30,000 judges who have to make their time available. Have we included the cost of that.

Mr Phelan: No, that is just our cost.

Mr Dawson: I might add that the national figure is in excess of 300,000, because the vast volume is done by law enforcement through the state and territory police, in addition to the 25,000 that the AFP spoke to earlier. So it is not only the preparation of affidavits and the attendance. Most of the warranted information is required to be represented by a legal practitioner, not a police officer, so you have to engage lawyers to go before the AAT and/or a judge, and they must be backed up by affidavits that often range anywhere from 20 pages to in excess of 200 pages—I have seen affidavits of that length. So the laborious nature of it is one point.

I think the other point we need to reinforce is the dynamic nature of the changing technology and, indeed, the applications and the devices that are now used. When a person is walking through a shopping centre, for instance, they are jumping from carrier to carrier to carrier with devices and applications. The digital technology is such that the broad nature of this is far different from what the 1979 legislation contemplated when it was copper wire technology with about three or four carriers. We now have several hundred carriers, and they are using voice over internet as the major digital system by which this is done. So not only is the crime that we are dealing with dynamic but you do not have the hours. You have, in a dynamic situation, the need to respond very quickly, but even in the more long-term investigations, with a subscriber, they are not always pure as the driven snow. So they do not actually acquire the SIM cards under their real names. That would not be a phenomenon when a drug dealer would be procuring a device, because they are not going to put it under their real name. So we have to then interdict those sorts of activities not knowing who we are dealing with, and we then have to try to investigate and unclutter the various devices and where they are being used in a very dynamic situation.

Ms Jones: Could I also just add in that context that obviously the bill proposes new oversight by the Commonwealth Ombudsman, and I think in that context that was recognised as an important part of the overall framework, noting the psychological influence that has on the way people operate when seeking access to data retention and recognising there is a comprehensive oversight regime. We know already about the IGIS and the role that it plays in relation to ASIO. It looks at the compliance with requirements for ASIO and has recognised that the compliance is very strong and very positive. I think we need to have the mechanisms of independent oversight and get the balance right in ensuring that the law enforcement agencies and intelligence agencies can act quickly and promptly in response to particular investigations that they are undertaking but that there is that layer of oversight that will ensure appropriate compliance, taking into regard the types of issues around privacy that we are all concerned about.

Mr CLARE: On a slightly different topic, Mr Ruddock talked earlier about the timeframe under this legislation of retaining data for two years. I just want to clarify something. My understanding is that there is only one other country in the world that, under legislation, requires internet data to be retained for two years or more, and that is South Africa. I just wanted to check with the department whether that is their view. I am talking here about internet data, not phone data.

Ms Harmer: I think there is at least one other country in that regard. We are intending to provide the committee, in the department's submission, with a broad overview of data retention, retention periods and practices across a range of countries. I think it may be Italy, but I cannot—

Mr CLARE: My understanding, and maybe we could check today, is that for South Africa it is three years; for Latvia, 18 months; and for Italy as well as Ireland, one year for internet and two years for phone. That would mean that what is being proposed here in this legislation, with the exception of South Africa, would be the longest timeframe worldwide.
Ms Harmer: Yes.

Ms Hartland: I think the directive is up to two years, and different countries have different regimes in that. But I will defer to the department.

Mr CLARE: But the status of that directive now I guess, given that court case is—

Ms Hartland: Yes.

Mr CLARE: And this one may be something that agencies can or cannot answer at this time, but international experience I think shows that about three-quarters of the data that is sought is usually six months old or less, and around 90 or 95 per cent of the data is one year old or less. I am wondering whether the department or agencies could comment on that.

Ms Hartland: We have certainly included some detailed information in our classified submission on this, but, as I think I mentioned in my opening statement, it is true that 90 per cent of the data that we obtain is in that 12-month period, which leaves 10 per cent that is longer than that, and obviously a smaller percentage as you go out. But the difficulty in that is that you cannot compare to say that that 10 per cent is the least important and that 90 per cent the most important, because in dealing with particularly complex and long-running cases and plots it may well be that the 10 per cent or the two per cent outside, at the longest length of retention, is actually the most crucial information that you are looking for in terms of networks and, as I think I said earlier, in terms of particularly espionage cases and cyber cases. Those sorts of things can go out for very long periods of time.

Mr CLARE: But it appears almost without exception that countries around the world have opted for 12 months or six months.

Ms Hartland: And I think—and I cannot speak for other countries—it is about trying to find that compromise between the security and privacy concerns. If you asked any intelligence organisation around the world whether they wanted to have access to data for a longer period of time or for a shorter period of time, I think I could say with great confidence that it would be for a longer time.

Mr DREYFUS: As a follow-up to that, I think the committee would be assisted if someone could indicate—to the best of your ability, and perhaps not now; you could take it on notice—why it is that almost all countries that have data retention regimes have opted for a shorter period than two years. I think that is where Mr Clare is going with this. And I appreciate that Ms Hartland says she does not know—fair enough—why other countries have gone for six months or a year. But it would be of assistance if the department were able to provide us with some information about why that might be so, because I am assuming that law enforcement needs and counter-terrorism needs here in Australia are not substantially different from those in comparable countries.

Ms Harmer: There are some insights that we can provide to the committee, and, as I foreshadowed, we intend to provide the committee with a submission that will outline at an overview level what those practices are. Clearly the committee is already familiar with a number of those. Those retention periods are in most cases guided by the former EU data retention directive, which mandated that member states retain data for a minimum of six months and a maximum of two years, which is why we see that pattern of anywhere between six months and two years. Obviously those member states have selected the retention period that they have applied. It would be difficult I think for the department to speculate on the particular motivations and views and reasons that the particular retention period was reached in those jurisdictions. But we can draw attention to observations that have been made in those jurisdictions, to a number of findings that have been made in the evaluation of the data retention directive about the value of older data in relation to particular crime types, and to some recent observations in a number of countries that are looking again at their data retention arrangements—in some cases to extend the retention period and in other cases to acknowledge that the current retention period or the range of data that is retained is not addressing operational needs. So where we are able to do so, we will draw attention to those issues and that international experience.

Mr Phelan: On the discussion about times, from a law enforcement point of view, there is absolutely no correlation between the length of time—how old the information is—and the value of that information, at the end of the day. Depending on the type of investigation, there is no correlation at all. It could be as important if it was five years old, two years old or 10 years old, or if it was yesterday.

Mr CLARE: I have a topic I want to pursue with the Attorney-General’s Department. Once the data is retained, what are its implications for the purposes of civil litigation, particularly this sticky issue of piracy? The Attorney has indicated that law enforcement agencies have no interest in using that data to pursue people illegally downloading material—and I do not want to go down that path. Some of the submissions that we have received—for example, the Law Council’s submission—made the point that limitations need to be imposed on how these data can be used for the purposes of civil litigation. The Communications Alliance has also expressed some
concern here that we might be creating a honeypot that people can use for the purposes of discovery for their purposes, civil litigation, to pursue people that are pirating material. This is a complex, difficult area. I am conscious that you would be disturbing existing practices by changing the law here. The Attorney-General's Department would be aware of this issue. Has the department given any thought to the implications for civil litigation of this legislation and would you be contemplating any changes here?

Ms Harmer: The telecommunications industry already retains a wide range of telecommunications data for varying periods. The Telecommunications Act administered by the communications portfolio does regulate the disclosure of that information outside of those circumstances which we have been addressing here—being the support of security matters and enforcement of the criminal law pecuniary penalties and protection of public revenue. So there are already frameworks around the circumstances in which carriers can disclose that information and there is already oversight of that by the Australian Communications and Media Authority around the number of instances and circumstances in which telecommunications data is disclosed other than for those law enforcement purposes.

Mr CLARE: With civil litigation there is a discovery order, people want to find out—a bit like the speculative invoicing we have seen in the case of the Dallas Buyers Club. You now have all of this data available that a content producer can use in order to try to dig a bit deeper and find out who is illegally downloading their material. Under the existing law, they would have the right and ability to pursue that in court. This additional data that is being preserved that otherwise might disappear over the course of the next five years or so would be available to pursue through those court orders. Does the department think that there needs to be some change there to the way in which civil litigation might operate?

Ms Harmer: It is the case, obviously, that data that is already available and data that will become available in accordance with data retention is available and amenable to other lawful process, including in the civil space whether that be through subpoena or other orders for production. Production in other contexts itself raises a number of challenges and the ability for persons in those proceedings to adduce such evidence as is relevant to their proceedings, and of course it extends into such matters as family law, other commercial situations other than the rights space, which has been the subject of some coverage. It is the case that that data would be available and it has been for some time and is amenable to that process.

Senator FAWCETT: Before I go to my questions, I want to put on the record my support for Mr Ruddock's comments around the administrative burden decreasing the efficiency and ability of the agencies to react. I have a deep concern about that. My substantive questions go to schedule 2 and section 110A and the complementary section 176A around the declaration of law enforcement agencies. Subpara 6 states: The declaration may be subject to conditions. Does the Attorney-General's Department have any view or have you considered what those conditions might be—whether they would be temporal in nature, whether they might reflect the scope of data that other declared agencies could access or whether they would apply to the thresholds of their access?

Ms Harmer: The provision is not limited in the conditions that may be imposed, so the Attorney would be permitted to take into account any relevant consideration and to impose such conditions as may be appropriate to access to data by the agency that is to be declared. Without limiting the kinds of conditions that might be imposed, it may be that, for example, the Attorney reaches a view that access to data would be appropriate in respect of some of the functions of an agency but perhaps not all. Alternatively, it could be the case that access to data might be appropriate in relation to some elements of the dataset but not all—for example, subscriber information as opposed to the traffic information, being the other five categories of data. So it would be open to the Attorney to consider a range of conditions that are appropriate to that particular agency's performance of its functions in support of enforcement of the criminal law, protection of public revenue and pecuniary penalty matters, taking into account the oversight arrangements that that agency has, in relation to both the use of its powers and its privacy arrangements. It provides a flexible mechanism for the Attorney to make appropriate conditions.

