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

Friday, 30 January 2015

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

Terms of Reference for the Inquiry:
To inquire into and report on:
Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.
WITNESSES

ASHTON, Mr Graham, AM, APM, Deputy Commissioner Capability, Australian Federal Police ............... 64
CLARKE, Dr Roger, Immediate Past Chair, Australian Privacy Foundation ........................................ 77
COPE, Mr Michael, President, Queensland Council for Civil Liberties, on behalf of joint councils for civil liberties .......................................................... 79
DE KOCK, Mr Hugo, Member, Liberty Victoria, on behalf of joint councils for civil liberties ............... 79
DICKSON, Mr Paul, Assistant Commissioner, Crime Service, South Australia Police ....................... 42
DUNN, Mr Matthew David, Director of Policy, Law Council of Australia ........................................... 29
ELSEGOOD, Mr Michael, Manager, Regulatory Compliance and Safeguards, Singtel-Optus .............. 13
EPSTEIN, Mr David, Vice-President, Corporate and Regulatory Affairs, Singtel-Optus ...................... 13
GANOPOLSKY, Ms Olga, Chair, Privacy Law Committee, Business Law Section, Law Council of Australia .............................................................. 29
HARMER, Ms Anna, Acting First Assistant Secretary, Attorney-General's Department .................... 64
JOHNSTON, Mrs Hetty Margarete, Founder and Chief Executive Officer, Bravehearts ....................... 1
KOPSIAS, Detective Superintendent Arthur, APM, Commander, Telecommunications Interception Branch, New South Wales Police Force ........................................ 42
LANSON, Assistant Commissioner of Police Malcolm Arthur, APM, Assistant Commissioner, Commander, Special Services Group, New South Wales Police Force ........................................... 42
LEE, Mr Simon, Acting Director, Attorney-General's Department .................................................... 64
LEONARD, Mr Peter Guildford, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia ........................................ 29
LEWIS, Mr Duncan Edward, Director-General of Security, Australian Security Intelligence Organisation ............................................................................................... 64
LINDSAY, Dr David Forbes, Vice-Chair, Australian Privacy Foundation ........................................... 77
LYNCH, Dr Lesley, Secretary, New South Wales Council for Civil Liberties, on behalf of joint councils for civil liberties .......................................................... 79
McCONNEL, Mr Duncan, President, Law Council of Australia .......................................................... 29
MCMULLAN, Ms Kathryn, National Manager, Specialist Capabilities, Australian Crime Commission ........................................................................................................ 64
MOLT, Dr Natasha, Senior Policy Lawyer, Criminal Law, Law Council of Australia ....................... 29
MORAITIS, Mr Chris, PSM, Secretary, Attorney-General's Department ............................................ 64
MORRIS, Mr Tim, AM, APM, Assistant Commissioner, National Manager High Technology Crime Operations, Australian Federal Police ........................................... 64
MURPHY, Mr Paul Vincent, Director, Media, Media, Entertainment and Arts Alliance .................... 38
PHELAN, Mr Michael, APM, Deputy Commissioner National Security, Australian Federal Police ............ 64
RONKEN, Miss Carol, National Research and Policy Development Manager, Bravehearts .................. 1
SEGRAVE, Inspector Gavan, Intelligence and Covert Support Command, Victoria Police ................. 42
WARREN, Mr Christopher John, Federal Secretary, Media, Entertainment and Arts Alliance ............ 38
WILLIAMS, Professor George, Private capacity ................................................................................... 4
JOHNSTON, Mrs Hetty Margarete, Founder and Chief Executive Officer, Bravehearts
RONKEN, Miss Carol, National Research and Policy Development Manager, Bravehearts

Committee met at 07:33

Evidence was taken via teleconference—

CHAIR (Mr Tehan): I declare open this public hearing of the Parliamentary Joint Committee on Intelligence and Security. This is the third of the committee's public hearings for its inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. These are public proceedings and the committee prefers that all evidence be given in public, but witnesses have the right to request to be heard in private session. The committee may also determine that certain evidence should be heard in private session. If a witness objects to answering a question, they should state the grounds for that objection and the committee will consider the matter.

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

Mrs Johnston: No, we are happy to proceed.

CHAIR: Thanks very much, and thanks for agreeing to appear before us at this hour of the morning. In your introduction to your submission you refer to statistics from the United States Department of Justice, which reports that one in five children who use the internet have been approached by a sex offender. Do you think we would be looking at similar statistics here in Australia?

Miss Ronken: Most definitely. What we see generally with this type of research is very similar patterns across the Western world. I would be very surprised if it was at all different here in Australia.

CHAIR: Also in your submission you refer to the fact that in 2013 police contacts shared a case study with you that underlined the importance of prescribing a minimum period for ISPs to retain data. Do you think you can, for the committee and also for those who are watching or listening, explain that case study?

Miss Ronken: Yes, certainly. We were contacted by one of our police contacts. He expressed the frustration the police have in investigating these types of offences. This was one of the cases shared with us. Back in 2008 they had referred a man for online offences and trying to convince others online to sexually assault their children via a webcam. Throughout that case they identified a number of different targets. If I remember rightly, it was just over 30 targets. I think it was around 34. They tried to identify these people to be able to identify the victims in the case. Unfortunately, because the ISPs did not retain any metadata to allow them to be able to identify these targets, the matter just fell to the side. They kept all the information and it was not until four years later when a young girl disclosed that her father had been sexually harming her that the pieces were put together and it was realised that this was one of the targets they had tried to identify back in 2008. The police contact's words were that he was 'completely heartbroken' when he found that this girl had been continually sexually harmed for those four years after they had initially discovered that it was happening. But, because the ISPs were unable to provide them with the data to identify the targets, this girl was left to be sexually assaulted for a further four years. We know that this is only one case and that those other targets that they were unable to identify would probably have had the same outcome and potentially there are children continuing to be harmed to this day because the ISPs were unable to provide that information.

CHAIR: As an organisation which operates very much on the front line dealing with these horrific, disturbing issues, through case studies and examples like this you obviously have fairly strong views on this piece of legislation in front of us.

Miss Ronken: Most definitely. For us, it is just so incredibly frustrating. We share the police's frustration. There are times that they have information that they could act on to protect these kids and get these children out of abusive situations but, simply because of ISPs not retaining the data or not being able to share it with police, children are continually being sexually assaulted. That is really frustrating for us.

Mrs Johnston: Perhaps I could add to that that we know that trying to find evidence to prosecute sex offenders is very difficult. This is why we have such a low conviction rate, because it is such a difficult crime to prosecute. And this is an opportunity where there is actually evidence; the police can get evidence. And we would hate to see that squandered, because it is critical in terms of child protection that this metadata is retained and that police have access to it in order that they can identify children who are at risk and go in and rescue them.
Senator BUSHBY: Thank you for your submission and for assisting us today. I think the evidence you are putting before the committee is very strong, because it is about the front-line effect of what the law enforcement agencies can do with this data. But my question goes to your submission regarding the data retention minimum period. I note that in there you support the two years, but you also suggest that after a three-year period an assessment be made of whether the two-year retention period is appropriate. Is that because you think it might be too long, or could be not long enough, or both?

Miss Ronken: Potentially it could be either. I think that we know that in the European Union’s experience most of the investigations were able to be completed within months. But we also know that from the police perspective sometimes there is information that comes forward after a much longer period. So, for us the two-year period is ideal, but we recognise that we probably do need to reassess that after a period of time to see whether or not it is appropriate.

Mrs Johnston: Just to check it with normal business practices—I think in terms of collaboration between police and the ISPs and just to see what is actually required to achieve the outcomes we are all looking for without putting too much pressure on anybody, really. We need to keep people safe. So, however long we need to keep the metadata for to do that is how long we need to keep it, and we think that two years would satisfy it. But we could be wrong.

Senator BUSHBY: It is a good starting point.

Mrs Johnston: Yes.

Senator BUSHBY: And on the basis of further actual cases, you think it is worth having a review to see whether it should be something different but potentially that could include a longer period.

Mrs Johnston: Yes. We would not want to put something onerous on the ISPs that is not actually necessary. I just think it is fair and reasonable and probably part of normal practice that you review your practices regularly.

Mr Byrne: Thank you, Mrs Johnston and Miss Ronken. I have just a couple of questions. One is: with the example you have cited, have your police contacts indicated to you how much capacity they have lost over the past six or seven years due to the fact that they do not have a data retention scheme?

Miss Ronken: No, they have not shared that detail with us. I know they have shared frustration. Obviously this is their job, and they are very passionate about it, and this is a hurdle for them, and the cost of having to pay to get that data in was also a major issue. Obviously as an organisation that is dedicated to protecting children our position is that ISPs and others have a moral responsibility as well as a business responsibility to ensure that they participate in whatever business they run—in this case, providers of online services, social networking services—that they cooperate with authorities to maintain the laws of the country, and that includes keeping children safe.

Mr Byrne: Do you get a sense from your ongoing conversations with law enforcement agencies up in Queensland that they feel that there is diminishing capacity for them to move to prosecution and investigation of these individuals because of their diminished capacity?

Miss Ronken: Absolutely. We work with police right across the country, and it is a common thread of conversation.

Mr Byrne: I have just one last question. And perhaps I could just commend you for the work you do in, as you say, keeping our children safe, particularly Mrs Johnston. You were indicating that you supported a review or periodic evaluation of the functioning of the legislation. Did you have any sense of a time frame in which you would think that review should be conducted?

Miss Ronken: After the first two years perhaps we could look at it and see how effective it has been: talking to police, getting the stakeholders around the table, looking at the costs on the ISPs—bang for buck, if you like, to be crude—and find out just how successful this has been. We are confident that it will be highly successful and that when we look at the individual lives of the children that this will save—and when these offenders are prosecuted of course they are removed from being able to offend again and again—I do not know what cost you could put on that. But I think the community needs to understand this too—not just for the ISPs and police and agencies like ours but also for the general community, to understand the rationale behind these types of legislation and the effects of it to remove any threats and all the issues that are being raised in opposition to this.

Mrs Johnston: And I think the two-year period would be able to do that, and I think to the community it is quite important—the effectiveness of this legislation and the real impact from this on protecting children.

Mr Byrne: Mrs Johnston, you mentioned a period of two years before you think the legislation should be examined. Do you think that this committee is the most appropriate committee to conduct that examination after the two-year period?
Mrs Johnston: It is probably out of my brief, but I would imagine so. I cannot imagine why not. But it is not really something I feel confident to comment on.

Mr Byrne: Thank you very much for your evidence.

Chair: If there are no more questions, I would like to thank you for giving evidence today. And thanks for your submission and your ongoing work in this space. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward it to the secretariat as soon as possible. If the committee has any further questions the secretariat will write to you.

Proceedings suspended from 7:47 to 8:01
WILLIAMS, Professor George, Private capacity

Evidence was taken via teleconference—

CHAIR: I now welcome the representative of the Gilbert + Tobin Centre of Public Law, Professor George Williams from the University of New South Wales.

Although the committee does not require you to give evidence under oath, I remind witnesses that this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the house itself. The giving of false or misleading evidence is a serious matter and may be regarded as 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?

Prof. Williams: Yes—and thank you for the opportunity to make a submission in oral form on this legislation. I differ somewhat from some of the other submissions in that my starting point is I do accept in principle the government's object of providing a regular scheme for data retention in Australia. I accept that there is a need for such a scheme, given the use to which such data has been put and how it will be used in the future in terrorism and other investigations. I also accept that, if no legislation is enacted, we will be left in the position of the ad hoc scheme we have at the moment, which I think is clearly unsatisfactory on a number of fronts. So the question from my point of view is only: what sort of scheme should we have, and is this an appropriate scheme? My concerns relate to that, in that I do not think that the bill in this form ought to be passed. In particular, I have three key concerns that I think need to be remedied before parliament ought to enact it.

The first, as has been raised by the submissions, is that I think that the bill does not do enough to make clear what data needs to be retained. Of course, guidance is provided in section 187A(2), but it is fairly loose guidance in the sense that the categories there only need to relate to one of the matters in order to be retained. Even on issues such as the question of web-browsing history, I am not convinced that that guidance would prevent the mandatory retention of data—that, even if it does not directly set out the web-browsing history, it might not perhaps enable the history to be reconstructed. The absence of clear data retention information leaves great uncertainty at the core of the scheme.

The second concern that we have in our submission is that the legislation does not do enough to make clear which bodies will be able to access this data. If we turn to the two different sections that deal with that—and they are in a similar form—they both provide a mechanism, firstly, for identifying which bodies can presumptively access the data, such as under a criminal law enforcement agency definition; but, after that, they give a wide discretion to the minister by legislative instrument to declare other bodies to be a criminal law enforcement agency or an enforcement agency. If I can take the committee through the legislation, it seems clear to me that that discretion is a very wide one.

The key section is subsection (3) of section 110A. It says the minister may declare an authority or body to be a relevant agency and, in doing so, the minister need only consider the variety of matters in subsection (4). The key point is that those matters in subsection (4) are only matters for consideration; they are not mandatory requirements. It is possible, for example, to declare a body to be a criminal law enforcement agency even though it does not have a function of investigating serious contraventions. The minister has got to consider that, but it is not built into the legislation as a requirement. Similarly, in clause (f) of subsection (4), the minister can take into account 'any other matter that the minister considers relevant'. In my view, the minister can go through a proper process of consideration but under subsection (3) declare a number of bodies to be either type of agency—they could be local councils, they could be a wide variety of agencies or bodies—because of the absence of mandatory criteria.

The third point that we raise in our submission relates to the authorisation regime. I think it is somewhat accidental that we do not have some sort of warrant regime in the metadata process at the moment. It is due to the nature of how we have got to this ad hoc scheme. But continuing without some sort of authorisation process, I believe, is unacceptable. The data to be collected does raise serious questions of privacy, as many of the submissions have identified. The data could be used, and has been used, in solving serious crimes by finding out intimate, important points of information about individuals and their relationships with others, and it strikes me that this is exactly the sort of information that ought to be subject to some sort of warrant regime. Having the self-serve basis that we have at the moment, particularly for bodies like ASIO and the like, who have such a broad discretion, is unsatisfactory, I believe. That said, I do accept that the warrant regime should be of a lower kind than we might find in other contexts.

My key point is that there needs to be a level of political accountability such that, when this data is accessed, at the very least there is some form of ministerial sign-off. It may be that that can be consolidated in some way so
that a single warrant can cover a variety of pieces of information, not only of this metadata kind or stored communications but also other types of surveillance information. It may even be that a class of information could be collected under the scope of a warrant, and I would accept the need for administrative efficiency with regard to that. Nonetheless, the absence of political accountability, given the potential to authorise even local councils and other bodies, is quite concerning, we would say.

They are essentially our three points, and we believe that if those things can be satisfactorily remedied then the bill ought to be passed.

**CHAIR:** Thanks very much. Do we have any questions?

**Mr BYRNE:** Professor Williams, you mentioned, I think in your submission, an issuing authority in terms of a single point of contact for authorisations for metadata to be accessed. Given the number of access requests that would have to be processed, is there any way around that? I do not know if you have looked at the United Kingdom legislation, but my understanding is that, with this emergency bill that they have pushed through the parliament, they have a single point of contact that each of the organisations seeking to access metadata have to go to. It could be a series of single points of contact. If this bill were passed into legislation, do you think we could examine something like an issuing authority? You have mentioned that in the past and also with respect to the SIOs. To try to funnel where those requests might come from or have some filtration process, there should be something like a single point of contact or an issuing authority—or, given the vast number of requests that you would have, issuing authorities or single points of contact.

**Prof. Williams:** I think that would be wise, yes. My point is only that there ought to be some external authorisation to the agency—ministerial, an issuing authority or the like. We do note in our submission the potential for a significant administrative burden if the warrant process is not done in the right way. I think it is one where we would recognise the limits of our own expertise. The agencies themselves might have some ideas as to how it could be done in a very efficient way—a single point of contact, possibly yes; minister, possibly yes; or perhaps even by consolidating some of the warrant processes so that, instead of going through a variety of processes, you can get a warrant covering a number of types of collection of information about a person so you do not need to deal with them on a separate basis. We do not have a firm view, simply because we would accept the agencies are better placed to know what would be efficient and effective.

**Mr BYRNE:** Could you have a look at the United Kingdom system for us and take on notice and provide some comments to the committee about that if you have the time? I understand that they have set some additional privacy protections that are not explored by the draft bill that is before us at the present period of time.

**Prof. Williams:** I am happy to take that on notice.

**Mr BYRNE:** Thanks. Do you think there should be a sunset clause with regard to the implementation of this particular regime should it be passed into law?

**Prof. Williams:** I would actually prefer a narrower regime that deals properly with the issue. I have not put forward the need for a sunset clause, and that is because I think it would be much better to get the legislation in the form it ought to be. This measure is not unknown in other countries; there are many nations that have data retention regimes. We already have a form of ad hoc data retention in Australia. I would say, though, that if we do not incorporate the sort of safeguards that many of the submissions are urging then a sunset clause and a mandatory review would be necessary, but it would be very inadequate to do that as opposed to just getting the legislation right in the first place.

**Mr BYRNE:** That is a good point. In terms of the draft data set, do you have a view as to how we on this committee could get greater clarity? Do you think we should accept as a committee that this should be just a regulation rather than incorporated within the body of the actual legislation?

**Prof. Williams:** I do not think that it is done in an adequate way at the moment. I accept the government's design for a level of flexibility; that does seem appropriate to me. But, to be frank, we have moved beyond flexibility to actually not telling much at all of substance about exactly what data will be collected. All we have are some guidelines which are fairly loose given they are relating to criteria, and I think what you have ended up with is a shell of a scheme that does not give you enough information about what data has to be held, who can access it and in what circumstances that can occur. On each of these key points I think parliament ought to be given greater clarity and so should the community. Regulation, in my view, is very unsatisfactory. I note there have been a number of other parliamentary reports and the like dealing with exactly that issue. So I think the balance here is to define as precisely as possible what the data set is while providing a power to the Attorney to make appropriate modifications to that within limits so that there is a degree of flexibility over time.
Mr BYRNE: We had evidence by ASIC yesterday that they discovered on the day that the legislation had been tabled that they were not automatically on the enforcement bodies list. They had some concern about the fact that, should the minister declare by legislative instrument that they be an enforcement body down the track, that could be subjected to challenge. Would you have a view as to whether or not that power that has been delegated to the Attorney-General minister could be subjected to challenge? Does that present an impediment to the Attorney-General's Department's desire to have bodies added onto that list of enforcement bodies subsequent to any legislation being passed?