Senator FAWCETT: Some of the concerns that have been raised go to the range of agencies that have to date been able to access metadata, going right down to local government and animal protection groups et cetera. There have been some suggestions that perhaps definitions of a law enforcement agency's limitations around the kinds of functions should actually be more clearly defined in the legislation. Has any thought been given to a practical way to put some hard markers to exclude some groups and some functions that clearly are outside the scope of what is intended whilst still allowing the flexibility for the Attorney to include and declare those groups that have a valid function?
**Ms Harmer:** The bill, I think, in some respects is intended to do precisely that. It identifies the class of agencies that may have a legitimate need to access data in the performance of their functions. So agencies that are involved in the enforcement of the criminal law, the administration of pecuniary penalties and the protection of public revenue are ones that the parliament has already envisaged through the legislation as it currently stands may be have a need to access data. The bill imposes an additional limitation upon that and says that, rather than your membership of that broad class creating an ability to access data, in addition there should be a requirement that the Attorney-General explicitly consider the extent to which data is required in support of those particular functions, the particular oversight arrangements that apply for an agency that wishes to access data and the extent to which that agency is the subject of binding privacy obligations. So the bill does insert a new mechanism to ensure that it is very clear which agencies are included and to provide key thresholds around that. There will be a clear list of agencies that have access to data, and for those that are not in there it will be clear that they do not.

**Senator FAWCETT:** Of those agencies who have an ability to prosecute people in both criminal and civil matters, ASIC would be a classic example. Is there any reason why a group like ASIC was not already listed in that list of agencies? Would it fall under section 110A or 176A for a declaration?

**Ms Harmer:** The list of agencies that are included on the face of the legislation are ones that the parliament has already recognised explicitly as those that should have access to data. They are already included either in the Telecommunications (Interception and Access) Act as it currently stands or in regulations made under it as ones who should have access to telecommunications data. The bill reflects the parliament's existing intention that those agencies have access. All other agencies have the ability to seek a declaration, to the extent that they are agencies involved in the enforcement of the criminal law, protection of public revenue et cetera—those categories that I have mentioned—to enable them to access data. You have given one example, ASIC, but there are a number of agencies that do have functions in the enforcement of the criminal law and protection of public revenue and have used data in the past and consider it to be an important part of the tools that they would use.

It is the case across the states and territories as well that state governments have given a number of agencies other than traditional policing agencies functions in relation to the enforcement of criminal law and bringing matters forward in the criminal space and elsewhere. So those agencies that have those functions are able to seek a declaration. It would obviously not be appropriate for me to pre-empt the extent to which particular agencies might be positively considered for such a declaration, but we certainly acknowledge, through the inclusion of the declaration process, that there are agencies who might properly be so considered, and the bill provides a series of criteria which those agencies must address before they should be brought into the scope of the scheme.

**Senator FAWCETT:** Do you have a feel at this point in time for the length of that declaration process—let us take ASIC again as an example—from the date of passage of the bill, or approval, through the parliament? I think you have got six months—that is my understanding—before it would come into effect. Is there a guarantee, if you like, that agencies such as ASIC would be guaranteed uninterrupted access, assuming the Attorney accepted their case—which I think in ASIC’s situation is fairly apparent—such that there is no interruption or gap in their ability to access data?

**Ms Harmer:** The change in the agencies who can access data would not take effect until the commencement of the bill, in the event that it is passed. That is, as you said, six months after royal assent would be given. So that does provide a significant window in which agencies could make an application and seek a declaration. Naturally, of course, the extent to which the Attorney can make a declaration is influenced by a number of factors, including the extent to which agencies bring forward information and make such an application in a timely way to enable it to be considered. But the department obviously has a role in advising the Attorney and considering such issues, and they would be considered as part of the department’s business and provided advice so that those matters can be considered by the Attorney in a timely way.

**Mr DREYFUS:** I want to turn to a different matter, which is cost. There have been estimates made by a range of industry participants that the cost of a mandatory data retention scheme would be in the hundreds of millions of dollars. I mention that because the range of estimates is extreme, ranging from tens of millions to hundreds of millions. Those estimates were made at the time of the 2012-13 intelligence committee inquiry. I will start with a simple question: are you in a position to say what the proposed mandatory data retention scheme is going to cost?

**Ms Harmer:** On that front, as the government has indicated, there is a range of work being done—and engagement with industry—to examine the implementation of data retention and to assess the costs of implementing the data retention regime. Industry, as you have noted, have presented a range of views, and a number of cost estimates have been circulated. I should say that a number of those cost estimates, I think, were made at a time prior to the introduction of draft legislation and prior indeed to the circulation of a draft data set which articulated a significant number of exclusions from the operation of the scheme which ensure that it applies...
to both a limited subset of data and a limited section of the industry that it applies to. So costing work in that regard is continuing, and industry are active participants in that. I am sure that a number of those industry participants will have views and will provide them as well.

Ms Jones: If I could just add to that, and I think it is consistent with some of the evidence that has been provided by our colleagues at the table here, just in the terms of the variability of the practices in the industry—the nature of their business models, the way they have information et cetera, means that any form of accurate costing of the implications of the provisions in the bill do require quite detailed consultation with industry, which is what we are doing at the moment. We have been working fairly closely with them, but, in terms of the types of estimates, they are not capable of being done without that close discussion and analysis, because of the different types of models that each of the providers are operating under.

Mr Dreyfus: I saw in the Implementation Working Group report that the government engaged PricewaterhouseCoopers in September 2014 to do a cost analysis. I read in the document that was provided to us last night this sentence at the foot of page 15—this is the part of the report that deals with assessment of the costs: [PricewaterhouseCoopers] consulted selected telecommunications industry participants regarding their current data retention practices, as well as their estimated costs of compliance with the proposed obligations.

The next sentence says:

Notwithstanding consultation on the draft data set, consulted providers observed that they did not consider they could provide accurate costings without draft legislation articulating and evidencing the data retention obligations.

The report then goes on to say that work is going to be ongoing, conducted by PwC. Are you in a position to indicate when it is thought that the cost of the proposed mandatory data retention scheme will be able to be estimated?

Ms Harmer: As I said, costings work is ongoing and the government is engaging closely with industry. We are seeking relevant information and collaborating with industry on what the impact is. That work is continuing, but naturally it also depends on the ability of industry to provide relevant information. As Ms Jones said, there is significant variability, which means that the impact on individual providers may be quite different and so that is a complex piece of work that is continuing.

Mr Dreyfus: If it is the case, as this Implementation Working Group report indicates, that no-one is prepared to provide an accurate costing without draft legislation that sets out the data retention obligations, then will it be the case that this committee is unlikely to have accurate costings provided to it?

Ms Harmer: Perhaps if I could clarify the comment that is in the report: that reflects comments that were made to PricewaterhouseCoopers during their preliminary analysis of costings, which took place prior to the introduction of the legislation. So that comment reflects that initial observations were informed by what could be indicated at the time. It is now the case that a bill is before the parliament and a proposed dataset is now well advanced and is the subject of consultation. Now that information is available to industry, it will inform those more detailed costings. Industry have advised, during the course of the Implementation Working Group, that it is the case that they consider that the bill and the proposed draft dataset do provide them with sufficient information to prepare implementation plans and, through that, obviously to cost what that implementation will be.

Mr Dreyfus: At the foot of page 17, which is headed 'PwC's key findings', we read:

• Further costings work is required and will be undertaken by PwC over the next month. [Attorney-General’s Department] and PwC both appreciate industry’s further engagement in the process.

Will this committee be given a costings estimate during the course of its deliberations, bearing in mind that its present intention is to report at the end of February?

Ms Harmer: As I said, that costings work is ongoing and industry are providing information to support that. While we have sought that assistance from industry, I do not know that I could say when we would necessarily have that information. I envisage that the committee would certainly seek views from industry on their thoughts on the cost of implementation, which, as we have said, vary considerably and so a number of providers will have substantially different costs.

Chair: I would also assume that industry will be prepared to give their views on this subject when they appear before us.

Mr Dreyfus: In the opening statement that Ms Jones made, she talked about several recommendations of this committee's 2013 report, notably recommendations 42 and 43, which were setting out detail of what this committee thought would be appropriate to provide for if there was a decision to go forward with the mandatory data retention regime. Part of recommendation 42 was that the costs incurred by providers should be reimbursed...
by the government. I wondered if you could confirm that the government is not implementing that recommendation in this bill—is it?

Ms Harmer: The government has indicated that it will make a contribution to the cost, but that is correct: it has indicated it will make a contribution to the cost rather than bearing the entire costs of data retention. It is the case already that industry bear a number of costs in relation to interception capability and related issues, being costs of a service that they provide and consistent with other sectors of industry that have an impact and provide support to law enforcement. But in the context of data retention the government has determined that it will make a contribution to those costs.

Mr DREYFUS: On that, Ms Harmer, the phrase that is used in the implementation working group report refers to making a reasonable contribution to the capital expense of implementing the proposed data retention obligation. Are you able to flesh that out at all—whether there is any meaning that can be given to 'reasonable contribution'?

Ms Jones: In terms of the concept of reasonableness I think it is an assessment based on the overall cost. In relation to some providers the obligations in the retention scheme may require minimal adjustment to their current infrastructure or practices; for some it might be more. It is difficult to be more precise. I think we should take 'reasonable' in the general understanding of the word. It will depend on that close work we do with each of the different providers and an understanding of what are the adjustments, if any, that they need to make in order to be able to comply with the requirements under the legislation and have a discussion with them in terms of what would be a reasonable contribution to that.

Mr DREYFUS: The phrase used here in the implementation group report is only about the capital expense. Is there any different approach being proposed in relation to recurrent expenses for telcos?

Ms Harmer: The report draws attention to the capital cost because that is the government's decision: to make a contribution to the capital costs which are associated with, for example, reconfiguration of networks to retain data. Naturally there are ongoing costs associated with that but it is already the case under the Telecommunications Act that there is a recovery on a 'no profit, no loss' basis under which providers may recover some aspects of their costs of providing that service, and they do indeed charge agencies in accordance with the work that is required to fulfil a request.

Mr DREYFUS: Is it going to be possible—so that when telcos turn up before this committee and say they don't know—to give some greater clarity to this in the next week or two or three? In other words, before this committee gets to the date when submissions close, and when we hear from telecommunications companies they are not in the dark and we are not in the dark about what a reasonable contribution might be and about what costs the government is prepared to bear?