Prof. Williams: I will say that personally I was surprised that ASIC was not on that list given its role in investigating quite serious crimes involving what can be significant criminal penalties. It would be much better for the list to be exhaustive and to include the appropriate bodies in the first place. As to adding bodies in the future: certainly challenges could be possible. The minister makes a decision that could be the subject of a variety of legal challenges, and that ultimately might be quite significant in proceedings because, if you can undermine the ability of the body to get the information, perhaps you might even be able to prevent the admission of that information in court proceedings and so prevent a prosecution.

That said, I think it is actually going to be quite difficult, if all the procedures are followed, to stop appropriate bodies being declared, and that is because, as I indicated in my opening remarks, the key clause is three, and it actually does not set down any criteria. It simply says the minister may declare the authority or body to be a criminal law enforcement agency or enforcement agency. There is no mandatory criteria. All the minister must do is consider certain things. So long as the minister properly considers them—the minister can consider, for example, whether they investigate serious contraventions but give it very little weight or determine that other factors such as those in any other matter should be given greater weight. So, yes, challenges are possible; but, if the minister follows the procedure appropriately, it is a very open door to nominating a number of bodies, including ASIC, that might be covered.

Mr BYRNE: That was one of the concerns with the previous committee, as you would be aware. It was the number of bodies that, as you say, could self-serve people's personal and private information. A thought that came to mind was: what if the Attorney-General then sought to prescribe by legislative instrument additional organisations? Do you think an appropriate safeguard would be that that would come before this committee so that we could examine whether or not it would be appropriate for those bodies to be added, given that we do have some measure of expertise in that area?

Prof. Williams: It would be a welcome safeguard because it would provide a level of scrutiny that is not otherwise there. Of course, your committee already fulfils similar roles with regard to prescription and other forms of Attorney's decisions. So that would not be inappropriate, but still I think it does not get to the heart of the concern that many people are expressing: that there should be greater clarity about the point of not only which organisations but, as you have indicated, the self-serve nature once declared that they can access the information. The information could be quite trivial. There is no requirement to access information about serious matters. Despite indications that this would only be used for serious crimes, there is nothing in this legislation that requires that. One option to overcome that issue might be, for example, to say that information can only be accessed if it does relate to serious crimes—perhaps punishable by a year or more in jail. Otherwise, the real prospect is that you could have local government bodies accessing information about parking infringements and the like. Indeed, that is far from fanciful; that is an issue that has arisen in the UK.

Mr BYRNE: Thank you for that. When you look at some of the comparable schemes in countries like the United Kingdom, would there be any other independent level of oversight that you would recommend if this data retention regime were implemented?

Prof. Williams: In looking at those other counties, the lesson I get is that oversight cannot fix this bill. As I just indicated yesterday, ASIO can comply with the law and do so rigorously, but nonetheless the problem is the existing legislation is so broad that information can be sought lawfully that is quite questionable in terms of whether indeed that private information should be accessed by an agency in the first place. So oversight cannot work unless you tighten up these key issues. What I would like to see is a bill that reflects the public statements of the Attorney in particular, indicating for example that it will not be used for things like copyright infringement and will be limited only to serious crimes and the like. I think a bill of that kind is appropriate, but this is not that bill. We do not have those safeguards built in. Even if the current Attorney does not want to go down the path of extending it into more trivial matters, there is no doubt that a future attorney could seek to do so.

Mr BYRNE: I do not know if you heard the evidence from IGIS about ASIO keeping data past a certain point and it not in fact being destroyed? Did you have any particular perspectives on that?
Prof. Williams: I did not hear the evidence. I did look at their submission. I was not surprised. It is almost a laissez-faire system for ASIO given that it only needs to relate generally to their operations. That is an almost nonexistent threshold given the breadth of their operations and the scope with which security might potentially be defined. And again there are problems there, of course, in terms of the use of the information and just how trivial it might be. So I think significant tightening up there is required. If we are going to move to mandatory data retention—which, as I have indicated, I support—then surely coming with that must be the appropriate procedural and other safeguards and greater clarity about how long information is held for and the circumstances in which it can be sought.

Mr Byrne: If the committee agreed to pass this particular bill, would you then suggest that as part of that we have a mandatory data destruction component of it—that any data that was not necessarily relevant to an investigation or that had been used and finished with by any enforcement agency, including ASIO, would be destroyed?

Prof. Williams: I think that would be appropriate and I think that would allay community concerns that their private information may be sought, perhaps legitimately, but then held for an extremely long period of time—well past the nature of the investigation—and perhaps looked at again sometime down the track in less appropriate circumstances. I think the community concern about what some see as a blanket surveillance regime is that the onus is on parliament to make sure a scheme is designed that is very well tailored to the problem. And there is a problem that needs to be met here. We need a bill that removes many of the quite significant loose ends, that being one of them, that as yet have not been adequately dealt with.

Mr Nikolic: You said a moment ago 'oversight cannot work'. Given that we are not trying to change the capacity of agencies to access metadata—we are simply trying to standardise the period of time for which metadata is held—how is oversight by the Ombudsman, IGIS and this committee failed to date in providing necessary protections? What egregious breaches can you point to?

Prof. Williams: What I said was that oversight cannot be effective in ensuring that a scheme operates within narrow and proper limits, when the legislation itself does not set down those limits. Oversight can only hold agencies to limits that are written into the legislation. My point is simply that we cannot expect oversight to achieve the sort of policy objectives I am suggesting—that is, narrowness in terms of, for example, when agencies access data, because the oversight function cannot actually compel that without the legislation reflecting it.

But I think your question also raises a broader point in terms of asking about breaches and the like. One of the concerns of the community and that I have about this is that if there are concerns of this kind we are unlikely to find out about them. By nature these processes tend to be secretive—they should be secretive. So I think it is important up-front that we know very clearly the limits on the scheme, knowing that it may well be that if something does go awry that it may not actually come to light.

Mr Nikolic: On page 2 of your submission you say:

… government has failed to satisfactorily justify why data should be retained for a period of two years. … [and] a stronger case needs to be made as to why it is necessary.

I am trying to weigh that view against substantial other evidence provided to the committee, including from the head of the AFP on 17 December, who talked about the absolute necessity, from his point of view, for a two-year period. New South Wales Commissioner Scipione says:

There's not a terrorism investigation since 9/11 that hasn't relied on metadata.

David Irvine, the immediate past DG of ASIO:

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

As I said, the head of the AFP said:

Without a 2 year data retention period, the AFP is concerned such investigations, which rely heavily on telecommunications data, will continue to be frustrated by inconsistency in the retention of data by Australian service providers.

In light of your view that government, and, I guess, by extension, the agencies have failed to justify the need, what weight, if any, do you place on the evidence of those people who actually conduct these operations.

Prof. Williams: It is a good question. The first thing I will say is that that statement was made on 9 December, when we did not have access to other submissions that now have provided a much higher degree of detail about this. Indeed, I would say that I am very pleased to see that those agencies are now strongly making the case as to why that two-year period is necessary. One thing I have also looked at carefully is the table on page 30 of the Attorney-General's Department's submission, where, based upon European data, they have also given an
indication as to when certain data is accessed. I do not have a strong view on this issue, because I think it is one that depends very much on operational issues. I think it gets outside of my expertise.

But I suppose the threshold question for me is that, based upon the European data, over 90 per cent of all requests are made within the first 12 months. Is the case compelling enough to extend it for another 12 months, given the cost and the extension of the scheme? As the submission indicates, it perhaps might be justified if it can be shown that in fact terrorism investigations, particularly, tend to take place in that second 12-month period. If that is the case then perhaps that threshold that I have indicated might be met.

Mr NIKOLIC: Could I acknowledge your comments there. Indeed, some of the comments we have received from the AFP highlight the difficulty of, for example, getting a lead with one carrier in a particular serious crime, potentially dating back 12 months, only to find that the links to that person and to others cannot be verified because the other carrier keeps the data for only six months, or not at all. So I agree with you that the case is being made out much more strongly. The other compelling piece of evidence I have heard in recent days relates to victims of crime, who often report well after the event. In some cases, when it comes to sexual crime, it is a considerable time after the event. For me, I found some of that evidence equally as influential as your are making it out to be.

Prof. Williams: Yes, I do find that evidence influential. I think the government has two choices. One is to remove the ability of agencies to access metadata and say that we should not be able to do that, in which case you would move away from the ad hoc scheme, or you move to what is being proposed: a scheme that is not ad hoc but actually deals with things more systematically. But I think the worst option, and the only one that is clearly not justifiable, is staying where we are. It is a scheme that has grown up without much thought. It is inconsistent. It does frustrate agencies in terms of their ability to access information across different networks. Also, it does not contain any of the safeguards that should be there. So the current situation is the worst. I think also it is clearly not satisfactory to remove access to the metadata. So for me the obvious solution is to move to a better scheme, but as I have indicated in my submission, do it properly and rigorously to satisfy people as to the appropriate use that will be made of that scheme.

Mr NIKOLIC: A number of submissions have talked about warrant access not just to data but when it gets into the content side of things, when the agencies have determined that they want to go a little bit deeper in exploring some networks or individuals of concern, but indeed in the pre-access period, when access to metadata is being sought. I am intrigued by the perspective that metadata is as privacy sensitive as the actual content of communications, which requires a warrant. But aren't non-warranted powers a normal part of any law-enforcement framework, whether it relates to banking, finance or health care? Also, are you aware of the distinction that Frank La Rue, the special rapporteur for the United Nations Human Rights Council, has made in a recent report that clearly distinguishes between the need for warranted access when it comes to content but says that an oversight mechanism is sufficient, if you like, for the metadata component? Why is your view different to that expressed by the special rapporteur?

Prof. Williams: Firstly, I would certainly say that, yes, I do think there are different degrees of information that require different levels of authorisation. I think there is a clear distinction between the stored communications as to content and metadata. But I do think that with metadata—in identifying the time, the place, who someone has communicated with, and, potentially, also enabling the reconstruction of web browsing history and the like—that is of its nature. I think the community is sending a pretty strong signal to your committee that they do see this information as sensitive. You only need to look at the public debate and the public reaction about this to see that the community does not see this as ordinary information but is actually very concerned as to the circumstances in which government agencies would access it.

I think therefore the question is: what authorisation regime should be in place? I am not proposing a heavy compliance regime like that found for other types of warrants, but something that is administratively efficient. The key point for me is that at the moment this scheme can operate without political responsibility being undertaken for metadata requests. That I think is very unsatisfactory because matters of this kind ought to have a level of political responsibility attaching to them such that in parliament and other places it is clear where that responsibility lies.

Mr NIKOLIC: Your comment about community concern is obviously engaging the minds of the committee. I have had a look at some of the data that is available on community perspectives here and I note a Lowy Institute poll in February 2014 that asks people to rate threats to Australia. International terrorism and cyber-attacks from other countries are identified by 94 per cent and 88 per cent respectively as being critical or important. And 80 per cent of respondents accept the need for some imposition of individual rights in dealing with counterterrorism. A total of 68 per cent agree that government had struck the right balance between protecting individual rights and
fighting terrorism. And over one in 10 thought that the government leans too much in favour of individual rights and needs to do much more in this area. Given the events after February 2014 that we have seen in Australia and elsewhere, I would imagine that those statistics could potentially even be stronger. I guess that is probably more of a comment. Feel free to respond should you wish. But to me that is fairly compelling evidence about public perspectives when it comes to action in this area.

Prof. Williams: I agree and I have no doubt about not only the community feeling about that but the demonstrable need to act in this area. It is why I actually support the government's in principle attempt to bring about this scheme. So it is the details I am concerned about. I also accept that seeking metadata will breach a person's privacy, but I think it is appropriate for that to occur. It only needs to be subject to safeguards to make sure it only occurs in the right circumstances.

I think the key distinction, though, between this regime and, say, the earlier bills your committee has looked at is that this regime potentially applies to every Australian. That is something that can change minds and also raise concerns. It is not as if we have been free from examples in the past where agencies have inappropriately sought information. I am not pointing any fingers, but there are many examples, even getting to roads and traffic authorities and the like, where people within organisations have acted inappropriately. These are the sorts of things that I think would make the community say, 'Yes, we accept the need for this, but you must have a scheme that makes it very clear that this is only accessed in the right circumstances.'

Mr CLARE: Professor, thank you for your submission. The three points that you have raised today are points that have been raised in a number of submissions to the committee. The point you made about whether the dataset should be in legislation or regulation we have had presented to us by a number of organisations.

I wanted to ask some questions, if I might, about your second recommendation—that is, that the power of the Attorney-General to declare law enforcement agencies under this bill should be more narrowly defined, or that we should reduce the scope of the power that the Attorney has. In your submission, I think you say that the Attorney should only be able to declare an authority or body as a criminal law enforcement agency if they are satisfied the agency is involved in investigating serious contraventions. In other evidence we have heard, it has been recommended to us that this power might it be limited to agencies that are responsible for investigating matters that are determined to be serious offences as defined under, I think, section 5 of the telecommunications interception act. I am just wondering if you might be able to provide us with more details about how you think the scope of the Attorney's power might or should be amended in the bill.

Prof. Williams: I think it can be dealt with quite simply. You simply need to move clause (4)(a) of section 110A into clause (3). That is, you would end up with a section that says, 'The Minister may declare, by legislative instrument, the authority or body to be a criminal law enforcement agency where that agency investigates serious contraventions.' So you would make it a requirement, as opposed to a mere consideration to be taken into account. If you said the minister can only declare bodies that investigate those contraventions, then you would provide a bill that is consistent with the statements of the Attorney-General, in that it would be limited to those sorts of bodies. I think that would allay the concerns I have, and many people have, because that would rightly knock out the large range of bodies that, frankly, should not have access particularly to stored communications.

CHAIR: To follow up on that, is that term 'serious contraventions' clearly defined? Would it be clearly understandable exactly what that meant?

Prof. Williams: It may well be appropriate to define that. You might, for example, limit it at a fairly high threshold to offences carrying, say, a criminal penalty of one year in jail or more, which is often regarded as a standard for a serious crime, or it could simply be something that involves any jail term, perhaps, to cover lower order offences as well. I accept that if you were to make it a mandatory requirement you would want greater clarity on that, but at the moment there is no clarity and it is only a mere consideration. So it is actually doing a very limited amount of work.

Mr CLARE: My only other question relates to your third point, which is the proposal of a simplified warrant regime. This has come up in some of the submissions that the committee has had presented to it. The counterpoint by law enforcement agencies is that there is a significant cost involved in any warrant based process, whether it is an internal process or a court based process. The practicalities of doing this are quite difficult, given the extremely large number of metadata requests—tens of thousands in any given year.

You made the point in your oral presentation today that this might be by way of some type of simplified sign-off at a political level by the Attorney-General. But would you be concerned that, if this was done in an extremely efficient way so that you would not have the Attorney-General signing off tens of thousands of different documents, it would be so generic as to be worthless?
Mr DREYFUS: I have a question relating to legislative drafting practice. We have been told by the government that the regulation to give expression to the classes of telecommunications data that companies are going to be required to keep is almost ready. It is being prepared now and of course this committee would hope to see it. But, as a matter of legislative practice, if something can be included in a regulation there is absolutely no reason, is there, that it could not be included in a bill?

Prof. Williams: That is certainly right and that is why I have been perplexed about the approach to this bill, because one way or the other it has to be drafted into legislation. Whether it is in a regulation or a bill makes no difference. In fact, you quite typically find in bills and legislation, as you well know, very elaborate schemes, definitional and otherwise. So it is obviously a strategic or political decision to put it in a regulation rather than a bill. But, as I have indicated, I think it is very inappropriate given that the definition itself is at the heart of whether the scheme should proceed in the form of this bill. It is something that excites some of the greatest community concern.

I suppose my underlying concern as well is: even though that has been indicated, do we even have a workable definition yet? Given public comments, I am still concerned that the government has not actually worked out what the data required to be retained is. I personally would like confidence about that. Even if we were stuck with the regulation, then you could not pass this bill without actually seeing the regulation, to have confidence that we know the very information to which it is going to apply.

Mr DREYFUS: Further on legislative technique, the bill already has within it a provision that would permit a ministerial lessening of the time period for retaining certain classes of data. As I understood your earlier answer to Mr Clare, your preference would be to see the bill contain the primary list, as it were, of all classes of data to be retained but it could provide for a regulation power for that list to be adjusted later—as indeed it already does in one respect, because it provides for a lessening of the retention period.

Prof. Williams: That would just be the normal way of dealing with this. And I must admit that when I first read the bill I was very surprised to see that the normal process had not been followed. And flexibility is required here, but set out a primary definition with a regulation-making power, and this does not strike me as an appropriate instance to depart from that normal course. In fact, it is a very clear example of something, in my view, given the community of interest, that this does need to be dealt with up-front, and the community needs some reassurance as to the sorts of data we are talking about, rather than merely passing a shell of a scheme and leaving that debate down the track.

Mr CLARE: Perhaps I could just ask one follow-up question on that point about having a primary definition in the bill and then a regulation-making power. In answer to a question by Mr Byrne, you made the point that you thought it would not be a bad idea, in the case of the Attorney-General making declarations relating to law enforcement agencies, if they came before this committee before those regulations were made. Do you have a similar view in relation to any regulations made that would alter that or supplement that primary definition of metadata or the dataset relevant to this legislation?
Prof. Williams: Well, the first point I would make as to both the definition of the data and the enforcement agencies is that the bill should just be very clear about what it has done, which would actually lessen the need for your committee to be actively engaged. I think your committee would need to be engaged if we have such a vague scheme that in the end it is so open-ended that anything from here needs exactly the same sort of scrutiny that you are providing now. If we have a tighter scheme, so only certain types of agencies can be declared, and if we also have a bill that sets down clearly what the data to be retained is, with guidelines as to how regulations can be made in the future, of a kind that is already there—so it is not an open-ended regulation-making power but a constrained one—then I think you would not need to mandate this committee being involved. But, nonetheless, it might still be involved in appropriate circumstances if a particularly significant decision was made that particularly sought to extend the data.