Ms Jones: PricewaterhouseCoopers, who have been engaged to look at this, are prioritising that work and engaging with industry, and we are waiting to receive that information back from them. I think you will find, as a consequence both of that engagement and in terms of now there has been quite a period of time that relevant providers have had the draft dataset and have been engaging with us at the higher level and also the technical experts that need to understand exactly what the technical requirements are to comply with the bill. They have now had some further time to consider that and I would expect that they would come before this committee with a more detailed understanding and would be able to give you the benefit of their understanding of the cost implications. At this point I can say that we are certainly prioritising the work with PWC and hope to have that concluded as soon as possible.

Ms Hartland: There is some detail in our classified submission as well that answers some of the questions that the committee put to us around some of that—the cost and the amount that we pay to industry. And, as you know, I think the committee is aware, on a case by case basis to industry providers. I would be happy to deal with that further in the classified hearing, but there is some information that we have provided to the committee on that. I think my law enforcement colleagues might add to it.

Mr Phelan: Yes, certainly. I am advised that we pay between $1.5 million and $2 million per annum for access to their data—and I would like to believe it is their marginal costs that they are charging us for that. That is obviously offsetting some of their recurrent expenditure, as opposed to their capital costs.

Mr DREYFUS: But it is some, not all. The recurrent costs would cover not just the retrieval costs but also the sheer cost of maintaining the storage equipment that is being used and systems.

Mr Phelan: Of course. And the telcos all charge different prices for us. Some are charging marginal—just for the actual retrieval—and I am sure some are charging us for overhead costs in addition to that as well.
Mr DREYFUS: By way of analogy: in the electricity transmission sector, there have been suggestions in recent years that some of the transmission companies have been engaged in a practice that is colloquially known as 'gold-plating'—in other words, building more poles and wires than they need to—which has contributed substantially to the cost of electricity in Australia. If the government is using taxpayers' money to bear some or all of the costs that telecommunications companies are going to incur, how is the government intending to ensure that telcos do not engage in gold-plating practices—in other words, bumping up the actual costs so as to recover more from the government?

Ms Jones: In terms of some of the work we have asked PwC to do, part of the purpose of bringing them on board was to ensure that they had some expertise in terms of understanding industry practices so that we could ensure that any reasonable costs that we did contribute were reasonable in the sense that they were necessary in order to comply with the legislation and were not being incurred for other purposes that may be part of their normal business practice. It is a complex issue—to be able to assess what costs are attributable to compliance with the regime—but we will be working closely with PwC. I do note that, on the working group, we have colleagues from the Department of Communications, who have expertise in understanding the communications industry, and they are assisting in those deliberations.

Mr Dawson: In terms of costs—and this goes to Mr Ruddock's question earlier about averaging costs—the Australian Crime Commission estimates that in 2012-13, the average cost per interception warrant, and this is inclusive of another figure, was $34,055. Of that, our estimation is that each interception cost from the carrier averaged $5,675 per request. In that sense, it is also important to understand—and this may be of assistance to the committee—that the larger telcos have a higher residual capability because of systems engineers et cetera. The smaller operators will not necessarily have the internal expertise, so they may well co-opt or contract other people in to furnish the data that is required for each request—they may not have the as a salaried employee.

Mr DREYFUS: To give some context: that surveillance warrant figure relates to real-time interception of a voice call. But that is not what we are dealing with here; we are dealing here with a requirement to force companies to retain what will be historical data. That is quite a different aspect of law enforcement practice, I would have thought.

Mr Dawson: Yes. It is not inclusive of the operating costs of, for instance, investigators either. I am just providing that response in addition to what Mr Ruddock asked earlier because the cost borne by industry—as has been answered by my colleagues—is subject to a degree of further deliberation. I thought that may be of use to the committee in understanding why the datasets are being requested in terms of an interception. It was averaged at over 5,000 per provider, as opposed to the labour costs that Mr Phelan was referring to earlier, that are borne by the interception agency.

Ms Jones: I just note that in terms of the concept of 'reasonable contribution', it is reasonable from the perspective of industry and reasonable from the perspective of government and taxpayers. I think both aspects need to be taken into account. Once we have received some advice from PwC in terms of giving us a more accurate understanding of their sense of what types of providers may need to do in order to comply—and some of them may need to have very minimal capital adjustment in order to be able to comply with the regime—we will be developing a fairly rigorous model in order to assess that on a case-by-case basis.

Mr DREYFUS: I will just finish that cost question off. Possibly my colleagues have some questions about it. I take it that the government has not yet been in a position to estimate the cost to taxpayers of this proposed data retention regime.

Ms Jones: In terms of a precise cost, no, we do not have an exact estimate yet. It will be subject to being properly informed by the work of PwC, and then our consideration of that and the model that we develop in consultation with the Department of Communications.

Senator BUSHBY: Thank you for assisting us today, again. One of the areas that I wanted to cover has been covered already by some of the questions but I just wish to clarify a couple of things. Firstly, looking at the impact of this bill, we have had evidence this morning that there is nothing in this bill that is going to provide greater ability for government agencies to access data. It is really just a matter of maintaining datasets that agencies already access and ensuring that that data is there when needed for investigations into serious crime. I see that you are all nodding.

Ms Harmer: That is correct.

Senator BUSHBY: I was particularly interested in the Deputy Commissioner's comments about the consequences of inaction in terms of the trends in metadata retention at the moment. You made the comment that law enforcement agencies—the state based ones as well as federal agencies—would find it almost impossible to
do their jobs in five years or so if current trends in terms of organic retention of data continue. Would you like to expand on that a little bit for me, please?

Mr Phelan: From our perspective a lot of the information is available. There are some carriers that have it and some ISPs that do not. We work within that environment at the moment. We are saying that, in terms of the amount of information that we currently use—when I say 'we' I mean all law enforcement and security agencies—the pool of information that will be available to us will diminish. A natural consequence of that is that we will not be able to use that data to help build pictures we need to help us solve crimes and prevent crimes. It is the linkages that are important. A linkage that I can get today because the data is being kept—because it might be the switching-information that the telcos are using, for example, if it is a phone call—is available today because it is there. In five or 10 years time, when they switch over to using internet protocol across the NBN et cetera and there are no copper wires, effectively I will be looking at IP addresses that are attached to one individual and another. If they are not required to keep that data then it will not be there. There is no need to keep that data for a commercial reason at the moment because they bill on the amount of data—not who it goes to, and so on. So we want to be able to make sure that that information or those indicators are available and that all those identifiers are available.

Senator BUSHBY: This is information, which is currently accessible by the agencies—

Mr Phelan: Yes.

Senator BUSHBY: and this bill does not change or increase the level of accessibility—has been of vital importance. Mr Dawson provided a number of case studies where it has been of vital importance in solving serious crime.

Mr Phelan: I have been appearing before committees for 15 years and I have never used the word 'critical'. I am now going to use the word 'critical'.

Senator BUSHBY: And the current trend for various business commercial reasons is driving the companies or the providers that hold that information to hold less of that information. And that is really the nub of what this bill is about. It is trying to ensure that information that has been of key importance, vital importance, to investigations over a number of years remains available to law enforcement agencies to conduct investigations in future.

Mr Phelan: That is correct.

Ms Hartland: Perhaps I could just add to that. You talked about degradation or diminution of ability to get this data in five years time. I would just point out that it is happening now, and that is the urgency of it, as Deputy Commissioner Phelan said, in terms of the criticality. So, that example that I have given before today about an ISP that was holding data for years and has now changed its business model to holding that for three months obviously has a big impact on investigations for both law enforcement and intelligence organisations. So, it is very real, it is happening now, and that is the urgency and why we are here today.

Senator BUSHBY: I think Deputy Commissioner Phelan's comments were in relation to that being almost non-existent in five years time. But the trend is highly apparent now and the urgency exists as a result.

Ms Hartland: Yes.

Senator BUSHBY: Most of the concerns that have been raised around this bill relate to privacy—or many of the concerns relate to privacy; there are other concerns. But with respect to privacy, how does the bill actually impact that? I find it hard to see where it is actually exposing those whose data may be accessed to further privacy incursions, given that we are not seeking to increase the access to that information or to provide additional powers to access that information. All the bill seeks to do is to maintain data which is already in existence in the hands of the providers—just ensuring that it remains there for longer than it currently might otherwise be. Now, I presume that there may be some security risks in terms of improper or illegal access to data which is maintained that might not otherwise be. But in terms of the legal access, which you already have, do you sympathise with any of the privacy concerns that have been raised? I fail to see where it is actually increasing the risk in terms of privacy from Australians' perspectives.

Ms Hartland: Certainly from an agency point of view you are correct. We rely on providers to keep that information now. We are not keeping any more information. There is not a different model involved in that. Our guidelines remain the same. So, we have Attorney-General's guidelines that direct ASIO staff in how to treat personal information. That talks about us only collecting, using, handling or disclosing personal information for purposes connected with our statutory purposes. It talks about us taking all reasonable steps to ensure that personal information shall not be collected, used or handled beyond that; it has to be in the law et cetera. And all of that remains the same. So, I agree with your statement.
Senator BUSHBY: And on top of that we have had evidence that there were additional oversight mechanisms that will be introduced as part of this bill.

Ms Hartland: Correct.

Mr Phelan: From the AFP's perspective, now the Ombudsman will be able to come in and inspect records if they do not currently inspect, under this regime. And let me tell you, we are not going to change the way we store that information from now to when we get the Ombudsman, because we are extremely confident that the way we collect and deal with that information now is robust enough to stand up to any scrutiny that the Ombudsman may put forward.

Senator BUSHBY: In relation to that, what guarantees are in place—and it is really I guess not so much what is being introduced by this bill, because we have already established that there are not any additional access aspects of the bill—that ensure that the information would be accessed for serious crime and not those, as has been suggested in some of the submissions for local governments accessing information to chase up unpaid fines or whatever it might be? What guarantees, what protections, are there to ensure that it is used only for serious crime?

Ms Hartland: Before Deputy Commissioner Phelan speaks, I should say it is also for security purposes as well.

Senator BUSHBY: So it for serious crime and terrorist activity?

Ms Hartland: Yes, and from a security perspective, the legislation remains the same, as it always has been, and, legally, everything that we do has to have a nexus to security, so that does not change.

Mr Phelan: And from our perspective, it would still be the same. It is either required for a criminal offence, executing a pecuniary penalty order or for missing persons, and nothing will change. Of course, the act still will have—the Attorney-General's Department might be able to comment a bit more on this—we will still have the prohibitions on the people that are holding information about how they can deal with it.

Senator BUSHBY: For the Attorney-General's Department on that, Senator Fawcett was asking some questions about the ability of the Attorney-General to add agencies that may be able to access it. Theoretically it has been suggested I think in some of the submissions that you could add private security firms or you could add all sorts of bodies or agencies that have no direct relevance to serious crime, to terrorist activity—to the sorts of things which this is intended to address. What protection is there to ensure that the Attorney-General would not add such bodies?

Ms Harmer: A number of different safeguards are included, both in the bill and which are available under the operation of other laws of general application in relation to both how data is accessed and how it is handled by providers. In terms of the declaration mechanism, as I said earlier, there is a threshold requirement there for the Attorney to be satisfied that the data is required for the purposes of the enforcement of the criminal law and the protection of public revenue or the administration of pecuniary penalties. So those are the broad classes in which the parliament has previously recognised that access to data may be useful and so that it is only agencies that are involved in those functions that could potentially be the subject of declarations. And of course the declarations are a legislative instrument, so they are subject to disallowance and of course sunsetting as well.

In terms of the access that is made by agencies, agencies have obviously commented on the oversight arrangements and their internal procedures, but I should also add that improper access to telecommunications data is a criminal offence and is punishable by up to two years imprisonment. And I do note that there have been prosecutions for misuse of telecommunications data and a term of imprisonment imposed. It is also the case that telecommunications providers who retain information are subject to laws of general application, both under the Privacy Act and the Telecommunications Act, which required them to deal with such information in a manner that is consistent with those laws.

Senator BUSHBY: So there are a number of other aspects that provide you with confidence—and I think the Gilbert + Tobin submission, to paraphrase, says that there is nothing in the legislation to prevent an Attorney-General declaring an authority or body as an enforcement agency, which could include local councils, gambling authorities, universities, private security firms, toll road operators, family law dispute resolution services and organisations responsible for enforcing copyright infringement.

Ms Harmer: An agency could only be declared if it had functions in relation to the enforcement of the criminal law, the protection of the public revenue or the administration of pecuniary penalties. And that agency would need to provide advice to the Attorney to satisfy the Attorney-General that it did indeed have those particular functions. Typical evidence of that might be the statutory functions of that agency or functions that have been conferred upon it either by this parliament or by state and territory governments, but it would need to

INTELLIGENCE AND SECURITY COMMITTEE
be clear that those agencies have those functions before access to data could be made through a declaration process.

Senator BUSHBY: And then, even having satisfied that, if they were declared, they would be subject to the same restrictions that you just outlined a few minutes ago?

Ms Harmer: Indeed. And then, on top of that, that is not the only threshold, it would also be the case that the Attorney would need to consider the extent to which there were effective oversight arrangements of that agency and the extent to which that agency is the subject of a binding privacy obligation.

Senator FAWCETT: I just want to follow up. Ms Harmer, you have used the word 'agency' continuously through that. Can we take out of that that the intent of the legislation is that it will only be government agencies or government bodies that would ever be declared, or is there a situation where a non-government organisation, body, group, could ever be declared?

Ms Harmer: The threshold around who can be declared is one that is defined by reference to the function—so, as I have said, enforcement of the criminal law and/or laws protecting public revenue or imposing a pecuniary penalty. It is typically the case that governments confer those functions upon government agencies however they might be described. We have seen over the operation of the current arrangements that a number of bodies have functions in that regard and, therefore, have had access to the data arrangements. So the precise constitution of a body that would be the subject of a declaration is naturally determined by the extent to which governments confer upon agencies or bodies functions in relation to the enforcement of criminal law. Enforcement of the criminal law is typically regarded as a function of the state, and so, as a general observation, I would say that those functions are conferred on government bodies, but the precise definition that is used in the legislation is around the characterisation of functions of those bodies.

Senator FAWCETT: If the committee were to recommend that the government adopt a legislative hard barrier to say that it will be an agency of a government as opposed to any other body, would that cause any concern to agencies or to the Attorney-General's Department?

Ms Harmer: It is certainly something that we could consider. I would like to give some further thought to that and the extent to which there are some unintended consequences that we may not yet have turned our minds to. But certainly it is the case that the agencies which currently have access and which typically perform those functions are ones which are bodies of the state in some form. I would like to give it some further consideration. It is certainly something that we could give some thought to.

Senator FAWCETT: If you could take it on notice.

Mr CLARE: Firstly, continuing on from that question and a request of the department to provide an answer to the senator's question, I ask the department if it might look at the submission from the University of New South Wales and, in particular, pages 4 and 5—Senator Bushby has quoted part of that—it provides its thoughts on potential improvements to the bill in the area of how the Attorney would declare criminal law enforcement agencies and also how it might amend the scope of the Attorney's powers with respect to other agencies that can access metadata. If the department to have a look at the recommendations from the university and provide feedback to the committee, that would be appreciated.

Ms Harmer: We can do that.

Mr CLARE: Secondly, can I go to this issue of the definition of serious crime. The Attorney said that this legislation would be limited to the most serious crimes. I just ask the department to have a look at the report of Joint Committee on Human Rights. They are concerned that there is no requirement in the bill that data disclosure relate to a serious crime. They recommend that the legislation be amended to limit it to where it is necessary for the investigation of specified serious crimes or categories of crime. I am conscious that you cannot necessarily provide us with your thoughts on that recommendation today, but could you take that on notice and provide written advice back to the committee on whether that recommendation poses any problems.

Ms Harmer: We can provide further advice on that front. I should say, though, that it is the case under the Telecommunications (Interception and Access) Act that access to data is available in relation to the enforcement of the criminal law. That access to data, as agencies have said, is an essential tool and building block of all types of investigations. And while it has particular value in relation to a range of very serious crime types, it is a useful tool and, particularly at the state and territory level, it is used in the enforcement of the criminal law broadly. We can certainly provide a response to that and, as we said in relation to the Senate Scrutiny of Bills Committee, we will naturally also be responding to the report of the human rights committee as well.
Mr CLARE: That in particular, because I am conscious that the government's response to those committees might be after our report, and it would be useful in our own deliberations to know what the government's thoughts are on that recommendation. So any advice the department could provide the committee on that in particular would be useful.

My final question relates back to costs. I want to ask the department about some concerns that the Communications Alliance have raised in their submission about whether individuals could make an application for their own metadata in court and the potential cost implications of that. In particular, they are concerned about, if a large number of individuals were to make an application for their own metadata, who would bear the cost for that. In their submission, at page 14, they say that the bill does not explicitly address the question of whether individuals should have the right, under Australian Privacy Principle 12, to make demands on CSPs to provide access to their personal metadata, especially the metadata captured by the mandatory data retention scheme. It may be a question to take on notice.

This concern has been raised by the telcos and they are interested in whether there would be anything in the bill deliberated upon by the parliament that addresses this. They would be interested in the department's advice and, if this were to be an open question, whether telcos would receive cost recovery for the costs of doing this.

Ms Harmer: There are a couple of things we can provide some preliminary comments on, at this stage. As Communications Alliance has probably flagged, there are arrangements under which people can access their own personal information. The Privacy Act provides a mechanism for individuals to request their own personal information. What is 'personal information' depends on the circumstances, but it is information that reasonably leads to the identification of a particular individual. What that is will depend on the circumstances and will depend on what the information is, the circumstances in which it is received and how access is arranged. Particularly in the telecommunications context, that can vary according to network configurations—whether a particular data point is one that identifies an individual. Nevertheless, it is the case that, to the extent that carriers have personal information, individuals may apply to those carriers and request their personal information. Indeed, industry is entitled to recover the reasonable cost and is entitled to charge for the provision of personal information under that Privacy Act framework.

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 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.

I suspend this public hearing until 2 pm. We are now moving to a private hearing, which will take place at 12.15. Could the media please respect us as we move from this public hearing to a private hearing. Thank you very much.

Proceedings suspended from 12:07 to 14:03
ALTHAUS, Mr Chris, Chief Executive Officer, Australian Mobile Telecommunications Association
ELSEGOOD, Mr Michael John, Member, Communications Alliance
FROELICH, Mr Peter, Industry Member, Communications Alliance
STANTON, Mr John Leslie, Chief Executive Officer, Communications Alliance

CHAIR: We will resume. For the information of our guests and visitors, we may have Senator Conroy appearing via phone hook-up. I welcome the witnesses. Would you like to add anything about the capacity in which you appear?

Mr Elsegood: I am with the regulatory team at Optus, and Optus is a member of both of the associations.

CHAIR: Thank you. 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?

Mr Stanton: Yes. We would like to echo the remarks that were made earlier in the day in testimony by expressing our sympathy, on behalf of our organisations and companies, to all of the individuals who were victims of the tragic events in Sydney this week, and in particular by sending our condolences to the families of those who lost their lives.

We are certainly grateful for the opportunity to make a submission to the committee and to appear before you today. Our submission is a high-level explanation of the issues that industry sees as important to consider before the legislation progresses further in the parliamentary process. If the committee permits, we might take the opportunity to provide supplementary material on these issues in the new year and before the final submission deadline.

I would like to emphasise at the outset that there is a long and very cooperative relationship between service providers and the telecommunications industry, and law enforcement and security agencies. As the committee has heard today, those relationships support more than 300,000 authorisation requests per annum. Service providers do recognise the importance of telecommunications data to the legitimate needs of law enforcement agencies and to their efforts to combat serious crime and threats to security.

Last time we appeared before the committee back in 2012 we stated on behalf of the industry quite clearly that we did not believe a case had been made for the type of mandatory data retention regime that was at that time being proposed. Today it is fair to say there is something of a range of views among our membership as to whether such a case has now been made, and it depends in part on the final shape of the regime, around which many questions remain.

Notwithstanding this, legislation has been introduced to the parliament. If parliament decides to bring the bill into law, we think it is vital that the legislation be clear in its requirements, that it be practical in terms of the impositions it places on telecommunications service providers, that it avoids unintended consequences, that it is mindful of personal privacy and that it is proportionate to the security challenges facing Australia. It is these issues that have driven the content of our submission.