Senator BUSHBY: Thank you, Professor Williams, for assisting us today. I just have some questions about the warrant process that you recommend. I note that in your submission, on page 5, you say that you are concerned by the prospect that enforcement agencies will effectively be able to access metadata on a self-serve basis. Without adopting your terminology in terms of the self-serve basis—which I will come to in a minute—it seems to me that you are suggesting that there will be a change in process for agencies in terms of how they access metadata, whereas the evidence before this committee suggests that there is no change in the process or the legislative authority for agencies to access metadata; all that this does is remove the ad hoc nature of retention of that data and try to consolidate and put in place, as you were just discussing, a degree of certainty around what metadata is retained and for how long. Are you suggesting that there will be a change?

Prof. Williams: No, and my underlying concern is that I do not think the current system is appropriate, but I think it is somewhat accidental that we have got to this position where agencies can access vast amounts of data—tens of thousands, perhaps, over a number of years—without any form of clear political accountability. I think the scheme has grown up without actually being designed properly. And if we were starting fresh—let us say we did not have this data access that we have at the moment—I do not think there would be any doubt about the need to have some sort of authorisation process in play. It is just that we have this unfortunate ad hoc regime that I think we need to move beyond.

Senator BUSHBY: Earlier you said something along the lines that there is nothing in the bill restricting the use of the info to serious crime et cetera. I am not sure; you may well be correct in terms of this bill. But as seen in ASIO's submission, and also evidence that we have received from the AFP and otherwise, there are accountability and oversight arrangements in place. And just looking at the ASIO submission, on page 43 they go through some of those that guide them in terms of what they do and actually restrict them in what they can do with this metadata. They talk about six guiding principles which are being incorporated within their oversight and accountability measures, including in the ASIO Act, which regulates the purposes for which ASIO can collect, analyse, share and report on intelligence, and guidelines issued by the Attorney-General which require their intelligence methods to be proportionate, and so on. There are in-built accountability measures that apply to ASIO and similarly to AFP. With AFP we heard evidence yesterday that the Australian Commission for Law Enforcement Integrity would monitor the use of this sort of material and if it came to their attention that it had been used outside authority then they would consider that a corrupt action and take action accordingly. So, although you may well be correct in saying that there is nothing in this act, there are in other acts and other accountability measures restrictions on what agencies can do with the metadata if they access it. Isn't that correct?

Prof. Williams: Certainly I accept that there is a range of other accountability measures that do apply in these circumstances. I would say with regard to ASIO that I did look at their submission but it says on their submission that it is confidential to the committee, so I do not have the benefit of the information in their submission.

Senator BUSHBY: The one I am reading from is actually a public document.

Prof. Williams: That is my mistake in that case. I would say that I think when you are moving to a mandatory data retention regime for two years, given the controversy it has excited, that even though yes, I do accept that there is a range of other accountability and other measures in place, it would be sensible in this bill to set them out directly, with clarity, and to make very clear the circumstances to which the information can be used, because I am not convinced that those existing measures are sufficient. Indeed, when I look, for example, at the submission of IGIS, it says to me that the threshold is too low and really it does deserve to be tightened up. And it is a quid pro quo that on the one hand I think yes, mandatory data retention can be justified, but coming with that should be certain obligations and safeguards that are not currently there to convince the community that under this new scheme the data will only be used wisely and appropriately.

Senator BUSHBY: Okay; I will leave it at that.
Mr RUDDOCK: Perhaps I could be mischievous enough to take up what evidence you may be able to offer about abuse. My understanding is that we have had a scheme in place, which you call ad hoc, and it has been there for something like 20 or 30 years, probably getting something of the order of 60,000 or 70,000 or 80,000 requests, and you wonder why there has not been some clamour to contain it. Isn't it because it really has not been abused, and there is no evidence of abuse? And we are only looking at this because we are now legislating. And I wonder whether, in terms of your submission, you are able to give us clear evidence of abuse that we should take into account when considering your suggestions.

Prof. Williams: Firstly on the ad hoc point, I see it as ad hoc because yes, it is an old scheme, and it was a scheme that was never designed for the electronic age in which we live. And of course at the time that many of the changes were originally made it just was not anticipated that metadata of many of the contemporary forms—through smartphones and the like—would be available. So, it is a scheme that just has not yet been updated. And, again, I support the government's objective of doing so.

In terms of abuse, I am cautious in my use of words in terms of potential for and fear of abuse. And of course it is something that has been very prominent in public debate. My underlying concern is that even though I do look at agency reports and the like this may simply not come to light in a way that the community would hope, partly because it is such an open-ended scheme in terms of how it might be used. So, the rigorous requirements are not yet there. And also the level of secrecy involved—appropriately—in the use of this information means that if there are issues arising it is not always clear that that would get the community attention that it might warrant.

Mr RUDDOCK: We could have a discussion privately some time. Even traffic cases: say someone is arguing to defend themselves—‘I wasn't there when the car was parked’—and you are able to find out that they were actually using their phone at a time when the car was parked at a particular place. It might have been a speeding offence. I remember the case of a former judge where this was a relevant issue. They are not serious offences. Maybe it is just helping our profession to give people a basis for getting themselves off.

Prof. Williams: Well, I think there is a distinction here between the example you are pointing to, which involved perjury, which was a serious offence and of course led to a jail term, and on the other hand whether it is appropriate for a local council to access this information where someone says, 'You gave me a parking ticket but I was not there.' Of course, metadata would be very useful to identify, 'Yes, you were there. Your phone shows you were there.' I think this is where—

Mr RUDDOCK: So you should get off and I should not.

Prof. Williams: That is a good question. I think the problem is that the bill does not give us answers to that. I think that is where the government should say that if the bill is to be used so that local councils can, for example, properly enforce parking fines then let us make that clear.

Mr RUDDOCK: I was willing to take councils off but you are helping to persuade me that maybe we should leave them on!

Prof. Williams: I am actually somewhat ambivalent about them, to tell you the truth.

CHAIR: Just for the record, I think this is Mr Ruddock's sense of humour. For all those who may be a little confused, he has a peculiar sense of humour.

Prof. Williams: I am well aware of his sense of humour. I have enjoyed it in the past.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions the secretariat will write to you.
ELSEGOOD, Mr Michael, Manager, Regulatory Compliance and Safeguards, Singtel-Optus

EPSTEIN, Mr David, Vice-President, Corporate and Regulatory Affairs, Singtel-Optus

[8:51]

CHAIR: I now welcome representatives from Optus. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as 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 Epstein: I will make some brief introductory remarks, essentially going to a summary of what we have submitted. Just as a preface to those remarks I thank you and the committee for extending me the courtesy of being able to appear today when I was occupied yesterday.

Just to provide some context, Optus, as you well know, is a retail service provider that serves over 10 million customers a day across a broad range of communications services. While we are not the largest carrier in Australia we do offer the widest array of communications platforms because, in addition to all of the services that people who have appeared before you have offered, we also offer satellite services. In addition, we operate a range of wholesale services on behalf of, at times, hundreds of other carriage service providers. So we can offer some perspective from that point of view.

In short, we are a fairly significant and critical national communications infrastructure operator. We have also invested in a range of equipment and processes that enable interception delivery capability across all of our platforms and services. Indeed, we operate a specialist team to service these functions called the Law Enforcement Liaison Unit, which essentially responds to requests for lawful interception, authorised requests for call data and other related requests from law enforcement and national security agencies.

The costs of this team and the infrastructure and capability to support it are, as you might imagine, substantial. Therefore we are a very interested and affected party when it comes to the proposed data retention regime. I would say at this point that we consider it ultimately a matter for government—and yourselves and indeed the wider parliament—to balance the fundamental principles at stake here in the proposed data retention regime. By that I refer to, obviously, the extension of state or federal government powers over individual data and, indeed, data held by corporate entities and the balances that have to be applied when it comes to privacy principles, civil liberties, the utility of the information and the utility of providing guaranteed access to certain sets of data for law enforcement and national security purposes.

We are, I reiterate, of the belief that this is very much the prerogative of government and the parliament, and we would not presume to conclude what the appropriate balance is or necessarily present a view on the relative merits—I will leave that for others. What we are really here to discuss are the operational implications and the practicality of what may or may not be proposed.

In this context, I would make some overarching points in terms of what we would see the priorities being for effective cooperation: first of all, a practical and stable legislative and policy framework which provides for business and compliance certainty for service providers. We do think that consideration should be given to a capital contribution from government to service providers where appropriate to meet implementation costs which may go beyond the normal parameters of what is expected of carriers and, indeed, social licence commitments, broadly defined. Also, any arrangements should be consistent with the privacy expectations of our customers and not unduly undermine the confidence and position of trust that service providers have to hold in the eyes of their customers.

In terms of what has been proposed, what is publicly available and what has been discussed with us in a range of fora, we consider the proposed dataset to be basically workable, with the critical proviso that, obviously, the appropriate level of detail and interpretive guidance is made available in regulations which are proposed to accompany the bill to prescribe the sort of information that needs to be retained and how it should be retained. We have also appreciated the ability to work with the Data Retention Implementation Working Group, convened by the Attorney-General's Department. Indeed, I think some of those discussions have helped to better inform both their understanding of some of the operational issues that arise and our own, in addition to informing the wider industry.

Against the background of some of those discussions, we made a number of recommendations in our submission and posed some questions. We would note that the proposed obligations impose a substantial net cost, operational scheduling and resource impact on Optus and, indeed, other providers, in addition to what we already
provide, which we would regard as substantial. We do not quibble with cooperating with government and agencies, but we do note that it does come at a cost. On this point, we have not been in a position to provide a definitive estimate of the costs under the proposed regime, although we have been cooperating with both the government and the Attorney-General's Department consultant, PricewaterhouseCoopers.

That is all I would say in the broad. It is probably more practical if we move straight to questions, I suggest.

**Mr Byrne:** With respect to the costing, when you say 'a significant cost impost', you are not in a position, I presume, publicly to disclose that—

**Mr Epstein:** Correct.

**Mr Byrne:** but you have disclosed that to PricewaterhouseCoopers—or a rough estimate. You said you did not get the exact cost, but one presumes that you have roughly estimated how much it might be.

**Mr Epstein:** For the record, I will make it clear that we do regard it as commercial-in-confidence and, while it is to some degree a matter of speculation and discussion, it is difficult to even provide indicative public numbers, just because they go to business processes that are very sensitive to our business and, indeed, could go to processes that might be sensitive to law enforcement and security operations. All I would say, at this stage, we have been able to have are ballpark discussions of the costs. As the likely dataset has been more refined, as I said at the start, we are certainly a lot more comfortable that we have got a workable regime and therefore something upon which to cost, if it is finalised. We have not given a definitive figure, either globally or for components, to PricewaterhouseCoopers—though they have recently come back to us and sought some granularity, which we are now attempting to look at.

The only thing I would say, in broad indicative terms, is: you will be aware of numbers that have been speculated about for similar regimes that have been proposed in the past, particularly in 2012-13. There were also some proposals in 2010. Some of those have been speculated about in the media. Our view is that, while the costs are substantial, what is proposed now, though, would be considerably below the upper end of what has been speculated about for previous proposed regimes. Indeed, as discussions proceed, if some of the refinements being discussed proceed further we can see the costs being reduced further, but you are still talking about—

**Mr Byrne:** Significant costs?

**Mr Epstein:** significant amounts of money.

**Mr Byrne:** In those discussions, has the government indicated to you or the technical working group or government body that you would be compensated for those costs?

**Mr Epstein:** That has certainly been a matter of discussion, and all the carrier representatives and indeed the wider industry representatives have put this view in the working group. I would note that the Prime Minister has probably been the most public and the most direct about recognising that there is most likely a need for some sort of capital contribution.

**Mr Byrne:** What would your expectation of that capital contribution be, in terms of the significant impost that you have indicated that might cost your organisation? What would your expectation be if you were able to publicly say what the costs are that the government would contribute?

**Mr Epstein:** Unfortunately, we are in a bit of a chicken-and-egg situation. Until there is broad agreement on precisely what would be required, it is difficult to specify. What I would say is: it is worth looking at some of the principles that you might apply if a cost reimbursement regime were to be put in place. The first thing we would say is that it would be inadequate, and probably inappropriate, to have a one-off regime. The corollary of that is: you would probably have to have a discretionary regime. If a regime were to be put in place, we would not object to any public scrutiny of it. I think that is entirely appropriate, given that it is taxpayers' money. But, for instance, these days the operation of telecommunications networks is increasingly about what I would call software systems and processes rather than necessarily hardware. In the past there have been capital contributions made for particular types of hardware if governments or agencies have sought access to certain types of interception or datasets that the ordinary capability or the ordinary systems of a telecommunications service provider would not necessarily accommodate. Sometimes you can purchase that sort of equipment, or we will have that sort of equipment already in our network or in contemplation for our network, and it has a latent capability where you simply flick a switch or change a line of software code. In that instance, the cost is minimal and, generally, if it is more than minimal, it is certainly of an incremental nature. Sometimes it requires the purchase or the construction of equipment or the writing of code to actually create the capability because it just does not exist and would not have been contemplated by the carrier, either for the management of a network, billing systems or customer identification or services. If it is of a minor cost, generally there is a bit of an iterative process and a bit of a discussion, then we have borne it; if it is of a major cost, governments have agreed to contribute.
We have faced a situation in the past where at one stage—and this certainly applies to both us and Telstra; I am not so sure about other networks—there was a particular type of network equipment that did not come with an in-built capability but it could, in effect, be purchased as a module. It was agreed that government should contribute on a once-off basis. That was later followed by a similar piece of equipment that had a latent capability. The view of the Attorney-General's Department was that we should all suck up the cost and that was a social licence cost. Then we had a third generation of something where we, again, found ourselves in a situation where something significant had to be purchased or a significant modification had to occur. People say, 'To the extent we made a capital contribution it was a once-off, and this is purely discretionary and a social licence cost.' There comes a point when there are judgements about the magnitude of costs and the utility of what has been provided for agencies. So we would say, firstly, there should be capital costs. Secondly, it should be a discretionary regime but certainly subject to scrutiny so that everyone is accountable.

Mr BYRNE: With respect to the costs, if there were not adequate government compensation would you then be required to recover that cost impost from your consumers?

Mr Epstein: That is probably the inevitable consequence, but we all live in a competitive marketplace. It depends on the nature of the marketplace at the time. It is very difficult to speculate on what the actual consequence would be, but you can certainly contemplate a situation where that would occur. It might be a minor cost, it might be a major cost or it might be something that applies to a particular customer class. You have to bear in mind public sentiment, our capacity to pass on the costs and our capacity to identify or not identify the costs. In some instances you may not want to identify the costs because that is actually providing a road map for people you are trying to deter.

Mr BYRNE: If this legislation is passed and there is an implementation process, how long in your view, with the facts that you have at hand at present, without them being finalised, would it take Optus to tool-up so that you could actually retain the dataset that the government would require?

Mr Epstein: In terms of the scoping and the conceptualisation it is not a particularly difficult task because there is not a great variation. The real question lies with the logistics of the capacity to store consistent datasets across a very wide range of platforms for certain periods, particularly when data usage is growing and indeed when networks are, historically, in a very high state of transition. Our view is that the proposed implementation plan, timetables et cetera are pretty workable but it may well take us up to two years to fully implement requirements.

Mr BYRNE: In terms of the fact that you would be storing this particular dataset, do you have any concerns about the fact that there would be other people trying to access that and have you articulated those concerns to the technical working group?

Mr Epstein: We have noted that in our public submission. I think it is a fairly obvious point. Indeed, some of our colleagues from Telstra yesterday noted it before you. Obviously, that sort of thing occurs in today's world. We are in an environment where we are not just talking about security regimes; we are also talking about commercial attacks et cetera. You would expect that sort of thing to occur. Against that, I think it should be noted that if you have got a well-defined dataset it makes it relatively easy to, at least, establish the design of discrete storage and, hopefully, be able to segregate it from your main operational systems and your systems that are potentially more exposed than others. There are two balances here: yes, people are aware that there is a dataset being held and will be attracted to it, but if it is tightly defined and stored in the manner we would envisage it being defined then you have probably got an easier design task in terms of what you need to do to protect it.

Mr BYRNE: Is it your understanding that the information that your organisation would hold in the draft dataset would be destroyed after that two-year period?

Mr Epstein: At this stage that is a little bit ambiguous. It is not a complicated task to build that into the regime—

Mr BYRNE: What you mean by 'ambiguous'?

Mr Epstein: It is a little bit ambiguous as to precisely what you would be expected to do in terms of destruction. I cannot speak for any data that is passed to agencies, obviously. I think that question should be asked elsewhere. I would be asking—

Mr BYRNE: We are asking that one; do not worry!

Mr Epstein: Yes, that would be better addressed elsewhere.

Mr BYRNE: At this stage you are saying that, with the dataset that you would be required to keep, you are actually not sure what you are going to do with it after that time period elapses. Is that where you are saying?
Mr Epstein: In terms of what might be stored for the purposes of this regime—and that obviously depends on the final shape of the regime, if it is implemented—we do not regard that as a particularly confronting question or task.

Mr Byrne: It confronts us, though.

Mr Epstein: It may well—

Mr Byrne: It is not so much the task as the fact that you are saying it is ambiguous about what you are going to—

Mr Epstein: It will not be ambiguous if you or the government come to a view. As I said at the outset, that sort of policy question is very much one for yourselves and the government. But we would stand ready to comply with whatever was requested, and the task of compliance should be straightforward.

Mr Byrne: Thank you for the clarification. I have no doubt that it is a matter that can be technically feasible. My concern is that, considering how far this has progressed, it has not been actively discussed given the privacy concerns that have been articulated frequently in the course of the evidence we have received.

Mr Epstein: I am not saying that we have not contemplated that ourselves. Our view is that privacy is important under any circumstance but I have to say that commercially we regard privacy as very important and so do our customers. Our general policy would be that you do not keep stuff unless you have to. I might just defer to my colleague, Mr Elsegood, because he has been involved in some of the more technical discussions and I am not sure whether this has come up in some of the more technical discussions.

Mr Elsegood: There are probably two broad areas of data that we would be keeping for the purposes of compliance with this legislation. There is information in existing systems which we keep for two years and sometimes longer, and our compliance with this legislation would be met because we are keeping that data for other purposes anyway. There would be other data that we would be keeping specifically for the purposes of compliance with this legislation. I would think that part of the design of that special data storage would be that it would automatically delete the information once it gets to the two-year period.

Mr Byrne: But have you had that direct conversation with government as part of your conversation with the technical working group? I find it a bit odd. You are being commercially responsible. My question is: has the government come to you and said, 'What are the protocols for disposal of the data after that mandatory period has elapsed?'

Mr Epstein: I hear where you are going. We have had discussions with the government which have been quite detailed and very up-front about how the principle of privacy is a matter of concern. I know my colleagues at Telstra have. For example, we have not wanted this regime to accidentally trip conflicts with other privacy requirements we meet either as a result of government or regulatory requirements or as a result of our own commercial decisions. We are proceeding on the basis of scoping out what might be potential designs for storage. You cannot store everything forever. To have a practical storage regime, you would destroy this dataset after the minimum requirement is met, unless there was something like an investigation or enforcement action afoot where you were required to have what we would call a retention regime—and we are used to retention regimes. You could ask me the question a number of times, and I will give you the same answer.

Mr Byrne: You can see that you have been working in politics, Mr Epstein—put it that way.

Mr Epstein: Well, I may well have been working in politics.

Chair: We won't ask which side!

Mr Byrne: Exactly—the good side! You have probably given me all the information I need. From what I heard you say, the government appears not to have had a proper conversation, in depth, about the disposal of the data it is requiring the telecommunications companies to keep. Can I say to you, quite frankly, that is a concern from this committee's perspective.

Mr Epstein: Of course you can say that, because you are on the committee and you are entitled to express a view and an opinion. What I would say in terms of what I was trying to convey to you is, yes, we have had discussions with government. I think they were entirely proper discussions with government. Whether they needed to be extensive or were as extensive as you might expect is a matter of judgement for you, not me.

Mr Byrne: It is almost Yes Minister. Thanks, Mr Epstein.

Senator Fawcett: Mr Epstein, you said in your opening remarks that the dataset that has been proposed in the legislation or in the draft bill is workable.

Mr Epstein: Yes.
Senator FAWCETT: I am assuming that is a statement made on the basis of your participation in the technical working group. We have had a lot of comment from people saying that nobody knows what really needs to be collected, because it has not been defined, only outlined. From a telco provider who has been involved in the technical working group, can I take it from your comment that you have sufficient understanding of what will be covered by that outline, that you know what is going to be included and that you think it is workable?

Mr Epstein: To some degree it is always going to be speculative—what is likely to be covered if the regime were to proceed along the lines discussed with us. Clearly, I think the point has been made by others that there is not an extant draft regulation that has been circulated, but in effect we have had fairly detailed discussions and they have gone directly to a consistent set of points, and you would assume that those consistent set of points would form the basis of regulations. And, yes, they are a bit better than in the broad workable; they appear quite workable. There are obviously points which we have noted in our submission where we think a little bit more granularity would be in order. For example, a more detailed definition of precisely what is an internet session would be one thing—going beyond the definition and ensuring that we had better mechanisms in terms of retention implementation plans and the arrangements around that to ensure that there was some certainty about the application of those, both in terms of how understandable they are and the period of time that they would operate. We would obviously like to have some confidence that decision making would be timely and efficient.

We do have some views about the capacity of a minister or a communications access coordinator to provide own-volition exemptions for classes of service, where necessarily the embrace might be out there in the proposed dataset, but in reality the threat assessment might be that it is not necessarily required given the total volume. I will not speculate about this in public hearings, but what I would say in the broad is there might be certain types of services—for example, entertainment services—that do not appear to be communications, how we commonly understand it, whether it be emails or voice communications between people that might necessarily facilitate the interaction between a service provider and their customer. They are literally someone turning a service on or off. But it may well be that someone develops a means of using that as coding or whatever, in which case normally you might expect that after a settling-down regime, unless a particular threat or behaviour is identified, you get a class exemption. So we would like to see not necessarily better definition of those types of services but good definition of an exemption regime that could enable a discussion about that. I cannot see why it could not be in an instrument that can be subject to some external scrutiny anyway.

Senator FAWCETT: To that last point, as your technology evolves and you wish to change your business practices to reflect the evolving technology, is definition by regulation good for you in terms of business practice?

Mr Epstein: There is always a bit of tension on this, because to what degree is a regulation accountable to the parliament or, indeed, to the wider community? But, yes, that is the practical way through. We face it all the time across all facets of our industry, whether it be competition or regulation—this sort of area—because you just never know where the technology is going to go and how it is going to be applied. So, wherever possible, we advocate instruments that are outcomes focused rather than process or technology focused.

Mr CLARE: Mr Epstein, thanks for Optus's submission. It is very comprehensive and includes a number of recommendations for the committee to consider, but it is also, I would have thought, quite important for the Attorney-General's Department to consider, given that you have made some quite specific recommendations about changes that might be made to the bill and to the draft dataset. I just wanted to see if I could get some clarification about whether Optus is in discussion with the department about some of those recommendations and getting feedback from the department about whether they agree with Optus in that respect.

Mr Epstein: I think—and Mike might also like to comment here—we have found the willingness to engage on the working group to be genuine. I suspect there are differences of opinion, and there may well be differences of opinion within the bureaucracy as a whole. The classic example would be how you treat costs, for example. We have a couple of former attorneys-general here who might be able to bear me out, but historically or culturally the Attorney-General's Department takes what we would describe as a fairly narrow perspective on what you would call social licence costs. Being an agency that probably does not enjoy a huge amount of funding in comparison to some of its counterparts within the Commonwealth, it has a natural inclination to say that stakeholders should bear the costs of enforcement services et cetera. So we will have differences on that but, in terms of some of the technical things that you have seen in our submissions, it has been a fairly cooperative and collaborative discussion. In fact, what I have said about our relative comfort with our understanding of what a dataset might look like results from that sort of discussion. Would that be fair to say?

Mr Elsegood: Yes.

Mr CLARE: Is that discussion still ongoing with the internal working group? My understanding was that they are now focused very much on defining the costs, but is that group still looking at some of the recommendations
you have made here about elements of the bill and the dataset, or is that a separate discussion directly with the department?

**Mr Epstein:** That tends to form the bulk of our discussions with the Commonwealth. Obviously we have all had contributions to make about the principle of cost allocation, and that is clearly why the PwC exercise is underway, but there is only so much you can say about those points. They are relatively simple points to make, and most people's positions are well known. We have to settle what the agreed principles might be and then how you might apply them if you had to proceed with a regime. So what we have really been focusing on is what is in and out, potentially, what the definitions are and how to make the definitions more workable et cetera.

**Mr CLARE:** And you have found the government open to that discussion?

**Mr Epstein:** Yes, discussions at the official level—

**Mr CLARE:** I might pursue that.

**Mr Epstein:** about being a professional.

**Mr CLARE:** Do you have a feel for when a draft regulation might be available for industry and the general public to look at?

**Mr Epstein:** Obviously, we have sought that. I think that is entirely a matter for the department and the minister. Clearly, we would like to see things sooner rather than later, but I suspect it is to some degree tied up with the deliberations of this committee.

**Mr CLARE:** And this committee are concerned about it, or I am, because we are being asked to report by the end of February, with the potential for the parliament to vote on legislation in March. Obviously, if it is in regulation, that is separate from the legislation, but it would be helpful for this committee to see that regulation before it has to report.

**Mr Epstein:** I think the shape of anything assists all parties who might be involved in this.

**Mr CLARE:** You have not been given any advice from the government, or from the Attorney-General's Department more specifically, about when that regulation might be available?

**Mr Epstein:** I have not most recently, no. Certainly, the main indication we have received from people is that they are very mindful of the fact that there is a keen desire to see something like this.

**Mr CLARE:** Okay. Turning to the issue of costs, do have a feel for how long it will take for Optus to have a more precise understanding of how much this will cost your business?

**Mr Epstein:** When a bill passes entirely through the parliament and is enacted.

**Mr CLARE:** And when the regulation is made, I guess.

**Mr Epstein:** Yes. For example, the deliberations of this committee might affect the requirements. When those sorts of things are more settled—that is the reality of this. It might be an unfortunate reality but it is the reality.

**Mr CLARE:** So we need to see the regulation as well as the legislation.

**Mr Epstein:** That would clearly be ideal, but settled law is ultimately the arbiter.

**Mr CLARE:** So it may be a period of three, six or 12 months before we know for certain exactly how much this will cost?

**Mr Epstein:** That depends on your processes and the government's processes, but that is entirely possible. As I have said, it could be a period of two years before things are finally settled. We have current systems, as indeed do other participants in the industry. It is not a static industry. It is an industry that is undergoing considerable technological change, moving to what I would call increasingly softer networks, which is a greater integration of our software and IT systems with our hard or physical infrastructure, or indeed, in some cases, the replacement of hard or physical infrastructure with software. As a result of that, the major carriers are moving to new operational systems. But on the way through, while we are implementing those changes within our business—and the same would apply to the other major carriers—if we are faced with a compliance regime, we would have to make provision for applying what we need to apply to legacy systems, such as sunset clauses, and ask: does that require exemptions or is it something that we cannot exempt because it is so critical to the successful operation of a regime? There are a number of variables and they shift as time goes on.

**Mr CLARE:** Mr Elsegood, you had something to add?

**Mr Elsegood:** Yes. There are a number of specialised business services that we supply to enterprise and government. We would hope that they would be exempt from the regime—some in full, some in part. Our historical experience has been that the agencies do not have a large interest in services that we supply to business.
Some of our costing is really dependent on those exemptions being in place, so that is another component of being able to come to a total figure for what this is going to cost.

Mr Epstein: Yes. On that point, I think there is a pretty mature understanding of that within agencies that are used to working with us. What Mr Elsegood is essentially getting at is that some of the larger enterprises and government services are technically carriage services but they are very much closed systems. Where what is being moved around is within a closed system, it does not necessarily affect people whose behaviour or activities you do not have other means of observing.

Mr CLARE: And whether that is in or out will have a significant impact on this—

Mr Epstein: It could potentially do so, but, as I said, I think there is a pretty mature and, indeed, longstanding understanding of how these things operate. Mr Elsegood has made the point that the calls on this are relatively small. One would have thought as a matter of common sense that you would not have a regime that excises them at the legislative level, but it might be classically an area where you might apply an exemption for practical purposes at the regulatory level.

Mr CLARE: On the issue not of cost but of the percentage of the cost of this scheme that you might be reimbursed for, has Optus had any discussions with PwC or with the government, particularly the Attorney-General's Department, about what that percentage might be? The reason I ask that question is that Minister Turnbull, when he introduced the bill, made the commitment to a 'substantial' contribution towards those costs, but the internal working group's first report, released in December last year, talks about a 'reasonable' contribution to those costs. I am concerned about whether substantial and reasonable are one and the same thing.

Mr Epstein: It is always a matter of concern, as you might imagine, and that is the horns of our dilemma. In terms of fixed percentages, no, we have not had discussions of fixed percentages and, quite frankly, I do not see a lot of merit in talking about fixed percentages unless we came to a point where views about the principles for reimbursement were close to irreconcilable and you just decided to split the difference. It goes to the point I was making before. Unfortunately, you find yourself in a situation where probably the most sensible way forward is a discretionary way forward, because sometimes there will be capability where the incremental cost of applying it or turning it on is minimal. Sometimes it will be quite substantial and require modifications, which cannot be amortised readily and cannot be amortised across other commercial functions that we might use equipment for because it is purely to do with an interception or law enforcement regime.

Mr CLARE: Does that potentially mean that the way in which ISPs are compensated could vary from one company to another?

Mr Epstein: I think it does, and for such a regime to work properly—and I think this is the whole intent of it—we need to get to a common level of data retention across all relevant service providers. You will have heard evidence already, and it is very apparent from some of the representations you will have heard from our industry group, the comms alliance, that there is a great deal of variation in capability, in capital capability and, indeed, in call. There are hundreds, I think over 600, service providers in Australia at the moment. Some of them are quite small outfits who may not have the capability themselves. A lot of these outfits are, of course, drawing wholesale services from some of us major providers. For some of our major wholesale customers, for example, if they have an interception capability plan, it is essentially our interception capability plan, which we are running for them on a wholesale basis. I cannot see why that sort of thing could not be accommodated in this regime when you are negotiating plans with individual providers, which might obviate the need for a standard set of expenditure or hardware or software requirements.

So, accordingly, it is likely to vary. Some people may want to go down one path; others might want to go down another. What I can tell you is that, as occurs today, the vast bulk of the burden will fall to the three largest carriers, in particular the two largest carriers.

Mr CLARE: Can I ask you about PwC. How expert have they been in their capacity to conduct this work?

Mr Epstein: They are a reputable accounting firm who know how costs are apportioned et cetera. Where they would clearly lack familiarity is precisely the sorts of equipment processes sources that might be needed here. That is obviously where they ask us questions because we can inform them with answers. And then we have the third dynamic, which we have been over at great length, which is precisely what are we asking of each other.

Mr CLARE: Let me go to the issue of certainty. This is an issue which Optus has expressed concern about and Telstra in its evidence yesterday also talked about it. Obviously the greater certainty about what the data set is and the less likelihood of it changing from time to time in an ad hoc way the better for your business because of fewer costs potentially involved in adjusting to changes to the regime. One of the ideas which has been presented to this committee is that the dataset, rather than being placed in regulation should be placed in legislation or at
least the primary principles with a regulation-making power. In your submission, you suggest something else which is that that dataset in regulation should be fixed for a period of time until after the three-year review which would in effect be for five years because there is a two-year implementation period and then a three-year period before a review. So you would be setting that datadec for five years. My question to you is: appreciating the importance of certainty, would the recommendation you have proposed be too restrictive and are there arguments that, instead of a model like that, it be better to do what others have suggested which is to place the principles in legislation with a limited regulation-making power?

Mr Epstein: I think it is a balance of utility. I think our preference would be a third alternative which would be a greater reliance on perhaps disallowable instruments, so not quite going all the way down the path I think you are suggesting in terms of having more in the legislation but ensuring that perhaps more in disallowable instruments the parliament did have some oversight, so there was the capacity to move faster than perhaps legislative change might occur and in a more precise way that the changes in legislation might—

Mr CLARE: And that is what the government is proposing now.

Mr Epstein: Yes.

Mr CLARE: But in your recommendations, you say that once that regulation is made it is set in stone for five years.

Mr Epstein: We did not precisely say five. That is your interpretation. It may or may not pan out that way. I would not necessarily assume that that is a fait accompli but we certainly say initially that a two-year regime would be preferable, a settling down period, and that might assist in terms of working out the practicalities of the operation of the proposed act.

Mr CLARE: I appreciate the point you are making, which is that industry needs certainty. I guess the question this committee is asking itself is: how do you provide that important and legitimate amount of certainty while also giving law enforcement in flexibility so that, if need be—

Mr Epstein: I understand that. As I said, it is a balance of utilities and how you achieve that, whether it is disallowable instruments that go on ad infinitum under a piece of legislation which is intended to be quite long term, whether it is a sunset clause in legislation—there are varying ways these things can be achieved and indeed have been achieved.

Mr CLARE: Optus has provided the committee with some information which I think is commercial-in-confidence about the proportion of requests by law enforcement agencies which are less than three months, six months, nine months, 12 months and beyond.

Mr Epstein: Yes.

Mr CLARE: Is there anything Optus would be prepared to put on the public record in relation to that, noting that yesterday Vodafone explained the information it had provided on the public record?

Mr Epstein: I would prefer not to go to the detailed elements of the information we have provided so far. I think to some degree Vodafone are in a different circumstance to us in that they have a less complicated service offering. And they are dealing with less volume. So in essence it is easier for them to answer the question publicly and offer a bit of commentary. The one thing I would say is to exercise some caution in drawing immediate conclusions about where the volume of requests lies in terms of the age of the information, because I think you always have to apply a matrix about the seriousness of the request and preservation regimes which might operate in tandem.

And indeed there is probably a filter that might be applied as this legislation is proposed if the government proposes limiting the range of entities that have access. For example, when I was a resident of Melbourne it always used to fascinate me the technologies that the City of Port Phillip used to apply to dog excrement—including all sorts of pathological techniques.

CHAIR: You didn't carry a bag with you, did you?

Mr Epstein: I certainly did. I lived in fear of the City of Port Phillip. So I think those sorts of things might affect the character of the regime. I really would caution against—I would not accuse you of being simplistic—applying that prism when you are looking at things.

Mr CLARE: We are certainly not, but we are keen to drill into it and understand the data a little bit more.

Mr Epstein: There is one other thing that perhaps I would say. This is particularly Optus specific, and it is not necessarily drawn out in the table that we have provided to the committee in confidence, but it is worth noting. We have a large, prepaid mobile base of customers and, indeed, are suppliers to resellers, who also do that. And there are a number of reasons why people might prefer prepaid phones. The turnover of prepaid accounts can
sometimes be greater. That does tend to explain a little bit why there is disproportionate interest in that particular cohort of customers. I think that does influence some of the timing and the age of the data that has been looked at to date.

**Mr CLARE:** In the data that Vodaphone gave us yesterday they said that that was telephony only. You may not know the answer to this question at present; perhaps you could take it on notice. I am just keen to understand if the data that has been provided by Optus to the committee in relation to time periods is telephony only or telephony and IP.

**Mr Elsegood:** It will include both telephony and IP. We do have capability across our fixed access to provide those IP addresses, if we are requested, and also across our mobile network, albeit for a much shorter period of time.