We think equally it is very important to recognise that this bill provides not only for a data retention regime. We have perhaps at times grown a little weary of hearing this proposal described as a requirement to do no more than service providers do today. It is in most cases far from that. It is a data creation regime as well as a data retention regime, for all of those providers who do not presently retain everything in the dataset.

Data creation is typically a complex and often an expensive process. This fact, I think understandably, bears on the minds of service providers in the current circumstances, where we do not yet have any visibility of what the government's contribution to the capital expenditure here will be, whether that is a reasonable contribution or a substantial contribution, as the Minister for Communications told the parliament in introducing the bill. And in those circumstances we obviously do not know how large the financial shortfall will be in implementing and complying with the regime, that shortfall being borne by service providers, but ultimately by their customers. So while I have spoken to one misconception, if you like, that tends to be in the public debate around this issue, we would also like today, in response to questions perhaps, to correct one or two other misconceptions that we feel emerged in earlier testimony.

Our submission to the committee contains a total of 13 recommendations. I do not propose to run through all of them, but I would like to mention some, if I may, very briefly. Our first recommendation was that as much as
possible of the proposed regulation be incorporated into the bill to guard against what is colloquially referred to as 'scope creep', and we also suggested some form of cost-benefit analysis or impact statement for proposed changes to regulations to help enable the parliament, when it examines those proposals, to decide whether it is proportional, whether we are being asked for a major impost in exchange for a very marginal gain in security.

Our second recommendation, I am pleased to say, is now also a recommendation of the working group—that is, if there are changes to regulations they ought not to be able to come in with immediate effect, but rather only after the parliament has had an opportunity to review them. In recommendation 3 we talk about retention periods. We note in the submission that the retention of telephony data for a period of two years is not too far away from what typically happens today, and so is certainly one of the less controversial pieces of the dataset from industry's point of view, but we have recommended a period in the order of six months for internet related data. We would be happy to talk to some of the issues around that with the committee. We have also made the point that in the event that the retention period for internet related data is less than two years, there may be some providers who would actually prefer to keep it for two years. If that is the case, then the legislation might need to provide an assurance that keeping it for two years does not expose the service provider to breaches of the Privacy Act.

At recommendation 7 we have raised questions around oversight arrangements. We do not claim to have solutions for those; it is more to highlight the issue. Similarly, at recommendation 8 we have noted, as was discussed this morning, the question of a generic warrant as it was raised by David Irvine. Recommendation 9 is important from our perspective; it is around the question of whether individuals will be able to access on demand their own metadata. We would like to reinforce the fact that the right to personal information stored by CSPs absolutely ought to be maintained—there is no question in our minds about that—but we are concerned about the precedent that may be set that enables hundreds of thousands or more individuals to demand access to their metadata. There was some discussion about this earlier today, and the sense, I believe, from the testimony was that cost recovery would be available in the event that this was exercised by individuals. We were not 100 per cent sure whether that was cost recovery from the customer or from the government, and that is something we will try to clarify offline with the department.

Mr RUDDOCK: [Inaudible] to your customer. If I want my data from my provider, then I ask the provider. If the provider wants to provide it, then they provide it at my cost.

Mr Stanton: That was the assumption we drew, but we were not certain. We were just looking for clarity on that, so thank you very much.

We have asked at recommendation 11 whether the regime is proposed as a proportional response, given in part the fact that there are many ways to circumvent it. At recommendation 12 we have asked whether the committee would like to reaffirm its previous recommendation that the costs to comply with the data retention regime be reimbursed by government. We also asked that the cost situation be clarified before the bill is next debated. We have also raised the question of whether there is a competitive disadvantage, which we believe there is, for local providers if they are expected to foot a large bill or a substantial proportion of the bill for a data retention regime when offshore providers offering services in Australia are not asked to do the same.

Finally, we have asked the committee to bear in mind that the telecoms sector security reform provision is coming down the chute towards us—in the new year, we believe—and it is worth noting that the last time that was described to us by government, it was proposed that industry also pay a multi-million dollar bill to support that initiative. We cover in our submission the question of exemptions, and I am pleased to say that the working group on which we have been participants has provided some clarity around the services that will be eligible for exemption—or are at least recommended to be eligible for exemption. There remains a significant issue though around business services, where it is not clear which of those may or may not be eligible for exemption. It appears we are looking at a bespoke process where individual applications will need to be made for an exemption. That makes it a little bit harder at this point to estimate the costs on the industry side as well. I will pause there, Mr Chairman; thank you for your indulgence.

Mr NIKOLIC: You say in your submission that government has not made a sustainable case for imposition of mandatory data retention. What in your view would constitute compelling evidence that would make that case?

Mr Stanton: We have not seen, for example, the information which I believe has been made available to the committee about the relative importance of data of differing ages. Certainly we look at the overseas experience where almost all the rest of the world has gone for a shorter period of retention around IP-related data. So historically we have not been convinced—

Mr RUDDOCK: So you are only quarrelling about the question of the length of time; you are agreeing that in principle that it is appropriate to access data?
Mr Stanton: We support the accessing of data every day of the year.

Mr NIKOLIC: But you make the point 'the government has not yet made a sustainable case for the imposition of a mandatory data retention regime in Australia', yet we have New South Wales Commissioner Scipione saying:

There is not a terrorism investigation since 9/11 which has not relied on metadata.

David Irvine, who you mentioned, said:

Unless metadata storage practices change, counterterrorism efforts will be severely hampered.

The head of the AFP said:

Without a two-year data retention period, the AFP is concerned investigations that rely heavily on telecommunications data will continue to be frustrated by inconsistency in retention of data by Australian service providers.

What weight do you place on the evidence of those who actually run these operations against your judgment that a sustainable case has not been made and what weight do you place on 35 Western countries imposing a regime—of varying durations, by your own admission? And if none of those things are compelling enough to say the case has not been made, what would?

Mr Stanton: The question of sustainability of the argument rests in part around the detailed scheme—whether it is proportional, how much is captured by it, what the exemptions are, what cost recovery arrangements are and how it deals with things like exemptions. As I said in my opening remarks, there is a diversity of views among our membership about a data retention regime. Some of our members have come out publicly and said, 'We should support it'. We are in a position where we are trying to better understand what the overall regime will look like. That is why we raise these recommendations and issues. We may come out of this process with a package which we think is sustainable because it has addressed the many issues from above the data set which we think need to be looked at.

Mr NIKOLIC: So you do not agree that the information available on the public record since 2001, the benefit of metadata for breaking a number of important, for example, counterterrorism cases, child exploitation cases and the evidence presented both publicly and to this committee—I am sure you are aware of that evidence from the various agencies who run these operations—that that still does not make the case, in your view, for a data retention regime? And you talked about your members and the diversity of opinions but clearly the weight of opinion among your members was such that you concluded government had not yet made a sustainable case.

Mr Stanton: And what we have done in our submission is put forward positive and constructive recommendations about how the regime could be brought to a position where it is sustainable. We are aware of the evidence which has been put on the table about how metadata assists the work of law enforcement agencies. We do not dispute it. We have said in our submission it is important that we acknowledge that. Every one of our members works hard to support those law enforcement agencies and has done so constructively for many years. We are not seeking to be obstructive in any way to the legitimate aims of the law enforcement agencies or the need to ensure that Australia is secure.

Mr NIKOLIC: I am not saying you are, Mr Stanton, but you are making judgments on the basis of relative value of this information to law enforcement agencies by your own admission here. One of your recommendations, to paraphrase you, says that you are not sure of the benefits of data retention because of the ways to circumvent it. I would be interested to know what is your group's experience in running intelligence led operations that would enable you to make a judgment on the basis of relative value of this information based on ways that you can circumvent the information. Surely those law enforcement agencies are pretty well placed to understand the relative values of both the data set being exploited by them for intelligence purposes and their ability to counteract an agile adversary that is trying to circumvent those things. Despite their intimate knowledge of those things, their strong evidence to this committee and in the public domain is that this remains something that is essential to their operations. You have made a recommendation. I am wondering on what basis you justify the recommendations that this may not have great value because of ways to circumvent it.

Mr Stanton: The recommendation raises the question about whether it is a proportionate response. That is based, in part, on our observations as to the many ways that such a regime can be circumvented. It is also based on the feedback that our members hear from agencies about the real-world experiences of circumvention. We do not in our recommendations say that this ought not be done. We are simply raising it as an issue that may be worthy of consideration.

Mr NIKOLIC: You also use the words 'potentially enormous cost' in the second paragraph of your submission. I am wondering what benchmarking you have done of those countries that have implemented some form of data-retention policy to reach the judgement that this is 'a potentially enormous cost impost'.
Mr Stanton: We know the calculations that we did three years ago, when this committee last examined this topic, and the numbers and estimates that we came up with at that time. Our members are still working through with PwC, as was said to the committee this morning, to see what this dataset—to the extent that the other elements of the scheme can be known—will mean in terms of costs. The last time we ran a ruler over this it was a very large number.

Mr NIKOLIC: A lot of things have happened in the last three years, including a number of similar countries to ours, western countries, implementing such a regime. My question is not what the results were of your study three years ago on the potential costs but what benchmarking you have done with competitors, like-minded countries, that might have imposed this sort of data-retention regime, to better understand what the costs actually are rather than what the estimate might have been three years ago.

Mr Stanton: There has not been any publicly available data that we have seen from overseas regimes. In regimes like the UK they are still arguing about what the legislation they passed means, so I do not think they have a concluded view on what the cost might be.

Mr NIKOLIC: The British telecom—and your other peer organisations around the world where these things have been implemented—I imagine, might have some idea. Has there been any interaction between the Communications Alliance and like-minded peak bodies or major telecoms, in countries where a data-retention policy has been implemented, to understand what their experience relative to cost is?

Mr Stanton: No, there has been no formal benchmarking study done. We have been more focused on what the regime would mean for us in our market.

Mr CLARE: One of the questions we posed to the law-enforcement agencies is what proportion of the historical metadata they rely upon is less than three months old or less than six months old, less than nine months old, less than 12 months old, less than two years old or more than two years old. We have had varying amounts of success in getting that data so far. I think I can speak for other committee members in saying that it is important information for us in our deliberations. Is that the sort of information your members might be able to provide to the committee with some level of detail, perhaps not here but on notice?