**Mr CLARE:** The reason I ask is that there was a sort of suggestion in the evidence that Vodaphone gave yesterday that the type of information that is sought by law enforcement agencies, or is relevant to law enforcement agencies, varies based on whether it is telephony or IP. Without verbalising them, the impression I got was that because IP addresses can be dynamic often the information that police or law enforcement and national security agencies are seeking tends to be not as old as telephony requests. So, if the data that you have provided to committee is both, do you have the capacity to break down the data you have provided so that we can see whether that is true or not?

**Mr Epstein:** I will take that on notice. I do not think it should be that problematic, should it?

**Mr Elsegood:** I really do not know. It is a question that we would have to take on notice.

**Mr Epstein:** It is just how our people keep the relevant stats. I had a look at the Vodaphone evidence. I think that was the point they were trying to make.

**Mr CLARE:** If possible, that would be helpful.

**Mr Epstein:** It makes sense that that would have been a point. The only other comment I would make, which would probably be in service of that, is that with the larger agencies and the more experienced agencies, who obviously deal with us quite a lot, there is a clear pattern that they tailor the nature of their requests because they know what we are capable of and what our customer base is. So, just to save time, that is how they do it.

**Mr CLARE:** And they know your business practices as well, so they know what they are going to get.

**Mr Epstein:** Correct. For example, I would assume one of the reasons why they are asking for a consistent set is that they are entirely aware that in the mobiles area increasingly, with the nature of the systems that are sold by our suppliers, you cannot necessarily assume that you would retain data for the length of period that we traditionally maintain it for more traditional services.

**Mr CLARE:** One of the concerns that the government has raised is of agencies going dark and a fear that, over the course of the next few years, data which is presently available on request by law enforcement agencies to organisations like your own may not be available in the future because of changes to business practices.

**Mr Epstein:** Yes.

**Mr CLARE:** My colleague Mr Dreyfus asked a question of Telstra and of Vodafone yesterday as to whether they had any intention of changing their current storage and business practices in relation to this data in the future, to which they said no. I am interested in whether Optus has any intention of changing its storage practices.

**Mr Epstein:** We certainly have no intention. I think the main influence on change and the overall character of the dataset, if you were look at it in the very broad, is that increasingly communications are moving to mobile services and increasingly—even with what we would regard as voice communications between ourselves—they are in effect data, and that has an influence on how data is kept. Depending on the supplier that we choose to buy equipment or processors from, it can have an influence on how long it is kept, and then you have complications in datasets: you can have dynamic addressing, for example.

**Mr RUDDOCK:** I cannot let that go in isolation. It is also a question as to whether or not your customers, because of the way in which you keep their data and their concern potentially to conceal information about their usage, move to other suppliers. That must be a factor.

**Mr Epstein:** Absolutely it has to be a factor, and that is presumably why this regime is about bringing everyone to a common set of standards. At the moment, probably the vast bulk of communications pass through the three major carriers in some form or another by means that are captured relatively well for the purposes of a regime like the one that we are discussing, but increasingly there is the potential for that to fragment. Indeed, people are always on the lookout for something. You will have seen media reports, for example, that drug syndicates and bikie gangs absolutely love BlackBerry phones from overseas carriers. There was a reason for that.
Whether they can feel entirely confident of what they are up to is another thing, but they have clearly tried it on because they are of the belief that they can evade the protections that apply or the enforcement regime that applies in Australia through mainstream services. So this sort of thing will always be about. It is also another reason why we are a bit reluctant to discuss the details publicly, because I guess it acts like a red flag.

CHAIR: And understandably so.

Mr CLARE: It helps us to understand that the concern presented to the committee by the law enforcement agencies relates not to changes by Telstra, Optus or Vodafone, the major providers, but potentially to another, smaller part of the market.

Mr Epstein: I think it is a combination of a smaller part of the market, fragmentation of the market, technological alternatives and a broader change to what I would call crudely a data based regime for communications, rather than necessarily a traditional PSTN type voice regime.

Mr CLARE: I have one final question on the issue of cost and security. This committee in 2013 recommended that, in order to ensure that there was proper security, the encryption of that data be made mandatory. This is not taken up in the bill before the parliament. But, given the importance of making sure that this data is secure—and, again, I make note of the point made by Telstra yesterday that this is potentially a pot of gold and we need to make sure that it is held securely—do you have a view about whether the recommendation of this committee previously is a worthwhile one? And what would be the implications in terms of the cost model?

Mr Epstein: I could not give you a costing off the top of my head, but I think it is worthwhile and imminently conceivable. Clearly you would look at all the security and preventive regimes—encryption is one of them, and segregating data. As I said earlier, having a relatively limited, well-defined dataset as opposed to our entire internal commercial dataset—which, if I was to use an analogy, is like a floating fish tank; there are all sorts of sub-elements of data that associate themselves with one another—just makes that task a lot easier. Mr Burgess from Telstra did say that yes, there will be a—I think the word he used was 'honeypot'. Clearly just the existence of a database will attract people's interest. But if it is a well-defined database and it is not the entire set of data or processes that we maintain, it should be a relatively straightforward task to segregate it for security purposes, and possibly encrypt it, if need be. It is a sensible thing to have things like electronic sand traps—all the access protocols that we apply to the most sensitive information already.

Mr DREYFUS: Mr Epstein, thank you very much for sharing your experience and Optus's expertise with the committee. Just to start off with, Optus, like all other carriers, keeps data for business purposes now. And, as Mr Clare has just taken you through, like Telstra and Vodafone, Optus has no current plans to lessen the amount of data that it is currently keeping.

Mr Epstein: Yes, I think that is a fair statement.

Mr DREYFUS: And it is significant, because it has been suggested that there is a deathly urgency about this legislation. And I am just trying to test that urgency. You have accepted the need for a mandatory data retention scheme and have worked very cooperatively with the Attorney-General's Department in devising what presently is a draft dataset. You have provided us, in fact, with some comments about the draft dataset, although you say that the regulations are not available yet and should be. It is the case also that under the scheme in this bill Optus is being given up to two years to comply, from the date that the bill becomes law. Is that right?

Mr Epstein: Well, that is effectively what it looks like, yes.

Mr DREYFUS: Would it be better, given the additional regulatory burden that we are talking about with this scheme, that the government and the parliament do everything possible to get the detail right before the scheme commences?

Mr Epstein: Well, as I have said, I think the task will be assisted by detail, and presumably that is what you are embarked on discussing here now, and deliberating on, as indeed the government is.

Mr DREYFUS: You have spoken about the need for certainty from Optus's point of view. It is the case that Optus and Telstra have participated in the working group organised by the Attorney-General's Department, but the great majority of the other approximately 600 service providers have not directly participated in the working group, although their trade association has.

Mr Epstein: I do not think that is strictly correct.

Mr DREYFUS: I am just trying to—

Mr Epstein: I will give you the answer. For the main working group, yes, Comms Alliance has been represented by Mr John Stanton. Suffice to say that the reason why Comms Alliance was there was so that it was not just the major carriers. If anyone knows Mr Stanton, they would expect that he was vigorous. For those who
do not, I can assure you that he is always a very vigorous advocate and, more to the point, I think he came with a quite deliberate and proper bias of representing the concerns of minor carriers. That is point No. 1. Point No. 2—and indeed we have been privy to this—is that he has had a very large working group involving what, I think, is a very representative sample of his membership, including the most vocal members and those most opposed, who have contributed to the comms alliance submission. Then there has been, in effect, an operational working group working under the main working group where comms alliance brought along representatives of some of those people who are not directly represented on the working group proper. Mike, I think you can confirm that.

Mr Elsegood: Yes, there were a couple of people.

Mr Epstein: Mike has clearly been present at some of those discussions. I do not know what other discussions have occurred with the Attorney-General's Department and some of those other carriers. But all I would say is that some of the smaller voices have been very apparent. Just because they are smaller does not necessarily mean they have not been loud.

Mr Byrne: From what you are saying it sounds as though it has been a pretty rigorous process?

Mr Epstein: I think it has been a thorough process, yes.

Mr Dreyfus: It is a process, though, that did not start until after the government announced the legislation on 30 October 2014.

Mr Epstein: That is correct.

Mr Dreyfus: As we understand the position—and the Attorney-General's Department gave a little evidence before us in December—the government did not do anything about this between the publication of this committee's report, in June 2013, and towards the end of 2014.

Mr Epstein: This is clearly a process, like your own process, that has begun in earnest once legislation has been very directly contemplated. Otherwise, what tends to occur is that there is a fairly regular dialogue not only industry as a whole but certainly between the carriers and a range of government agencies, both policy agencies and operational agencies.

Mr Dreyfus: Just while I am on the committee's report, the 2013 report of this committee made a number of recommendations for reforms of the Telecommunications (Interception and Access) Act, which of course is sorely in need of updating. They have not yet been proceeded with, have they?

Mr Epstein: No.

Mr Dreyfus: Another set of reforms was recommended by this committee, in 2013, to the telecommunications sector security reforms, the TSSR. They have also not yet been proceeded with?

Mr Epstein: No. They have clearly been the subject of ongoing discussion under governments of various persuasions over the last decade.

Mr Dreyfus: Back to the other telcos, as you say, Mr Stanton has represented them as the formal representative of the Comms Alliance in the working group process. Those 600-odd other service providers also need certainty in respect of this quite substantial regulatory burden that they are going to face?

Mr Epstein: I think everyone needs certainty. Certainty is always a good thing.

Mr Dreyfus: I am not sure whether I have the time to go into the detail I would like, but your submission is comprehensive. You have made a number of very detailed recommendations regarding amendment to the bill. Mr Clare touched on this. But looking at page 3 of your submission, paragraph 1.8—which is our page 9—I see that you would like the dataset to be not changed for a certain period. I need to point out to you that the 2013 report of the committee recommended that there be a review by this committee three years after the commencement of this legislation, if it were to come in.

Mr Epstein: Yes, I am familiar with that.

Mr Dreyfus: The bill, on the face of it, provides for a review by this committee five years, in effect, after the commencement of this legislation, because the government has opted not to accept the committee's 2013 recommendation and, rather, is providing for a review two years after the end of the two-year implementation period. Because of that difference, I am just checking: what period is Optus suggesting is an appropriate period for the dataset to be kept fixed?

Mr Epstein: I think we could live with either regime that you are canvassing in terms of our bottom line. On the practical application, we have clearly—

Mr Dreyfus: The reason I ask is that the committee might think, as it thought in 2013, that three years is the appropriate period, and I am checking if you are asking for it to be fixed for three years or for five?
Mr Epstein: I will get back to what I was trying to say.

Mr DREYFUS: Sorry.

Mr Epstein: In terms of the practical application, I think a minimum two-year period would be sensible. If it were a longer period, that would clearly be of benefit to us, but we are not the only stakeholders, and the others might have other views about the utility and the practicality of that.

Mr DREYFUS: As you have said at the foot of page 4 of your submission, you are going to be required by this legislation to put in place a new set of arrangements—in other words, build new systems to capture data that you do not presently capture or capture data in different ways from the way you capture it.

Mr Epstein: Correct.

Mr DREYFUS: That is the reason for wanting certainty for a period?

Mr Epstein: That is primarily the reason. For the sorts of systems that industry is currently implementing and, certainly, what we are contemplating implementing, these will be multiyear tasks with capital requirements—our own capital requirements; this is nothing to do with the regime—that go into the hundreds of millions of dollars, sometimes into the billions, and with large capital projects of that type you would hope to have some certainty or at least predictability.

Mr DREYFUS: Now, I do not want you to take me as having ignored your recommendations, Mr Epstein—

Mr Epstein: No, that is all right.

Mr DREYFUS: the committee finds very helpful these detailed recommendations that you have made. If I can go first to page 8, paragraph 3.11, you are looking for the draft of the proposed regulation—in other words, the final version of the dataset—to be available to assist both this committee and the parliament.

Mr Epstein: Yes.

Mr DREYFUS: Next in your submission, starting at paragraph 3.12, you have made a pretty detailed suggestion. I do think there is any way to deal with it other than grappling with the density of it—

Mr Epstein: That is all right. I might require Mr Elsegood's assistance here, but we will see how we go.

Mr DREYFUS: which is grappling with the problem of incoming internet communications. You make the point at paragraph 3.14 that there is an attempt made in clause 187A(4)(b)—it should be (b)(i)—in relation to the supposed exclusion of 'an address to which a communication was sent on the internet' and so on. I wonder if you or Mr Elsegood could explain, as best you are able, why you have made the recommendation in paragraph 3.18 about the need for greater certainty about 'the policy intent that service providers are not required to keep information about a subscriber's web-browsing history' because, on the face of it, the exclusion does not go far enough. If Mr Epstein is not volunteering, it must be you, Mr Elsegood.

Mr Elsegood: If I could make an attempt at explaining that to you. In the discussions I have had with the Attorney-General's Department on the detail of this, they have indicated that it is not their intention that the detailed incoming packet addresses that are going to a particular customer are captured as part of this regime, but it seems to me that it is open for the regulations to require that in the future. I think for certainty it would be better to have some explicit mention of that in the legislation—that the intent is not to capture the packet addresses that are incoming to a particular customer that tell you where those packets came from. If you look at it in the sense—

Mr DREYFUS: It is because of the fact that examination of web-browsing packets that come from the other end of the communication could enable the web-browsing history of a customer to be reconstructed? Is that the concern you are trying to deal with here?

Mr Elsegood: Yes.

Mr DREYFUS: And you have suggested a quite detailed test—your amendment to 187A(4)(b)—that, to your mind, would take care of that?

Mr Elsegood: Yes.

Mr DREYFUS: That is to try to put beyond doubt that the web-browsing history is not required to be captured and nor, incidentally, should other information be kept that would enable reconstruction of a web-browsing history.

Mr Epstein: The other thing that we have put—not formally in our submission, but certainly in discussion—is that that might be assisted if it were buttressed by remarks in an explanatory memorandum, if there were to be a revised bill, for example.

CHAIR: Do you know whether that view is also supported by other telecommunications carriers?
Mr Elsegood: We have not had a discussion with other carriers about this particular point.

Mr Epstein: Certainly when I have been in discussion and others have been there, no-one has disagreed. But I would not describe it as much more than a nodding of heads.

Mr DREYFUS: I am very conscious of the time, so I am going to go as quickly as I can. Your next recommendation related to paragraph 187(A)(7), which uses the phrase 'single communications session'. You have suggested that there is a potential ambiguity in the term 'session' and made a suggestion as to the need for clarification of that drafting to avoid the ambiguity.

Mr Epstein: Yes.

Mr DREYFUS: Have you got a proposed redraft of the provision?

Mr Epstein: No.

Mr DREYFUS: It is a matter for parliamentary counsel to fix, but—

Mr Epstein: It is an easy problem to identify but it is something that will require a lot of discussion around what a session actually is. What we have put in our submission goes to what is probably a rapid sequential series of calls which might form part of a conversation—even something that results from people dropping calls or interrupting a conversation, turning off a mobile phone or whatever, to something that might be more extensive and complicated, in that, as a result of dynamic addressing, the addressing might actually shift within what is effectively one session.

Mr Elsegood: There is also change in service because of the way the internet is working, because of the way that apps are being used over the top of the internet. Today a telephone conversation still looks very much like a telephone conversation that has been happening over the history of the industry, but there are multimedia sessions or multimedia communications which are emerging where people can swap from video to text to voice communications. These are used in educational circumstances now but could be used more broadly by a community. The question in those sorts of circumstances is: if it is just using voice, is it a telephone call or is it just part of an internet session? That is where, in the future the definition of 'session' is important so that you can build systems with confidence that you are complying with the legislation.

Mr Epstein: And, indeed, it can vary from app to app and provider to provider. To give you an analogy from gaming apps, for example—if we step outside the conversation—there are some that people have on their phones that are constantly interacting but they are interacting in one unbroken communications channel. There are others where there are multiple channels turning on and off, which absolutely drives us nuts as carriage service providers because they chew up huge amounts of network capacity, but it is a very good illustration of the differing types of things that might amount to a session. You and I might think that we are communicating on an over-the-top app and it is one single event, but for technological purposes it might be via multiple routes.

Mr DREYFUS: To finish up on that, because I did not want to discuss the actual drafting—it should not be beyond the wit of parliamentary counsel to come up with something—I see from your submission that that has been discussed at the Data Retention Implementation Working Group, which you have been participating in.

Mr Epstein: It has been, probably more so in the group that Mr Elsegood has been involved in.

Mr Elsegood: Yes, but there has been no suggestion of how the definition could be improved.

Mr Epstein: But it is certainly understood.

Mr DREYFUS: The next matter you raise concern about is, as you put it at 3.31, that the bill does not have a mechanism for the time period—that is the two-year time period provided in the bill—to be varied. I want to test that a little. Your proposition is that there should be the possibility for lesser time periods to be prescribed by regulations. Would you explain as briefly as possible what kinds of circumstances that might arise in.

Mr Epstein: Probably the least sensitive area might be on-demand IPTV and what goes behind transmitting how and when you want to, say, time-shift a program or you might want to interact with a program. There are even concepts these days where you can choose the plot line of a program.

Mr DREYFUS: Happy ending or sad ending.

Mr Epstein: Happy ending or sad ending—is that a significant communication for what we need or what people claim they need? Probably not, but would you necessarily want to exclude it from legislation? It might be prudent not to because someone might find a means of communicating by happy and sad endings—hopefully not too many sad endings.

CHAIR: But it is a tiny bit more complex than that, isn't it—

Mr Epstein: Absolutely.
CHAIR: because some carriers might think it is a lot easier just to set up for two years and know that that is uniform compared to others whose systems might allow more flexibility in these types of things.

Mr Epstein: Correct, and that is why I deliberately chose what is probably a more trivial example.

Mr DREYFUS: What you are putting is that, regarding the process that is already provided for the Communications Access Coordinator, a new official that is created by this bill, to vary or exempt a requirement in respect of a particular provider, you are looking for something more general than that—that there be the possibility of a regulatory flexibility or a regulatory lessening of the period across the board for particular classes of warrant.

Mr Epstein: Correct—an element of practicality.

Mr DREYFUS: At 3.38, you have made another suggestion. I am really not going to spend time on this and I will try to summarise it. You have suggested that the Communications Access Coordinator—that is this new official being invented here—should be able to have a certain power in relation to deeming equivalent compliance by providers. At 3.42, you recommend a similar change for deeming compliance. Again, they are drafting matters that can be picked up.

Mr Epstein: Yes.

Mr DREYFUS: But in essence what you are asking for—and it is in the box there at 3.45—is some greater flexibility that allows for ease of compliance. I am not suggesting Optus or any of the other providers want to evade or avoid compliance. You are simply wanting to make it more practical in a regulatory sense.

Mr Epstein: Correct. You would crudely describe it as offering the possibility of a grace period, if required. I think for the smaller carriers and service providers we were discussing earlier that would be of some benefit. They may choose to comply directly themselves or they might choose to comply by drawing services off their wholesale providers, if we major carriers could do it for them. But they might make a judgment that their business is going to evolve in future and they might want to develop some capability themselves. That would classically be an area, in addition to areas where there are just simple large system changes, and a balance of judgment might be made about the urgency or the utility of the information that government agencies require.

Mr DREYFUS: Going to your suggestion in 3.50, which you have explained, is that just to give more regulatory certainty to the 600-odd providers by putting in some time limits or times for steps and review steps not just by the new regulator here, the Communications Access Coordinator, but also by ACMA, which, according to this bill, will continue to be involved?

Mr Epstein: Yes.

Mr DREYFUS: I am just trying to get to the type of change that you are suggesting here, and its purpose, because we have the detail in your written submission. If I could take you to paragraph 3.71 and paragraph 3.74, they, too, are suggestions for drafting changes that make the new regulatory regime that is being imposed here more workable.

Mr Epstein: Correct. They are also consistent with suggestions we have previously made before in response to the government's red tape reduction policies. For example, in the case of ACMA records they may well remove the ambiguity that has become apparent in evidence to this committee about the number of requests being recorded.

Mr DREYFUS: That is right. We had evidence yesterday as to why it is that there is a discrepancy by some hundreds of thousands between the ACMA reporting and the parliamentary report.

Mr Epstein: We have long argued that. If these statistics are collected in a robust way by other means, what is the utility of ACMA collecting them?

CHAIR: So you would agree entirely with the evidence we received yesterday?

Mr Epstein: Yes.

Mr DREYFUS: In 3.84 that is precisely the matter that the reporting consolidation into one reporting obligation goes to.

Mr Epstein: Correct.

Mr DREYFUS: You have some detailed submissions at the end of the submission about costs, but Mr Clare has asked you adequate questions about that. Section 4, which is at our page 24 and your page 18, contains some detailed suggestions. This is no criticism of Optus here, but doing the best you can with the current state of drafting the government has reached with the data set—and that is as much as you know—you have made some very direct suggestions about some of the items, the first one being the 'data volume usage parameter' and the
need to ensure that it is consistent with the allowable kinds of information that are set out in the bill. Are you, and perhaps Mr Elsegood as well, able to speak to that?

**Mr Epstein:** That is an ideal question for Mr Elsegood.

**Mr Elsegood:** The agencies have expressed the view in the working group that this was a piece of information that they would find useful, and there is no debate with that. It has been included in the draft data set in the report from the working group. So this is something that was added in through that process. But in reading through the bill, it is not apparent that that particular item is covered by the specific items that are in the bill at the moment. So, for consistency, I think that what is in the regulation needs to be covered by the bill.

**Mr Dreyfus:** Then, on the following page—your page 19 and our page 25—you have three more suggestions about the specifications in the data set. The first one reads:

Optus recommends that the Committee find that further consideration is required of parameter 1 of the draft data set to remove potential replication of records and to make it clear that the data retention regime does not require retention of customer passwords.

In your view, is the current drafted data set something that could potentially be seemed to require retention of customer passwords?

**Mr Epstein:** It does not directly exclude it, so there always is that risk. Aside from complicating the data storage task and probably complicating the public policy considerations that you might bring to bear—because clearly there will be people with views about passwords—what I would say is that it does have the potential to, at least at the margins, increase the risk of penetration of a database, because clearly people can get at the passwords as well as at the primary data, and they can use passwords for all sorts of things. That would clearly be attractive to badly motivated parties and people. One would prefer not to have it, but, regardless of that, it just simplifies the task quite frankly.

**Mr Dreyfus:** The last two, despite the brevity of this passage in your submission, strike me as concealing incredible complexity. They both in a sense go to similar points, which is the degree to which a service provider has visibility of information. The first suggestion you make is that the obligations to keep:

... be adjusted to only require collection of information relating to events that the access service provider can reasonably control, rather than elements which are more directly related to actions that end users take and which providers have no easy method of determining at all, or only via detailed packet inspection of the content of a communication.

Are you able to speak to that to explain what the problem is that you are dealing with there?

**Mr Elsegood:** As an example, we supply some business services that use voice over IP as the telephony component. That in the main is provided over the broadband service we supply to the customer. But it does have the ability for remote access and login. It means that the customer could go to an airport lounge and log in there and use their telephony service. But we cannot determine that location in that particular circumstance.

**Mr Epstein:** It is inside their walled data, so to speak.

**Mr Dreyfus:** The last point goes to a similar question of the location of information. I would like to ask a precursor question to this. In the bill, at 187A(4)(e), there is an apparent exclusion of this kind of information. It is described as:

(e) information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected.

From other evidence we have been given, my understanding is that that relates to a device sending a signal to a tower, not in connection with the making of a call or the carrying out of any operation, but simply checking in or pinging its location. Is that also your understanding of that exclusion?

**Mr Epstein:** That is my understanding, crudely, but Mike has more detail. I understand it is purely about pinging a tower. Whether it is the device itself, or whether someone is running other apps that might be background refreshing or whatever, that perform functions that it is not the intention of this bill to look behind, but that require the device to communicate a location or destination.

**Mr Dreyfus:** Are you able to cast any light on how this exclusion came about. We can ask the department about this. You are not sure?

**Mr Epstein:** I would go to the department for that.

**Mr Dreyfus:** Going back to the last point you have made about the data set—page 19 of your submission and our page 25—you have suggested that:

... the data set be adjusted to reflect the fact that some service providers will have no location information available to them and that in these circumstances the obligation at section 187A(6) to 'create' such data should not apply.
As I understand it what you are getting to there is that at 187A(6) there is a provision that says that, if the first part of this provision requires a service provider to keep, in relation to a communication, information that is not created by the operation of the relevant service, then the service provider is nevertheless required to use other means to create the information or a document containing the information. What is the problem there, as Optus sees it?

Mr Elsegood: Again, in those circumstances the example there is about email. If the email is being sent from a wi-fi location rather than over your particular service that it is being associated with in the first place, then you do not know that location. You cannot determine it. The combination of the provisions needs some clarity so that you are not put in a position from a compliance point of view to say that an interpretation of the legislation is that we have to have location information available, but we do not have it available to us.

Mr Epstein: An example that might be equally applicable or perhaps easier to understand is that a service provider of some type—it might not even be a registered service provider but could be an app creator—might create a form of crude voice over IP that does not apply the normal protocols that a carriage service provider or indeed one of the reputable over the top providers might include in their service, just to ensure that there is a robust service, or for other compliance reasons, or indeed customer service provisions. It might just be a very crude service that comes in, again, via wi-fi. What do you do?

Mr DREYFUS: So your concern is that neither Optus nor any of the other 600 service providers has imposed on them an obligation to do what might amount to a great deal of research and creating an entirely new system to collect data that you have no business use for, and there is some difficulty about that?

Mr Epstein: Yes.

CHAIR: To follow up on that, what is your recommendation as to how we could address that or change it?

Mr Elsegood: In broad terms, if you as a provider do not have the information available to you, you cannot create it. So if it is practically not possible for you to know the location then there should not be an obligation associated with it.

CHAIR: So it is a matter of just understanding clearly what your capabilities are and what they are not, and making sure that that is reflected either in the legislation or the draft data set, or whatever the case may be.

Mr Elsegood: Yes and I guess the conflict with that is you do not want to be creating holes in the legislation so that people can avoid their obligations. It is that clarification between having a robust set of obligations that people cannot dodge through but at the same time not creating obligations that people cannot practically comply with.

CHAIR: Thank you for giving evidence at the hearing today and thank you for your submission, too, which was very detailed and very good. You will be sent copies of the transcript of your evidence to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions the secretariat will write to you.
Evidence from Ms Ganopolsky and Mr McConnel was taken via teleconference—

CHAIR: 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 of 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. Evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr McConnel: Yes, please. The ability to enjoy the freedoms of our democracy rests on the ability of law enforcement and security agencies to protect and defend Australians and our country from threats of terrorism and serious criminal activity. While crime and threats to national security are not new, times have changed since the Telecommunications (Interception and Access) Act was introduced in 1979. Technology is different, new risks have emerged and the capabilities of those who wish harm have evolved. But care and prudence is as vital today as it was in 1979 to protect the freedoms upon which our nation is founded. This committee is well accustomed to facing the challenges of legislating in this area and is familiar with the careful task that is required, particularly that our policies and laws should be founded on sound evidence of necessity. Reasonableness and proportionality are also essential to limit the impact on freedoms to the least degree necessary.

The Law Council acknowledges that the bill seeks to pursue the legitimate objective of addressing and preventing serious crime and threats to national security and the Law Council's position is that this is a commendable objective. However, there are several elements of the proposed mandatory data retention scheme which the Law Council considers require further consideration. For example, the scheme is not sufficiently defined in the primary legislation to allow people to know the extent of the restrictions on their rights and for service providers to know their legal obligations. The nature and scope of the telecommunications data to be retained and the agencies that are to be permitted access to such data remain uncertain and are subject to change by the executive through regulation.

The Law Council also has concerns about the proportionality of the data retention regime, privacy, security of the retained data, and particularly the impact on privileged and confidential communications. As a consequence of these concerns, the Law Council has recommended in our submission to the committee that the bill not be passed and that it be withdrawn, amended and released as exposure draft legislation for public consultation. This accords with a previous recommendation of this committee that a mandatory data retention scheme, if proposed, should be released first as an exposure draft.

If this is not accepted by the committee, the Law Council encourages the committee to carefully consider how the bill may be amended to address four key issues: accessibility and legislative precision; privacy and proportionality; security of retained telecommunications data; and privileged and confidential communications.

If a mandatory data retention scheme is introduced, then the Law Council has made a number of key recommendations, which I will summarise briefly. Firstly, the dataset must be clearly defined in the primary legislation. Secondly, the agencies which can access stored communications and telecommunications data should be exhaustively listed in the primary legislation. Thirdly, access to communications data should be limited to agencies required to investigate serious indictable offences or specific threats to national security. Fourthly, access to telecommunications data should ordinarily be issued by independent tribunal warrant or, in an emergency, by a ministerial warrant. Fifthly, specific protections for privileged and confidential information should be included in the scheme—for example, where agencies seeking access must demonstrate how privileged information will be protected before a warrant is issued. Sixthly, minimum standards for protecting the security of the data are needed. The Law Council considers that a privacy impact assessment of the scheme ought to be conducted by the Office of the Australian Information Commissioner prior to the bill's enactment, and, finally,
that the data retention period should be no longer than the minimal period as demonstrated to be required by law enforcement and security agencies.

In terms of direct questions, I will just indicate that Mr Peter Leonard, as I indicated, Chair of the Business Law Section's Media and Communications Committee, will be able to answer questions directed to the dataset, who is covered and what is to be retained; and Ms Ganopolsky, who is the chair of the Privacy Law Committee, will be able to address questions relating to privacy issues, security of information to be retained, and the role of the Information Commissioner and Privacy Regulator.

CHAIR: Thank you, David Bushby.

Senator BUSHBY: Thank you, Chair, and thank you to the Law Council for assisting us today and for your comprehensive submission. I am just going to focus a few questions on your submission where it talks about the scheme's necessity not being sufficiently demonstrated. Clearly, members of the committee have had the benefit of in-depth briefings by the security and law enforcement agencies, a lot of which we cannot necessarily discuss today, but there are submissions from ASIO and from the AFP that have been submitted to the inquiry that include case studies, and some of those are redacted to some extent, but, nonetheless, others contain enough information to clearly identify the value that the metadata that was used in those cases was, in being able to identify persons of interest and being able to put together details of conspiracies; to move on—and, in some cases, with a high likelihood of having averted something that would have occurred that could have been quite disastrous or injurious to Australians, and in other cases having actually secured convictions. Have you looked through those case studies from ASIO's and AFP's submissions?

Mr McConnel: I cannot say that I personally have looked through those. I might have to defer to the other members present.

Dr Molt: We certainly looked through a number of those case studies, and they definitely have the benefit of showing why agencies such as the AFP consider the value of telecommunications data. In our submission we have made the point that there seems to be a lack of statistical data that indicates the value of such data in terms of securing criminal convictions.

Senator BUSHBY: As I intimated in my question, there are a number of benefits that flow to Australians from the investigations that our law enforcement and security agencies undertake, which include accessing metadata. I use as an example what is in an unclassified version of ASIO's submission regarding the prevention of a terrorist attack, Operation Pendennis in Melbourne and Sydney. I believe that did lead to some convictions, but not convictions for the actual conduct of the terrorist attack. Similarly, there are a number of other cases where presumably law enforcement and security agencies have access to metadata and can avert the commission of a crime, and that is not going to show up in your statistics.

I note in your submission you talk about evidence from comparable jurisdictions:

… for example in Germany, research indicates that a mandatory data retention scheme led to an increase in the number of convictions by only 0.006%;

That indicates that there were some cases, and—I do not know; I do not have the details—they may well have been ones that stopped a major terrorist attacks. The tinniness of that percentage needs to be combined with the severity of what was dealt with as a result. The proportionality often gets thrown around here. I am putting to you that statistics are not always the sole determinative factor in whether something like this is proportional in terms of balancing the need to protect Australian citizens from criminal and terrorist acts and the consequences of undertaking such a scheme as this.

Mr McConnel: Yes, I would accept that as a general proposition. Those comments are made in the context of the overall submission, which identifies particular features of the proposed scheme which the Law Council has difficulty with. If, for example, you are talking about confining the scheme to serious crime and terrorist threats, then the value of the retention of that type of data increases accordingly. If you are talking about retention of the data to make it available for the pursuit of more everyday, low-level criminal conduct—if I can describe it that way—such as Centrelink fraud, then that raises the question of the necessity of the retention of this data for the pursuit of prosecution of those sorts of offences.

Senator BUSHBY: Okay, I might deal with that in a minute. You clearly would be aware that this bill does not increase the authority of agencies to access metadata. If anything, it actually narrows the authority by limiting, to some extent, the agencies. I understand there is some uncertainty about that, and the committee will work through that issue. But it does limit the number of agencies that are able to access metadata, and it also provides additional oversight. To some degree it actually narrows the access aspect of it, but what it does do is increase the likelihood that the metadata that is required by agencies when they do seek it will be available.
Mr Leonard: That I think goes right to the necessity point, because the examples that you gave were examples where the metadata had been available under the existing voluntary regime. So that does not demonstrate the necessity of this new regime; it demonstrates that the existing regime is working.

The difficulty is that submitters to this inquiry were asked to take on face value the statement that carriers are in fact reducing the amount of information that they retain such that the voluntary disclosure regime may become less effective over time. I do not think that that has been demonstrated in evidence or at least that I have seen in the submissions.

Senator BUSHBY: We had oral evidence from the AFP—and also from ASIO, I think, but I may be wrong on that—at the hearing on 17 December that, in their view, the changing business practices and business models that are being used by telecommunications providers are leading to a significant decrease in the retention of some of the data that they have traditionally been able to access in order to undertake their activities. My memory—and I may be wrong—is that they said that it is not so prevalent in the major carriers but is prevalent in the new operators that are coming into the market. And they said that it is, to some degree, noticeable in the major carriers. There was a statement by the Deputy Commissioner of the AFP, I think, that the AFP are concerned that within five years their ability to undertake the type of investigations they currently do will be severely hampered and that it will have severe implications for the work that they do on serious crime and terrorist activities. That was where the urgency came from. That, together with other information we have been provided, is what motivates certainly me when it comes to the need for doing it. The reality is that you cannot go back to reconstruct data if it has not been kept.

Mr Leonard, I believe you have read these, but both the AFP and ASIO talk in their submissions about how their figures are indicative only and cannot be said to represent the entirety of investigations or leads that may have been actively pursued had they been confident that the data had been retained. I presume you have read those as well. The data was there for the case studies I referred to, but there may well have been other things that could have been done if data had existed.

Mr Leonard: We are not debating the policy as the government sees it. We as the Law Council are here to assist in the formulation of law to address the policy concern. The key point is that we are seeing the legislative response as disproportionate to the demonstrated necessity. I think the cases you referred to were all serious crimes or terrorism offences. One of the points that we make in our submission is that there might be a case in respect of some classes of data but not others.

Senator BUSHBY: You mentioned earlier the risk that, because there is an opportunity for the Attorney-General to add agencies to the list of enforcement agencies, agencies could be included that are not actively involved in serious crime or terrorist activities, which is something that the committee have had a lot of evidence on and we have worked through that. But, in the event that the metadata is retained, does the Law Council acknowledge that there are strict rules around how the AFP and particularly ASIO can access and use that and that there are procedures currently in place to make sure that they are only accessed for legitimate purposes by those agencies?

Mr Leonard: I think our principal concern is the self-certification process within agencies as to whether use is reasonably necessary. There is the reliance upon such checks and balances and safeguards as there are in the legislation of the individual agencies. For example, you referred to the safeguards that reply to ASIO which come out of their legislation, but when you come to this legislative scheme all that is required is a self-certification by the agency concerned that the disclosure is reasonably necessary for its law enforcement functions. Our concern is that that is, in essence, both a low threshold and without any form of independent oversight or overview for the determination of what is reasonably necessary.

Senator BUSHBY: Okay; I note that. I do not know whether you were here earlier when I looked at some of the restrictions—using ASIO as an example, as you just raised—that are placed on ASIO in terms of accessing its surveillance activities and accessing information, and how that works. Were you present?

Mr Leonard: Yes, I was.