Mr Elsegood: We can certainly take that as a question on notice and go back to our particular units and ask them the question. But I would make an observation around that. It would be fair to observe that the agency requests are probably tempered by their knowledge of what individual providers keep. It might not tell you what necessarily they would like to get, but it may reflect simply that their experience with individual operators is that one operator may keep it for three months and another operator may keep it for six months, and they would adjust their requests accordingly.

Mr NIKOLIC: That makes total sense. They know company A holds the data for this period of time and they will amend their application so they are asking for data that is less than that. That leads me to the next question. I appreciate this is commercial-in-confidence information for the different ISPs. It would be useful for the committee to get a greater level of detail from ISPs about how long they hold information for. I am conscious that ISP A does not know how long ISP B holds this information for. Is there a way—perhaps if the committee was to write to Communications Alliance or a number of different ISPs—that we would be to get more granularity from the ISPs and hold that information in a commercial-in-confidence way so that we understand exactly what is being held now and for what period of time by different organisations?

Mr Stanton: I would be happy to take that request to our members. I guess that I was assuming that PwC, even if it was in an anonymised way, would be able to give at least a snapshot of the samples it has taken at various parts of the sector and provide some information. But I am happy to take that one on notice.

Mr CLARE: Just by way of explanation, one of the reasons I think this is useful is that law enforcement is keen to make sure that there is not a further degradation of data available to them over time. I suspect that information that ISPs might be able to provide might indicate that, given the time frames they are holding data for at the moment, if it is held for a longer period of time than is currently the case there will be additional data that would be available for law enforcement. In order to know if that is correct or not we need that data from ISPs.

Mr Stanton: All right, thank you.

Mr RUDDOCK: I put the proposition, earlier, that once you have established the principle, the length of time may not be all that relevant. The marginal cost of keeping the information for three years or four years—if you have to keep it for two years—is probably not all that significant. Would you like to comment on that?

Mr Stanton: I will ask Mr Froelich to comment on that.
Mr Froelich: I guess the costs are not strictly incremental but more exponential. In terms of the way that data growth is in the industry at the moment, as you start to blow out the time period from two years to three years, four years, five years or whatever you propose, the volume of data usage on an internet-type service is growing at a factor of 10 times. So you will have those exponential growths on top of the basic incremental growth of the length of time you want to store the data. So the costs involved—perhaps I will talk indicatively—are around some of the more mundane things like power and air conditioning, floor space and things like that. That is where the costs will be driven up as we start to store more information, and store it at an exponential rate. Particularly as the growth of access services with higher access speeds goes up those transactions are going up, which means that the volume of data retention and metadata goes up as well. I suppose those are some indicators towards costs and potential do-ability of achieving those outcomes. Does that answer your question?

Mr RUDDOCK: Not really. I assume that the major cost is the capital costs of putting in place a system, and once you have a system then you have the cost of running that system. The point I was making is that if the major cost is the capital cost, just continuing to run the system may mean only a marginal cost. Somebody said it might cost each customer a cent a day. Maybe they said it was less.

Mr NIKOLIC: I think it was 1c to 20c per customer per annum.

Mr RUDDOCK: It was between 1c and 20c per customer per annum. That was just to keep the information and to be able to access it.

Mr Froelich: I am not in a position to answer about specific cost amounts at this point in time. What I was trying to get to was that the capital cost to set up a system initially, the life-cycle costs and the growth of those systems to develop for an exponentially growing industry is not simply an incremental cost. There is a factor of multipliers based on how the industry is growing in those areas. I suppose a simplistic mathematical model does not necessarily answer your question but it is more than just the incremental cost.

Mr CLARE: What you are saying is that the longer the time that you hold the data the more the capital cost, as well. Is that right?

Mr Froelich: It is capital costs, but it is also the nature of the capital that you have invested in the first place to develop perhaps search engines and structures to actually access that information. As the depth of that data increases because of the exponential growth of the industry, it increases the amount of search functions, and the capacity of the systems you put in place to go and find that information becomes more processor intensive and it becomes more costly to do that. So the costs start to mount up as you go longer in a retention period, yes.

Mr Althaus: Chair, just as a comment: the indicative growth that we are seeing, if you look at the Communications and Media Authority's numbers released for the year ended 30 June 2014, is that we have an aggregate of 50-plus per cent growth across all categories of data and nearly 100 per cent in mobile over smartphone devices. But the big growth is in fixed-line broadband, where it has moved from just over 600,000 terabytes to nearly a million terabytes in a year.

Mr CLARE: Chair, I might move into a different area, if the committee is okay with that. I wanted to go to this issue of the 'honey pot'. You were concerned in your submission about civil litigation and how people might use the data for purposes that the data is not proposed to be used for here. I invite Mr Stanton to tell the committee a bit more about that.

Mr Stanton: At the outset, we recognise this may be a difficult issue to tackle, given that civil litigants do have rights to seek discovery for those sorts of data. I guess our concern is that, once it is known—through the requirements of the dataset—exactly what data is being retained by each service provider and for how long, that may generate a tsunami of action in commercial disputes, in marital disputes and in many other cases where the data is being mined in circumstances where we may not be able to recover costs for all sorts of purposes that the data retention bill was not designed to facilitate.

Senator BUSHBY: Currently, a lot of providers hold a lot of that information anyway. Some of them hold it for longer than two years; certainly, in the past they have. Have your members experienced such claims up to this point—and to what degree?

Mr Stanton: Yes. I cannot speak to the degree in a numerical sense. Our concern, I guess, is that this is a high-profile exercise and it will put it very clearly in the public consciousness that a defined set of data is available from every service provider, and we think it may start an industry, if you like, and—

Senator BUSHBY: Okay. So it is not really a problem at this point with the data. It is the same data that is being held; it is just that it will be held for a defined period, if this bill is passed.
Mr Stanton: For most service providers, no, it is not the same data that is being held. It is more data, to
meet—

Senator BUSHBY: The evidence we had this morning—

Mr Stanton: the requirements of the dataset.

Senator BUSHBY: The evidence we had this morning from the Attorney-General’s Department—correct me
if I am wrong—was that they would not be requiring providers to hold anything other than what they would have,
even if some providers just hold it fleetingly. I think, basically, the requirements would be that it is only things
that the providers would actually be holding at some point.

Mr Stanton: No, that is not correct. There are elements of the dataset that many of the providers do not hold
at all today.

CHAIR: [inaudible] there are the six categories that—

Senator BUSHBY: Okay, but that was tested, and she indicated that there was an expectation that it would
only be—

Mr DREYFUS: In fairness to the representative of the Attorney-General's Department, what she said—and I
am sure that the Hansard will be able to be checked at some point about this—was that the telecommunications
data is necessary for the operation of the system and will fleetingly, possibly only fleetingly, be in the possession
of the provider, but that in some cases, perhaps in many cases, the data is not kept at all. It exists but it passes. So
I would not want to overstate the evidence that was given by the representative of the Attorney-General's
Department.

Mr Stanton: Sure. And I am not trying to pick a fight with AGD either! But there are elements of the dataset,
for example, that require data to be collected and manipulated in ways that it is not today—historical aggregate
records of upload and download volumes, for example. I do not know of any provider who manages to put that
material together today. There is no business requirement for it. The feedback from some of our members is that
that will be quite difficult to do. So there are elements within the data set that do place creation demands on
service providers.

Mr DREYFUS: If we can unpack that for a moment—no pun intended—you have got a fact of a certain
volume of upload or a fact of a certain volume of download for a particular customer but it is not kept at all.
Nothing in the systems of some providers keeps that information, and they would have to in fact build part of
their system in a way that would enable them to capture that data.

Mr Stanton: Yes, that would enable them to bring that data together—to record it in the first instance and to
manipulate it in a way to meet the requirement being put by the agencies.

Senator BUSHBY: That is not inconsistent with my understanding. It goes through—

Mr DREYFUS: No. I don't think it is, David. I am just trying to get this clear, because I do not think, with all
respect, that there is a difference of opinion between what Mr Stanton is saying and what the Attorney-General's
Department expressed today.

Senator BUSHBY: I was interpreting the witness's evidence, and maybe incorrectly, that you need to go out
and find stuff, that it does not actually pass through the providers hands at all. You would have to go off and find
information that has nothing to do with what you are actually doing. I think Mark has clarified that.

Mr CLARE: Can I follow that line of questioning with an additional question about what difference this
makes for a big ISP as opposed to a small ISP. They come in all shapes and sizes. Doing that additional work
would be different for a Telstra or an Optus as opposed to a rather small ISP. Can you explain to me what the
difference would be. If we are dealing with a regime where it is not a full cost recovery but government is paying
either a reasonable or a substantial amount of the cost, this is probably quite relevant for small businesses.

Mr Stanton: We have asked some of our members who represent small service providers to do some research
on this. There are a couple of factors that bear on it. One is the extent of flow-down, if you like, of data from a
wholesale service provider to an aggregator or to a small retail service provider. In traditional telephony, for
example, a lot of that can happen through the distribution of core records. It is much less certain and much more
varied in the IP world, where it is not clear whether the small providers will be able to rely on their upstream
provider to give them those sorts of data, because often they will be effectively buying a pipe and what they do
with the pipe is what gives them the ability to add value and sell to their customers.

It is fair to say that all of the smaller providers are resellers, and that typically means they are operating in a
narrower margin environment than those further upstream. It would also appear likely that they would tend to
move in the direction of manual workarounds as opposed to putting in place new systems for which they typically
will not have capital. I am awaiting some further advice from those who operate in that part of the market. I think it is a legitimate question to ask as to whether the impost of the regime would make life sustainable for some of those smaller players.

Mr CLARE: Just following on from that, as part of the PwC work and the working group's work in stage 2, there is an anticipation that they will look at that, because the last thing you would want is a new impost that puts businesses out of business.

Mr Stanton: There is a very clear indication that PwC will look at that. We have been told by AGD that they will take samples from the various parts of the sector curve—small, medium and large—and will try to get a representative idea of what the regime means in terms of cost impost for those different categories of player.

Senator CONROY: John, do you think that the Commonwealth should cover 100 per cent of any of the extra expenses? Is that the industry's position?