Senator BUSHBY: This act may not impose restrictions to the extent that satisfy the Law Council.

Mr Leonard: Yes.

Senator BUSHBY: The question is: does ASIO's act, which then controls how they deal with that information, satisfy the Law Council?

Mr Leonard: I think the ASIO Act is probably sufficient, except that we make some recommendations about reporting as to uses, with the aim of getting harder evidence around the data that is used and the age of that data.
Senator BUSHBY: Also, with ASIO the Inspector-General of Intelligence and Security does come in and examine the record keeping, and the submission from ASIO indicates that every time they do that they record why, and the purpose for which they sought the data. That is all recorded, and IGIS has access to that to make sure that that is the purpose, and they can do their inquiries to make sure that it has been accessed for the reasons stated and so on. So, there is the oversight there. Similarly, the AFP, if it accesses information, is subject to accessing it for legitimate purposes. Yesterday ACLEI, the Australian Commission on Law Enforcement Integrity, indicated that if they became aware that officers in AFP were accessing information and using it for purposes other than legitimate purposes then that would be, in their view, a corrupt activity, and they would be investigating that. Does that provide any degree of comfort that retained metadata being accessed by these agencies—ignoring other potential ones at this point—does have an appropriate mechanism to ensure that it is being used only for legitimate purposes?

Mr Leonard: The difficulty is the circumstances in which the independent regulator might become aware of, in your example, corrupt activity. Our concern is not corruption within the AFP; our concern is overreaching investigation. And there is simply no oversight of that, because there is no mechanism for anyone to look at the way in which the investigations are being conducted.

Senator BUSHBY: There is no independent mechanism, other than internal mechanisms?

Mr Leonard: That is right.

Senator BUSHBY: Okay; I hear your evidence. I think I might leave my inquiries at that point.

Mr DREYFUS: I want to ask you I suppose a philosophical question. Actually, before I do, I should disclose to the committee my interest in the Law Council of Australia, as a former director—as the representative of the Victorian Bar for some years on this body. The philosophical question goes to how one deals with the proportionality question and how this parliament ought to approach the proportionality question. You have rightly described this bill as blanket retention of telecommunications data. And Senator Bushby has put to you some questions. I want to make sure I do justice to him, but effectively there is anecdotal evidence that one can point to of the use of telecommunications data for investigation purposes. There is anecdotal evidence of the use of telecommunications data to prevent serious crime—to prevent a terrorist act, on more than one occasion—from occurring in Australia. And there is some anecdotal evidence of the use of historical telecommunications data to support a conviction.

So, that is on one hand—individual instances, if you like. On the other hand, there is the possibility of a more statistical approach, such as we see in the United States Supreme Court decisions and in European court decisions. And I would add to that that of course the European court has a particular jurisprudential framework that it is using to consider the proportionality question. The United States court—or courts, because it has been at the Federal Court level recently—is considering questions of blanket data retention against the fourth amendment of the US constitution—unreasonable search and seizure. Here in Australia where we do not have quite the same jurisprudential framework as Europe and certainly do not have the same constitutional framework with the bill of rights that the US enjoys, what approach or framework should we be using to consider the proportionality question that you and many other submitters have raised? I am sorry for the long question.

Dr Molt: I think the proportionality test that we should be using comes from the International Covenant on Civil and Political Rights. Article 17 of that covenant discusses the right to privacy. So I think that is the source where we start from. In certain circumstances I suppose that right can be infringed upon. What we have suggested in our submission is that, when looking at the issue of proportionality, we can rely on the decision of the European Court of Justice where they discussed a number of factors in relation to their EU data directive on proportionality. That included, for example, that a prior review by an independent body is desirable when you are looking at a question of proportionality. They also make a number of other suggestions.

Mr RUDDOCK: Could I put to you another view, which I discovered yesterday, in the submission from the Australian Privacy Commissioner, quoting from the United Nations High Commissioner for Human Rights, who had this to say:

The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal.

You would not disagree, would you, with the view that if we have some chance of preventing terrorism, privacy rights ought not to prevail?

Dr Molt: No, we would not disagree with that, but what we would say is that there still need to be some kinds of limits on how that is framed.

INTELLIGENCE AND SECURITY COMMITTEE
Mr RUDDOCK: It does not say that. It says 'some chance that it may protect a person's right to life'.

Dr Molt: That is right.

Mr RUDDOCK: You are suggesting that privacy of others should have some greater priority over the state's capacity to protect my right to life?

Mr Leonard: No, I do not think we would suggest that, Mr Ruddock. What we would suggest—

Mr RUDDOCK: Let me be clear: I am also associated with the Law Council and you are not speaking for me.

Mr Leonard: Sorry. Our view is that the proportionality must be assessed at two levels. Firstly, the proportionality of the initial data collection and then the proportionality of the people who can have access to that data and the circumstances in which they can have access. Certainly, if there is some chance that data that is collected may assist in the prevention of terrorism, the detection of terrorism or of serious crime, we would accept that there should be proper procedures for accessing that data. The difficulty is that if you say that data should be retained in the first place because there is some chance that it may be of assistance to law enforcement, it describes no barrier, no boundary to what information is to be retained.

Mr RUDDOCK: I am suggesting that if there is some chance of it preventing terrorism and protecting people's right to life we should pursue it. I guess what you are arguing is that if you have that information, there may be some limits on the purposes for which it can be used—I am prepared to accept that—but the question as to whether or not you should be able to get it, I think, is beyond doubt, given the terrorism issues. 'If there is some chance'—that is what the high commissioner was saying.

Mr Leonard: The smart phone that we now each carry does carry the information of what we do in the home, in the workplace, in transit and at leisure and, added to the other devices that will soon track our activities within the home, in essence creates a pervasive surveillance capability—

Mr RUDDOCK: Oh come on! All it tells you is that I am at home. If you are going to find out what I am doing on it when I am at home, you have got to have a warrant.

Mr Leonard: It will tell you enough about what you are doing at home that many inferences can be drawn without obtaining a warrant. There were some interesting examples in the appendices to the Privacy Commissioner's report of how that could occur.

Mr DREYFUS: I am genuinely interested to hear from the Law Council as to how this parliament should approach the proportionality question. Just to pick up a phrase used by Mr Ruddock in his question, drawn from a European human rights authority—

Mr RUDDOCK: The High Commissioner for Human Rights.

Mr DREYFUS: The UN agency based in Geneva. The UN Human Rights Commissioner—and I do not have it in front of me—refers to some chance that particular forms of data might be able to be used. To take perhaps an extreme example, one could hypothesise that if some Australian government were to put a police officer armed with a submachine gun—or perhaps two, for good measure—on every street corner in Australia, and subject the population to random search and seizure, that would provide some chance that terrorism could be reduced. Stating that—it is an extreme example—to my mind demonstrates the problem. I would invite the Law Council, for the assistance of the committee, to reflect on how this question of proportionality is to be approached not in relation to access alone—because we can all, I think, understand more readily how proportionality can be applied by comparing the purpose for which the information is being accessed by a law enforcement authority, as against intrusion of privacy—but, rather, in relation to the blanket retention of telecommunications data, which is what is proposed by this bill.

Mr Leonard: I think the Privacy Commissioner, in his submission, which is where the quote came from, applied that reasoning to then conclude—and I would agree with it and I think the Law Council would agree with it—that, in determining proportionality, it is important that any scheme only requires service providers to collect the minimum amount of information necessary to meet needs and to retain that information for the minimum amount of time to meet needs and that the needs then be demonstrated after conducting a privacy impact assessment. Privacy is always a right that is balanced against other rights, including my right to walk down the street—

Mr RUDDOCK: No, I am saying 'some chance' to protect my right to life—and you are wanting to water that down.

Ms Ganopolsky: From a privacy perspective, I fully support, and also wish to add emphasis to, the articulation that the Privacy Commissioner has set out in paragraphs 10, 11 and onwards in that submission. But
in terms of assisting the committee to consider the proportionality in the Australian context, I think we do have to go back to the discussion on article 17. The specific section in article 17 that I think would assist this discussion and the committee's deliberations is the emphasis on the arbitrariness of the intrusion. So most of what has been said in submissions—certainly the submissions that the Law Council has put forward—is about the ability to balance these considerations. The absence of independent oversight goes to the arbitrariness questions, and therefore the quite difficult conceptual balancing exercise that we are now undertaking.

So if it would assist the committee, in addition to just noting article 17 generally, I think we need to focus on the specific wording of article 17. It is clearly emphasising the problem of having arbitrary interference with privacy and reinforces that with the fact that everybody has the right to the protection of—

Mr RUDDOCK: There may be questions about the adequacy of oversight but there is oversight. You may question the adequacy of it but there is oversight.

Dr Molt: We acknowledge that in our submission.

Ms Ganopolsky: We question how arbitrary it is and I think that that is the emphasis. To the extent that we are here to deal with the creation of new laws rather than debate complex policy questions or very detailed and logistical issues around law enforcement and surveillance, from a privacy perspective I think that is our starting and finishing point. I think it is also worth considering, as part of this deliberation that the amendments to the Privacy Act that came into force as recently as March last year were a substantive review of the frameworks around privacy and how Australia would meet its obligations.

The important element there is that, specifically, the Privacy Act in essence expanded its jurisdictional remit by what is a new definition of what is personal information. And increasingly what we are seeing—and certainly from the discussions and the submissions that have been made today—is that most of the information that would form part of the retained information would be personal information. And I draw the committee's attention to the fact that section 6 of the Privacy Act has a definition of 'personal information' that is no longer linked back to the ability to identify an individual from that information; it is the ability to identify an individual per se.

I do not wish to take up any more time of the committee by stating the obvious—the volume and sensitivity of the information that would be part of the retained data, including sensitive information as defined. I only draw attention to the fact that we have effectively a newly revised privacy regime which casts a very broad set of protections in any environment where personal information is involved. It is the legal framework that we live in.

I go back to the legal question about how you go about assessing proportionality. I think it is really a combination of what article 17 directs us to and the jurisprudence, as has already been noted, stems from article 17. So I think we are in good hands into determining how we consider proportionality if we focus on the arbitrariness question.

Mr Leonard: I do think it is useful to think of the number of rights that are in play here—not just see this as privacy versus the needs of national security. I would say that there are at least three individual rights that are in play. The first is a right to privacy. These are in no order of importance. The second is a right to personal security and the security of those other citizens. The third is a right that is not as well formulated but is a right to conduct my life free from pervasive surveillance.

The fact that data is retained about me is not, of itself, pervasive surveillance, but it does enter into the balance between those three rights—that if there is a risk that data may be used to undermine the other rights that I should enjoy, then that should be assessed in determining the proportionality of the data retention. So I think it is necessary to look, firstly, at the data retention, and balance its effect on other rights before we go to the question of proportionality as to how the data is used.

Mr DREYFUS: Thanks, Mr Leonard. Perhaps to wrap this up I will see if I can focus it a bit more. This bill draws some lines. It draws a line in saying, 'We the Commonwealth will require the 600-odd service providers in Australia to keep data for two years.' That is different to the line that was drawn in some European countries in respect of some classes of data, which was at six months, or in other European countries, including Britain, at one year. That is one line. Another line, just by way of illustration—there are multiple lines, obviously, that have been drawn—is the one that I raised in questions to the Optus representatives which I think you were here for. I was pointing out to them, and they have a concern about it, that there is an exclusion in this bill of the requirement to keep information about the location of a telecommunications device if information about the location is not used by that service provider. That is another line that has been drawn.

In both cases, there is—to use Mr Ruddock's phrase or the UN High Commissioner's phrase—'some chance' of the use of information about the location of a telecommunications device for national security purposes, even if that information is not being used by the service provider. Equally, it is possible to conceive that there is 'some
chance' that national security purposes would be served by accessing data that is older than two years. So I would ask again, having—

Mr RUDDOCK: They are very useful suggestions we might be able to follow up!

Mr DREYFUS: If Mr Ruddock would let me finish, this time. I ask again: what framework does one bring to bear on this, in the proportionality sense, to draw those lines? I will be asking the Attorney-General's Department about this too because they are the originators of this bill and represent the government in these hearings. But what framework should this parliament apply to assess where the line should be drawn?

Mr Leonard: I think the lines have to be determined by reference to the safeguards around the use of information. If, for example, a decision is made that this information might be available without a warrants process or without any form of independent oversight of the decision to access particular information about communications, I think that then says that the line should be more tightly prescribed. The real issue, though, I suspect, is not the breadth of the dataset but rather the oversight of how data within that dataset is used. There are obvious concerns that the dataset might be redefined over time, adversely to both citizens and ISPs that bear the cost of a broadened dataset. But the greater concern, in the Law Council's view, is the absence of safeguards around the way in which that information may be accessed and used.

Mr RUDDOCK: It is not 'absence'; it is adequacy. There are safeguards.

Mr Leonard: There are safeguards, yes.

Mr RUDDOCK: It is their adequacy that you are calling into question.

Mr Leonard: Today, in the act, through the self-certification process, the only safeguard is a decision made by the agency itself as to whether the—

Mr RUDDOCK: No. No. There is the role of the Inspector-General of Intelligence and Security in overseeing these matters. There is the separate role of the Commission for Law Enforcement Integrity in investigating these matters. All I am saying is that there are safeguards; it is a question of their adequacy. You said 'absence'. That is all.

Mr Leonard: Those safeguards are external to this act and the evaluation of this act, and it happens that they are quite comprehensive in respect of two agencies, which are both, I think, within the purview of this committee; and that is probably, therefore, reflected in the adequacy of those safeguards.

Mr RUDDOCK: It is adequacy, not absence. That is the only point I am making.

Mr DREYFUS: To pick up Mr Ruddock's question, the two safeguards Mr Ruddock has identified for you, which you have correctly said relate to ASIO on the one hand and to the Australian Federal Police on the other—is that right, Mr Leonard?

Mr Leonard: That is right.

Mr DREYFUS: But not to any of the other bodies potentially that could have access to this data?

Mr Leonard: We would need to look at the safeguards that operate in respect to each of those bodies but many of those bodies that can currently access data and potentially could under this legislation are not subject to safeguards at all.

Mr DREYFUS: There is one other matter to make clear—your submission is very detailed and that is of assistance to the committee because it means we do not have to take up time in these oral hearings—and that is your proposition that the dataset, that is the description of the data that the 600-odd telecommunications providers are going to be required to keep, should be set out in the bill itself. Particularly at paragraph 38 of your submission which is on page 11, and at our page 39, you say: The Law Council's Rule of Law Principles require that the law must be readily known, available, certain and clear. The current lack of definition to the scope of data to be retained in the bill is inconsistent with this requirement.

Is one of you able to speak to that proposition arising as it does from the Law Council's rule of law principles?

Mr Leonard: The key aspect of this legislation is the definition of the dataset that is to be retained and therefore potentially available. A matter such as that which is at the heart of the legislative scheme here and any assessment of proportionality of the legislative requirement to have this data retained and available requires it to be clear and likely to remain static for sufficiently long that decisions can be made about the legislation which implements that requirement. The difficulty is that firstly we are talking about a dataset that currently is in draft form that may or may not be the dataset that is initially promulgated and then secondly that dataset can be changed over time without any prior oversight and with only the opportunity of the parliament to review retrospectively as a regulation. It is then a question of whether the dataset is embedded in the legislation itself or
other safeguards are included to ensure that there is, for example, proper consultation and consideration around any change to that dataset. I noted with interest that the Privacy Commissioner included some recommendations about how the dataset might be subject to review if it were not specified in the legislation itself and in particular the concept of prior public consultation on a draft and the regulation not entering into effect until the parliament had an opportunity to review the regulation and that there should be prior consultation with the Privacy Commissioner. I think they are all excellent suggestions. We had suggested in our submission that it should be included and therefore locked in the legislation itself in the interests of certainty but we do hear other evidence which says that there is a need for some flexibility, ability to change over time, and if it is considered that to lock the dataset into the legislation itself is excessive, then there are these alternative safeguard mechanisms that could be used.

Mr DREYFUS: Thank you, Mr Leonard, and thank you to the Law Council.

Mr CLARE: Can I follow that line of questioning and ask: such as? What types of safeguards are you principally talking about there?

Mr Leonard: We would, I think, endorse the recommendations of the Privacy Commissioner that if there is to be a change to the dataset then, firstly, that it be initially exposed in the form of a draft regulation with a period for public consultation; secondly, that it be subject to a privacy impact assessment, which should include the consideration of the cost of the implementation of the change and any effect on individuals' privacy through that change; and, thirdly, that the regulation should not enter into effect until that had occurred.

Mr CLARE: Do you have a view about what potential role this committee might have in reviewing any potential changes to the dataset by way of regulation before the regulation was made?

Mr Leonard: This committee clearly has the advantage of working with knowledge of the requirements of intelligence agencies and law enforcement agencies where sometimes that knowledge cannot be made public. So this committee does have unique advantages as well as skills in reviewing legislation of that type.

Mr CLARE: I wanted to ask you about the recommendations that the Law Council makes at page 21 of your submission that deal with the issue of the availability of retained telecommunications data for civil and non-law-enforcement purposes—specifically the recommendations at No. 96. Above that, at point 93, the Law Council notes that:

Significant risks include attempting to determine journalists' sources, cases involving alleged infringement of online copyright, family law proceedings, civil claims involving use of machinery or motor vehicles, class actions or other legal proceedings.

It then goes on, at 94, to say:

The Law Council recommends that access authorised by other Federal, State, or Territory laws, or pursuant to court process should be precluded to ensure that the impact of the Bill is clear and limited to achieving its stated purpose.

I just want to be clear about what you are proposing there, because one of the concerns that has been raised in some submissions is about access to this data via discovery purposes in civil litigation and how it might apply to some of the things that you have identified there. Is it your proposition that any data that is preserved under a scheme like this should not be made available or should not be accessible in the course of any civil litigation?

Mr Leonard: We think a relevant concern for this committee is that many of the submissions and much of the public comment about the impact of data retention and the safeguards around the use of retained data have focused exclusively on the operation of this bill and the safeguards that this bill creates. What we are potentially creating here is a very rich data source that could be of value in a broad range of other circumstances, such as those that you have just referred to. The question then becomes: 'Should the committee be concerned as to those potential uses, and the lack of safeguards within the act itself as to those uses?' and that is our concern.