Mr Stanton: We certainly were warmed by the PJCIS recommendation along those lines the last time the committee looked at it. There are a number of considerations around whether these are data that are already being retained for business purposes or whether they are being created or collected for the first time just for the regime. Mike, do you want to add to that?

Mr Elsegood: First of all, we need to break it down into the sorts of data that we are talking about. There is usage data, which is just how the customer uses the service, and there is more static information about who the customer is. On the consumer side of our businesses—who the customer is and what sorts of services they have—we keep most of that sort of information for two years or so. That is for a range of reasons. Firstly, it is to deal with the customer themselves. Secondly, it is to deal with any complaints they might have through the industry ombudsman scheme and those sorts of things. That might vary, though, on the business side—servicing corporate and government customers. For some of those customers, there is no business reason to retain the information if you do not have that customer any longer. On the usage side is where I think there is probably a greater discrepancy. Some service providers might be billing on a fairly bulk basis and would not be collecting fine-detail information about the customer's services. In that sense, they may not have the detailed usage records that might be required out of a data retention regime. On the mobile side, any information about mobile location may not be being stored in systems at all because there is simply no business reason to keep track of where your customers are. From an operational point of view, you may keep that for a very short period of time to deal with customer complaints or technical complaints about the operation of your network. So you might keep some short-term records about how your network has been performing. But in the long term you would not be keeping that sort of stuff.

Another thing that comes into play is compliance cost. There is a cost involved in going through all of your services to make sure that you are meeting the legislative requirement once it comes into place. And there is an associated cost in just building a search process—and Peter alluded to that before. There is no point in having this data if it cannot be searched. You have got to make sure that you have indexed it on the searches that you know are going to happen, and you have got to have a machine that can search through data in a reasonable period of time so that you can respond back to the agencies. So you have got to have that to go with it. It is not just a matter of sticking it on drives that you buy from Dick Smith or Officeworks and just storing data on disks. It is a more complex situation than that.

Mr CLARE: Following on from that, I have a series of questions about the timetable that the department expects for getting some accurate information on how much this will cost industry to comply with the legislation. Can you provide us with any thoughts that you have on how this process will work over the Christmas break and through January? This is part 2 of the working group's activities, isn't it?

Mr Stanton: We know that PwC has reached out and is working with a whole range of service providers at the moment—including the two on my right. I do not have overall visibility as to how successfully that is proceeding and whether they are asking the right questions and drawing out the data they need. I am not sure if Michael or Peter would like to comment.

Mr Froelich: In terms of developing those costs, from an industry perspective there is still a fair bit of work to do to work through our standard engineering processes to do requirements and solution definitions to get to a fairly solid business case in our internal models. From a larger industry perspective, it will take us a further six months worth of work to develop those really detailed costings. Everything we are doing at the moment is a very rough order of magnitude costing, and over a two-year build period. So it is very rough stuff at the moment.

Mr DREYFUS: Are we likely to get those costings any time soon?
Mr Stanton: I honestly cannot be certain. I know that the working group has that as its next phase of work and has an objective to provide material in a timely fashion for the committee and before the bill is next debated.

Mr Stanton: I honestly cannot be certain. I know that the working group has that at its next phase of work and has an objective to provide material in a timely fashion for the committee and before the bill is next debated. Certainly as we have said in our submission, we would be quite concerned if the bill was finding its way into law before we have answered the riddle of what the costs are and what the shortfall is.

Mr CLARE: That would be a concern for us, too. We are expected to report by the end of February and I would expect then that legislation would be debated sometime after that. What I am hearing is that it is possible that we may not know what the total cost of this scheme is at that time or, because the government is proposing to fund part but not all of the cost of the scheme, at that time when we are considering our own recommendations but the parliament is debating the legislation, it is possible that we will not know how much of that cost will be passed on or what the total quantum is of total costs that will be passed on to consumers.

Mr Stanton: I wish I was in a position to make a strong prediction about when it will arrive, but I am afraid I am not.

Mr CLARE: Right. I might just turn to a different topic. I think one of your first recommendations was about how much of the dataset can should be embedded in legislation. I am interested in just exploring that in a bit of detail in terms of the certainty that provides for industry. The government has been doing some work in red tape repeal in the communications space in a very cooperative way with industry, and it has had, by and large, support from both the telco sector and consumers.

Mr Stanton: Yes.

Mr CLARE: One of the advantages I would think of embedding as much of the dataset as possible in legislation is that the certainty provides for industry as well has the ability of industry to be able to adapt to any changes in a more methodical way rather than having to deal with quick changes to regulations and scope creep that can emerge. Can you tell me: what is the difference for industry, from an industry point of view, of having the dataset in legislation as opposed to regulation?

Mr Stanton: I think it provides a greater level of certainty about what is going to be required and a degree of assurance that changes cannot be made in a less than disciplined way. We certainly recognise the good intention behind the way that the dataset has been created. We have had concerns about the use of open-ended language in the dataset and the general concern I guess that, a few years down the track when the passage of this legislation is a matter of history and service providers are dealing with agencies, if it is possible to change the regulation and expand the scope of the regulation quite quickly and without proper oversight, then the beast we are creating might look very different and might impose much larger imposts on industry without necessarily there being a commensurate addition to security. So we have raised the general point in our recommendation. To be honest, looking at the dataset we find it a bit hard to see how you would split it up and put some in legislation and some in regulation, but we have a general preference for it being in the bill.

Mr CLARE: Thank you. This is my final question, Chair. In your submission you explore the possibility that you could have a different time frame for the retention of telephone data as opposed to internet data. I am interested in a bit more information on that. I know that that is certainly the case in other countries. From industry's point of view, that would not create any problems for different telcos, if that were to be the case?

Mr Stanton: No, albeit that at least one of our larger members has stated a preference for having a single duration of retention across all services for planning and system simplicity. The majority of others have said that they would prefer a shorter period for IP related data. So that was the basis of our suggestion that, if the government agrees to a shorter duration for IP data, there still be the ability to retain for a two-year period that internet related data without infringing the privacy act.

Mr CLARE: Thank you.

Mr DREYFUS: I see from the schedule to your submission that different countries have opted for, in some cases, radically different periods for telephony data as distinct from internet related data. Are you able to explain why there is a preference for a shorter period for internet related data?

Mr Stanton: It relates mainly—as far as we have seen from looking at the EU countries, in particular—to the same sorts of issues we have identified. There are storage, maintenance and other costs associated with IP data, which is typically growing at a much faster rate than telephony data; the longer you need to store it the more it is going to cost. Also, there is a general recognition in many of those jurisdictions that it is the younger data, overwhelmingly, that is useful to the pursuit of serious crime and national-security issues.
Mr Froelich: As a slight extension to that, you might also consider the maturity of the product. The traditional public switched telephone network is obviously a much more mature technology product, and the billing functions and cycles around that are already well in place. You will hear that law-enforcement agencies already access that information. They get very good access to billing records from traditional public switched telephone network metadata or billing data. It is less problematic, perhaps, than the volumetric type billing exercises we do in internet data.

Mr DREYFUS: And presumably no one has to build a new system to produce traditional telephony data, if I can call it that.

Mr Froelich: Yes, because a lot of the billing systems already enable those sorts of functions, traditionally anyway.

Mr Stanton: Our own telecommunications consumer protections code, which I do not think was mentioned this morning, explicitly requires retention of billing data for six years to be able to provide it back to customers.

Mr DREYFUS: You probably cannot answer this question. How much impact does a retention period of two years as distinct from six months have on the cost?

Mr Froelich: Again, it depends on the maturity of the products. As we just discussed, a PSTN has zero impact. You have the data anyway. For internet products I think the discussion before was about there being fleeting or transient information on the network. You have to build systems to take that fleeting or transient information to put it into a centralised location to be able to sift, sort and deliver that information. So the difference in cost, as I tried to allude to before, is exponential based on the number of transactions. As Chris mentioned, that exponential growth in data means an exponential growth in transactions which, again, adds to the storage and security functions—the boring stuff—around housing it with power and air conditioning and floor space, all those sorts of things that are not very sexy to talk about in this type of environment but are real costs and actually drive up the end-cost to the telcos.

Mr DREYFUS: I wanted to ask you about something you mentioned at page 16 of your submission, under the heading 'Efficacy'. It is the part of your submission where you talk about over-the-top secure-messaging apps and the use of VPN, and you put it forward in the context of whether use of VPN or secure messaging apps or encryption of various kinds might render mandatory data retention ineffective. It is a fairly short part of your submission. Are you able to elaborate on that?

Mr Stanton: Certainly we think the technological means available today, to get around the data-retention regime will by definition make any regime less effective. There are many circumstances where things such as VPNs, encryption on various types of mobile phones and other techniques are being used by the 'clever' bad guys to effectively remove themselves from the reach of many—I am sure not all—attempts to detect their communications.

For us, this is something of a double-edged argument to put in a submission because you could argue on the one hand that, for the effectiveness you gain via a data retention regime given the inherent holes not just in Australia but all around the world, it may not be worth the additional cost. Equally you could make the argument that because there are holes you should make the pieces you can cover as absolutely stringent as possible. That is not an argument we are advancing, but we think it is an issue worthy of considering in the overall picture.

Mr DREYFUS: Are you able to tell me anything about best practice for storage of sensitive personal information in the industry? I ask in the context of a recommendation made by this committee in its 2013 report. The precise wording of the recommendation was, if there were to be a mandatory data retention regime, that:

- the data should be stored securely by making encryption mandatory …

Would that be something you would favour—that the government mandate encryption at the same time as mandating retention?

Mr Stanton: The service providers already need to comply with the government's Information Security Manual and with the Protective Security Policy Framework, which are both pretty stringent requirements that need to be met today. Peter, perhaps you might be better placed to address the question directly.

Mr Froelich: I think the two documents, the PSPF and the ISM, that John has raised are trigger documents. In fact, whenever we go through any cost-recovery exercise with the government those are part of the compliance objectives the government puts in front of us. So we have very stringent requirements around security. But, beyond that, as an industry, we have every reason and every intention to protect the privacy and security of our customers. For our industry members, there would be no reason why we do anything less with their data under this regime than we do under anything else. All of those security structures and tools available to us—firewalls,
physical security and encryption—we would put in place to ensure that our customers' privacy and security is maintained along with the interface with government as well. Those are standard practices now in the way we deal with law enforcement and national security and the way we deal with customers' data.

Mr DREYFUS: There have been a series of high-profile data breaches in recent years. How well can the industry guarantee the security of the stored personal telecommunications data that we are talking about here?

Mr Stanton: In this day and age, I guess it is impossible to provide any absolutely ironclad guarantee that there could not be a successful attack on a network. I think the industry in Australia is very security capable and certainly would pay very diligent attention to its obligations in that regard, as it does today, but I do not think it is possible to guarantee the integrity of any network anywhere in the world. As you say, there have been high-profile breaches recently, not so much in Australia but overseas, that demonstrate that even very hard networks are not impregnable.

Mr Elsegod: I will just add an observation to that. In meeting these data retention obligation we need to recognise that particularly law enforcement liaison units within businesses will be accessing that information and so we need to put security around that for the reasons that Peter has mentioned. One of the options that may be considered is putting all of this data onto its own system, its own separate database, so that the only people who can access that system are the law enforcement liaison unit staff and it is not available for other people in the business and so, therefore, it is not linked out into the wide world where people can attack it from. That is one of the options that providers could give very serious consideration to. We would not regard that as gold-plating; we would regard that as perhaps reasonable business practice in the circumstances, given the need to protect the interests of the agencies in terms of the things that they are asking us to do, as well as the privacy impacts et cetera, from our business point of view, of that information not getting out into the public domain.

Mr CLARE: I have a final question perhaps to representatives of Telstra and Optus. You could use the case that the cost of the scheme is not fully funded by government, and, as you say, there is an exponential growth in data that will be retained over time. To deal with or address that gap in cost, will Telstra and Optus pass the cost of administering and operating this scheme onto their customers?

Mr Froelich: It is a difficult question to answer, but I guess in terms of how we run a business, everything gets paid for somewhere. There would be an expectation, I guess, that there would be transactional costs in dealing with law enforcement and national security and that those transactional costs should cover somewhat towards the life cycle of running a system like this. That is not particularly clear at this stage. I do not have any clear direction from the proposals at this stage how that could run if we were to call that day 2 operation of a system like this. I do not really have a clear indication—

Mr CLARE: So you are looking for clarification about cost-recovery for opex, effectively?

Mr Froelich: Those transactional costs down the track, yes—clarification around that.

Mr CLARE: But, if there is a cost gap in capex, can you rule out passing that cost onto customers?

Mr Froelich: I am not in a position to rule in or out anything at this stage. I can compare it, perhaps, to the way we run interception functions in cost-recovery in interception, and those incremental costs on interception, up to a point, are borne by law enforcement and national security, and so my expectation is—

Mr CLARE: Through a cost-recovery mechanism?

Mr Froelich: Yes, there is a partial cost-recovery mechanism in place for lawful interception components.

Mr CLARE: But we understand, in relation to the way this scheme will be established, that government will provide funding for either a substantial amount or a reasonable amount but not the total amount, so there is a gap.

Mr Froelich: But there is also a lack of clarity around opex but also a lack of clarity around if there is an alteration to the recommendation or the regulation in day 2 or day 102—if that alters our business model, will government come back and re-address those as well? So we do have a lack of clarity around the ongoing structure of the legislation.

Mr Stanton: As a general point, it is fair to note that at least one of our larger members has publicly stated its opinion that, in those circumstances, there would be a cost passed through to end-user customers. That was not Mr Froelich's organisation but another one among the top 10 in Australia. So that certainly is in the minds of some providers.

Mr CLARE: So it would not be misrepresenting the industry to say that some members of industry have said they will pass it on; others at this at this point cannot rule it out?
Mr Stanton: Some have certainly said that their assumption is that it would end up being passed on. I do not think they have made a formal commercial decision at this point, but they have said that their assumption is that that is the way it would go.

Mr DREYFUS: This is a technical question. The Attorney-General has suggested that we could think about metadata as the envelope that can be entirely distinguished from the content of the letter inside. Since that analogy was offered, quite a number of technical experts and industry representatives have raised serious doubts about that analogy and suggested that there are some very significant challenges that exist in separating the content of some communications from the metadata relating to the transmission. Are you able to speak to the committee about the technical challenges in maintaining what is, according to this bill and according to the second reading speech and according to the explanatory memorandum, a critical distinction between content and data? Perhaps to go on and flesh it out, how would that separation be maintained in practice?

Mr Stanton: I will let Mr Froelich open the batting on that one.

Mr Froelich: In terms of the comparison with the envelope, yes, I have heard that. But perhaps if we talk about more specific case points; perhaps email as a case point. The to and address and the from address on an email are quite clearly pieces of information that are in scope; the subject line on an email is considered to be content, but it sits within the addressing information of that piece of technology. We would have to do post processing of each email to just pull out the to and the from email addresses and the time stamping, and I think the size of the email is still in the structure perhaps—I am not sure on that. We would have to actually create that piece of data retention information by pulling apart the email, pulling out the pieces that are relevant and storing those in a separate file function, a searchable file function, elsewhere. There is what we call in a technology sense—you would have to pass that information to extract the pieces you want and do a packet inspection to pull out the parts you need.

Mr DREYFUS: That phrase you have just used, 'packet inspection'—just pause for a moment on the email example. We have hundreds of millions of emails being sent in Australia every day, all of which are going to be captured by a mandatory data retention requirement. What would have to be done in order to maintain the distinction between content and the telecommunications data that is being retained?

Mr Froelich: Effectively, we would have to build a quasi-interception machine to actually intercept each email and pull out the information we want, and then send that off to a separate storage function. If you will, it is a quasi-interception function to do that. A full interception function is more simplistic in that you just take everything that is there, under warrant, and pass that on, whereas this data retention regime would require us to unpick it and put aside the pieces that are required. The technology is perhaps not overly challenging from an engineering function—given enough time and money we can build anything—but the concepts of actually unpicking it and putting it aside are certainly a little bit more challenging than perhaps meeting the standard TIA Act interception obligations.

Mr DREYFUS: But the same problem does not arise, presumably, with traditional telephony?

Mr Froelich: There are some components of traditional telephony that are a little challenging under data retention. There are functions called uncompleted calls where we do not create billing records. Those sit as transient pieces of information within the outlying parts of our network, so you would have to actually drag all of that information into a central location as well. We keep completed calls and we bill a customer for those. Those functions are pretty simple. That is available now. It is uncompleted calls that cause some extra work in pulling those out of the network and storing them.

Mr DREYFUS: And what about with texts?

Mr Froelich: I think text messages are not particularly onerous in that there is a to and a from field and a billing function for those. We discreetly bill for those and the actual text line does not exist in the billing function. That one I do not think is particularly onerous for us.

Mr DREYFUS: Good to hear of something that is simple! And what about internet more generally?

Mr Froelich: This is where it starts to get a bit overly technical. Perhaps you have heard people talk about IP version 4 and IP version 6 in terms of addressing space—the length of the address field? It depends on the type of network you are running, but then even if you are running the latest version of IPv6 addressing, where each thing can be uniquely addressed, the way networks are structured you might do tunnelling and send an IPv4 communication stream within another IP structure and so it starts to get overly complex in how those are done. Because of the way the IPv4 addressing space is run out, they are reused; IPv4 sessions are reused typically hundreds of times.
Mr Froelich: Yes. So dynamic address allocation happens now and that will be, I guess, a difficulty for the law enforcement side of things to produce a disclosure request with fine enough granularity to ask for a particular IP address down to millisecond, to ensure they get the right information in their disclosure request because those transactions are happening at a very fast rate.

Mr Stanton: At the carrier level, there is also a big difference between providing an IP access service and the way you can collect data about that service, as opposed to an over the top service which may be operated by another entity who may not even be in Australia. There are elements of IP that are either difficult to collect or are essentially uncollectable at least from a service provider point of view.

Mr Froelich: Perhaps I can be a little bit more confusing—

Mr DREYFUS: You are doing quite well so far!

Mr Froelich: I am trying to put it as simply as I can but it is a difficult topic. When you are looking at those overseas transactions and you see an IP address coming from Australia that is not actually the IP address the customer is using. The customer is using a private IP address that is allocated to them by the carrier and the carrier translates that to a public IP address to use in the public internet. I apologise: it is a very confusing topic, but there are those ways of using the same IP address multiple times to deal with all of the customer base we have in Australia.

Mr Stanton: So either side of the router there will be a different IP address being used. The service provider cannot necessarily see beyond the router to which device is being used by which IP address on the customer side of that barrier. It does create additional complexities.

Mr DREYFUS: And that is a function of over the top generally which is not even calling for any use of any kind of security devices or masking or encryption—it just is a feature of the system?

Mr Stanton: Yes. The last point is it is just a function of the need to try to make a finite number of IP addresses to serve the world.

Mr DREYFUS: What is that number? Is it in the order of about four billion?

Mr Froelich: Four billion.

Mr DREYFUS: And that is the finite number of IP addresses under the current system, which is why we have dynamic identifiers.

Mr Stanton: That is right. IPV6 is arriving.

Mr DREYFUS: Forgive me: I'm a lawyer.

Mr Stanton: Chairman, I am wondering whether I could make one offer to the committee, which is to provide some further information about an element discussed in testimony this morning which may be confusing—around the comment made several times that there is a real problem in moving to Voice over IP because once you move to Voice over IP on the NBN or elsewhere suddenly there is no data to retain in the traditional telephony sense. The reality is that at the product and application level a Voice over IP is not a homogeneous technology. There is over the top VOIP like Skype applications and those sorts of things. There is also carrier grade Voice over IP which many service providers have been using successfully for years. There will at some point be mobile Voice over IP once we start using Voice over LTE on 4G networks.

So the suggestion that the onset of Voice over IP means disaster for the data that agencies will be able to access was somewhat overstated. I wonder whether it will be useful for us to prepare a one-pager on the different types of Voice over IP and the data that these throw up and make available, just as a matter of clarity.

CHAIR: I am sure, if you want to provide some additional material, you would be more than welcome to do that.

Mr Stanton: 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 it to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you. Thank you for coming this afternoon.

Committee adjourned at 15:14