There are a number of ways in which this could be addressed. One might be a process whereby access to this data outside the regime was precluded but for regulation allowing access of particular bodies for particular purposes—again, following public consultation. That at least would provide some control over the ways in which this information might be used.

We go back to the point raised earlier by Mr Dreyfus as to how you measure the proportionality of this data retention in the first place—that is, before you look at the question of access under this legislation. If in fact this data set can be accessed in the broad variety of ways using civil process and discovery processes, then you need to assess the impact on individuals of that retention on the basis of an indeterminate class of people looking at that data, and the only control being such controls as the courts might choose to impose when issuing subpoenas. In fact, in litigation nowadays the controls on the issue of subpoenas are relatively light, so one might expect that as...
this data set is recognised as being of value in these broad range of proceedings, many litigants, both civil and in
class actions, will seek to use this data source.

Mr CLARE: That begs the question: should the legislation be silent on this? Should we leave that to the
court? Or are you arguing in your submission that there should be something in this legislation that proscribes
access to this data, conscious of course that at the moment civil litigants already have access or potentially can
subpoena this type of data?

Mr Leonard: Our submission is that the bill should be amended to preclude access. An alternative submission
would be that it proscribes access so that access would only be permitted if and where particular access or classes
of access were permitted by regulation.

Mr CLARE: And in that case you are talking about certain agencies or certain situations, because two that
have been brought to the attention of the committee already have been civil litigation that might involve online
copyright, or a private health insurance agency wanting to get access to metadata on a client, potentially in
relation to their health records, via the Fitbit they carry around on their wrist. When you are saying that you would
limit that to certain situations are you limiting it to certain agencies? How would you limit the way the court
might make decisions about what can and cannot be accessed?

Mr Leonard: To answer that question would require an assessment of the impact of the change. That is both a
privacy impact assessment and consideration of other human rights as well, such as the right to go about our
business free from pervasive surveillance. So I think it is difficult to answer in the abstract, but I can envisage that
regulations might allow access either by agency, by specified level of court or by class of action.

Mr CLARE: Specified level of court?

Mr Leonard: Yes.

Mr CLARE: So it may be that a Supreme Court, for example, might be able to make decisions in relation to
subpoenaning access to certain data?

Mr Leonard: Yes.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your
evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please
forward this to the secretariat as soon as possible. If the committee has any further questions the secretariat will
write to you.
MURPHY, Mr Paul Vincent, Director, Media, Media, Entertainment and Arts Alliance

WARREN, Mr Christopher John, Federal Secretary, Media, Entertainment and Arts Alliance

[11:29]

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

Mr Warren: I would like to make some very brief introductory comments. We obviously had the privilege of hearing the previous discussion concerning the Law Council. They have raised many of the issues and concerns that we also share about the scope of the legislation currently before the committee. Obviously we have general concerns about the legislation but the specific concerns we want to talk about are the very real impact that this legislation will have on the operation of a free and democratic media in Australia and that effectively the legislation in its current form will prevent the media properly fulfilling its role of scrutinising and reviewing the actions of government and others in power to the extent to which it would be impossible to say that a free press would be able to continue to operate in Australia. For that reason, we believe the legislation should not be proceeded with, that it should be taken away, reviewed and redrafted and, at the very least, there needs to be with this legislation, as there should have been with the earlier two tranches of national security legislation, a clear exemption and exclusion of the media and the operations of the media from these laws. Thank you.

CHAIR: Thank you. Does anyone have questions?

Senator BUSHBY: I have a question on that last point. How do you imagine such an exemption would work? Would it be an exemption on the retention of metadata around journalists or an exemption on accessing it? The first I could see would be quite difficult practically to put in place.

Mr Warren: The first would be preferable. I accept the difficulties with excluding people and indeed there is a risk that excluding certain categories or rather manipulating the metadata in advance can in some ways be worse than the disease, which is why we believe it should not be recorded in any event. The real concern of all of this is that the use and the keeping of metadata makes the ability to identify confidential sources and the communication between a confidential source and a journalist transparent to the authorities. We have seen over the past 10 or 15 years an increasing amount of referral to particularly the Australian Federal Police for investigation of breaches under the Crimes Act. The simplest way of investigating those breaches for unauthorised disclosure of information is by accessing the metadata of the journalists involved. That is what has occurred in the past and that is what should be prevented from occurring in the future.

Senator BUSHBY: I understand your position on that. Also, though, if you were able to work out how to exempt the retention of metadata, presumably there would also be times when journalists work with law enforcement and security authorities and may be contacted by people involved in criminal or terrorist conspiracy activities and being able to access their metadata might be of assistance, with the agreement of the media personnel involved, in working out what is going on. That could present a risk or undermine the ability of our agencies to conduct investigations.

Mr Warren: It is difficult to speculate on hypotheticals—I suppose it is only hypothetical if you are speculating. Generally speaking, the historical case has been that there are many examples where a journalist has become aware of an action of a law enforcement authority which is an ongoing action and would approach the law enforcement authority, and in most of those cases—in fact in all of them, to my knowledge—there is then some arrangement entered into to restrain publication until such time as—

Senator BUSHBY: I am aware that journalists work with law enforcement agencies at times where they become aware of criminal activity.

Mr Warren: We are also very concerned about the monitoring of that. There has been a lot of evidence come out in the last few weeks, particularly in the United Kingdom, about monitoring of not just the metadata but all of the emails of individual journalists, particularly investigative journalists, and we—

Senator BUSHBY: I do not believe that can happen here unless they are a person of interest in the first place.
Mr Warren: One of our criticisms of the first tranche of the legislation is the extent to which it would facilitate ASIO, in that case, to treat journalists as persons of interest, which is how this problem began in the United Kingdom. So yes, we do not have direct evidence of it happening in Australia yet, but there is now a legislative framework, or a legislative permission, for it to occur.

Senator BUSHBY: I understand the risks that you see here and that you are putting forward, and I was trying to work through that particular point. If we did put those exemptions in place, either on the metadata or otherwise, what impact might that have and how could we work through that to try and come to ensure that the end result—if the government were to adopt what you are suggesting—could still work so that we do not unduly restrain the activities of our law enforcement and security agencies but theoretically try to meet what you are trying to argue?

Mr Warren: Another way of doing it, which I think was the suggestion of the Law Council—and, again, I say this with the view that our prima facie position is that there should not be a data retention regime because of the risks it involves—is to restrict rights to access to serious crimes that involve risk of life. The difficulty that we have is that a lot of the discussion is about hypotheticals, but in our case it is a real case. There is no doubt under the current legislation, because of the failure of repeated governments to decriminalise the leaking of information, that a whistleblower or a confidential source of whatever nature is committing a crime—when they are a government employee—when they release information to a journalist. We know that those crimes are routinely referred to the Federal Police, they are treated as a crime and the police rely on metadata to prosecute. Partly as a result of that, we have had the conviction of two journalists for refusing to reveal confidential sources, and, in fact, the major cases of prosecution for unauthorised leaking of information over the past decade have involved the use of metadata identified by accessing the phone records of the journalists involved.

Senator BUSHBY: I am happy to leave it at that.

Mr Byrne: I have a question in relation to a separate submission—I think it was The Guardian submission, but I am not quite sure. In another matter we were looking at a control order being initiated, and on behalf of the person who was subjected to the control order there would be a public advocate almost, separate to the legal process, that would be seconded the moment that the control order kicked in to act as a liaison point and to make sure that the rights of the individual that was subjected to the control order were being looked after.

I know that this is a deep concern within the journalistic fraternity. Should a journalist come under the aegis of a metadata request, that public advocate—who obviously would have to be security cleared, so there would be security matters—could be engaged so that the rights of that journalist could be taken into account. Is that something that you would see as a potential safeguard?

Mr Warren: I am not sure how practical that is. Of course, it is not just the rights of the journalist; it is the rights of the whistleblower as well. The problem of having a criminalised approach like that is it acts as a very serious chilling effect. The main impact of this legislation is to have a chilling effect on any potential whistleblower or confidential source releasing information they would not want to release. If there is a data retention regime, I cannot think of anything that would be practical short of an exclusion either specifically or by restricting the degree of severity of the crime that is being investigated and/or by government or the parliament taking up the recommendations of, I think, two law reform commissions to decriminalise the unauthorised disclosure of information.

Mr Byrne: Have you had any consultation with the Attorney-General's Department or the technical working group to outline your concerns outside of this committee process?

Mr Warren: On this legislation, no. As you know, we have made repeated submissions to this process and have written to governments about it.

Mr Byrne: Your views have not been taken into account, though. You were not asked to provide a view?

Mr Warren: No. I think we have written to successive Attorneys-General on this.

Mr Byrne: Did you get a response to this particular matter that you raised?

Mr Warren: I do not recall, but I would not want to be definite about that.

Mr Byrne: Okay.

Mr Dreyfus: I want to focus in on what it is that the media alliance is seeking. You have given examples on page 8 of the cases of Harvey and McManus—Kessing also, although I am not sure he was a journalist—

Mr Warren: He was convicted as a result. In his particular case the Federal Police looked at the phones of the journalist who wrote the story and identified that he had been called. As I remember it, the relevant journalist on The Australian newspaper had been called from a public phone around the corner or near Kessing's home address. That and the fact that he was the author of the report that had been leaked were what they put together to establish
the case against Kessing. In the Harvey and McManus case, again, the public servant in that case who was then prosecuted—Kelly, I think his name was—was identified as a result of looking at the phones of either Harvey or McManus. I forget which one it was originally; it was a joint by-line story. Through that they were able to identify an incoming call from the particular public servant in, I think, the Department of Veterans' Affairs, who was then prosecuted for unauthorised disclosure of information and was convicted. His case was then overturned on appeal. In the course of that first conviction case Harvey and McManus were put into the witness box, were asked a question to reveal their source, of course refused to do it and so were then prosecuted for what I think in the case was the statutory offence of contempt of court and were convicted. So both of those cases, which were a couple of the major cases that flowed from the direct use of metadata to put a source and a journalist or journalists together.

Mr DREYFUS: So what is it that the Media, Entertainment and Arts Alliance proposes if some form of legislation requiring data retention goes ahead?

Mr Warren: As we say there on page 9, there should be in the earlier tranches—particularly the first tranche on reporting the actions and activities of ASIO—a media exemption to ensure that press freedom related cases are not caught up in this legislation, so journalists and confidential sources and whistleblowers can go about what they do. That is a key part. There should be a means of training agencies in press freedom, embedding the concepts of and commitment to press freedom and media freedom in the day-to-day operations of those relevant agencies. We set out those recommendations on, I think, page 9 and 10 of our submission.

Mr CLARE: Can I just explore that in a bit of detail. I presume what the telecommunications companies would say is that it is impossible for them in the preservation of data to exempt certain individuals based on their occupation—put aside for a minute the definition of a journalist. I guess what I am thinking is that one potential solution here might be making metadata that is collected by law enforcement agencies that relates to a journalist not admissible in court in certain circumstances. Would that address the concern?

Mr Warren: It would not get over the chilling impact, because of course the authorities would then be able to identify the whistleblower, the confidential source or whatever, and then use that to take whatever action they want to.

Mr CLARE: But if it is hard for the ISP to not store it and it is hard for law enforcement when it makes a metadata application to an ISP, perhaps not knowing who they are investigating but then getting telephony or IP details back that lead them to identify that a journalist is involved, and they do not know that until they get that information back, is the solution—

Mr Warren: In practice that is probably not right, because what the law enforcement authorities are trying to identify is who has spoken to whom. They know who 'whom' is because it is the journalist's or the media organisation's by-line or representation. So, once you know who 'whom' is, the nature of metadata is such that you can use that to work out who 'who' is.

Mr CLARE: In circumstances where the 'who' is the journalist, that is correct, but that will not always be the case, will it?

Mr Warren: Practically, it would normally be the case, although again the problem would be overcome by the Law Council's recommendation that there be a legislative restriction on the use of metadata for serious crimes or for crimes that involve serious threat to life, or however it would be defined.

Mr CLARE: The law council's recommendation about limiting access or use of the data for serious offences?

Mr Warren: Yes.

Mr CLARE: Do you think that would satisfy your concern? There would still be instances there of press freedom issues, wouldn't there?

Mr Warren: Potentially, but there would be fewer. Our concern would always be in this instance that we are already deeply embedded and deeply affected by the regime and the inevitability of scope creep in these things. I know this came up a bit in the discussion earlier about access to the data in civil proceedings. Indeed, that is a serious concern, because of course whistleblowers are not just confined to the public sector. It is a criminal offence in the public sector; it is not necessarily a criminal offence in the private sector but it may well be a civil offence—breach of contract of employment, breach of copyright or some such related offence. There would be a concern if the data could be accessed in a civil hearing to enable a private corporation, for example, to seek to identify an internal whistleblower whose action may not be illegal but may be a breach of their contract of employment.
CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you. Thanks very much.
CHAIR: Welcome. Although the committee does not require you to give evidence on oath, I remind witnesses that this hearing is a legal proceeding of parliament and warrants the same respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Mr Dickson: In my position as the Assistant Commissioner of Crime Service in South Australia, I am ultimately responsible for all investigations of serious offending that occurs in the state. Part of those investigations rely heavily on the subject of our meeting today. I am also the chair of the Serious and Organised Crime Coordination Committee, which is a national body made up of the heads of all crime areas and other law enforcement partners in tackling serious and organised crime.

The data retention bill, if approved, will require companies providing telecommunications services, carriers and internet service providers to keep a limited but prescribed set of telecommunications data for two years. I believe that the data referred to in this bill is best described as information about a communication and not the content of that communication. I think it is very important that we understand the difference. In simple terms, the bill seeks to retain data that provides evidence that two parties contacted each other. The bill does not refer to the contents of that communication.

SAPOL routinely requests and obtains telecommunications data from telecommunications service providers. The data more commonly referred to as subscriber texts, call charge records, reverse CCRs and cell dumps contains information which is often critical evidence in serious criminal investigations which have a significant impact on the community. Currently there is no defined period of time for which service providers must store this data and, as a result, availability differs from carrier to carrier. The data retention bill seeks to legislate the compulsory retention of this data by service providers for the period of two years, which I support.

Access to metadata plays a central role in almost every criminal investigation, including investigations into murder, sexual assault, drug trafficking and kidnapping. In the offence of murder, the ability to actually identify people who have contacted each other is quite critical. It is the same in cases of child exploitation and, obviously, serious and organised crime matters, where you may have people involved in illicit drug-taking or dealing in drugs. Those are significant issues for us. SAPOL has requested metadata to be provided on about 17,000 occasions over the last five years. It is important to note that over 60 per cent have resulted in requests for data that is older than 12 months. Unfortunately, we do not keep records of any greater period of time. We just do not have that capacity.

This proposed amendment bill will provide both the community and policing agencies with valuable information that protects the community and, importantly, provides consistency in approach for the actual carriers. I think that is one of the main issues we have got here. From a policing perspective, there is no consistency in approach. A good example of the issues we have is the inconsistent and unregulated approach and how it negatively impacts on policing. I note that talking about stored data is not within the purview of this committee; I fully understand that. But I think this is a good example of how an inconsistent approach does create issues for investigators.

Currently, a service provider destroys the communication on a 24-hour time frame. Every 24 hours, that stored data is destroyed. So we could have a murder which occurs today—now—and SMS messages could have been sent previously. The investigators become aware of it tomorrow and do their investigation. We can never obtain that stored data because it will be destroyed at 12 o'clock tonight. Because there is no regulation in relation to that it is a good example of how, if we do not have a regulated position, it creates significant issues for our investigators.

Another thing I want to say is that the bill is critical to prevent the capability of Australian law enforcement and national security agencies being degraded. It does not expand the range of telecommunications metadata, which is currently being asked for. We are not asking for any more. It is simply to ensure that metadata is retained...
for a two-year period and that it will assist the investigators and law enforcement to protect the community. Thank you.

**CHAIR:** Thank you. Would anyone else like to make some introductory remarks.

**Mr Lanyon:** Yes, if possible. Can I express my appreciation to the committee on behalf of the New South Wales Police Force for the opportunity, firstly, to provide a submission and, secondly, to give some evidence here today in relation to it. Can I start with an apology. New South Wales Police Force prepared a submission for the committee some time ago. I was advised this morning by our Department of Premier and Cabinet that that submission had not reached the committee. I have arranged for it to come through by email this morning, so it will be available. The submission itself provides a number of case studies which are relevant to the topics I will speak about and certainly in relation to the nine questions posed by the committee. It will provide some further evidence.

The issue of data retention is critical to the efficacy of criminal investigations within New South Wales and also nationally. It is relevant to point out that counter-terrorism and serious and organised crime syndicates traverse traditional borders and, for that reason, data retention impacts on all law enforcement agents, be they state or Commonwealth. New South Wales supports the objectives of the data retention bill in order to ensure a consistent regime occurs with carriers and providers in order to best aid the investigation of criminal and national security investigations. A model piece of legislation would redress some of the current inconsistencies for retention. For example, reverse call charge records vary between seven years and eight weeks with other carriers. Cell tower dumps vary between seven years and six to eight weeks, depending on the carrier. Similarly, by providing a standardised dataset the current situation, whereby approximately 80 per cent of IP requests made by New South Wales to carriers did not identify the end user of the server or subscriber because they are not currently kept, may be ameliorated.

New South Wales Police Force has a vested interest in maintaining access to stored data as the largest user in Australia. Last year, New South Wales made in excess of 122,000 requests to carriers and providers for metadata. Accordingly, whilst agreeing in principle with the objectives of the bill, New South Wales Police Force does hold some concerns with regard to the potential unintended consequences of limiting a period of up to two years for the retention of that data. As indicated earlier, New South Wales Police Force is currently able to access certain telecommunications data for up to seven years. That is generally our call charge records and reverse call charge records.

At a time when encrypted mobile and internet based communication degrades our interception capability, it is imperative that telecommunications data is retained for as long as possible to facilitate investigations. It is also worth highlighting the differences between law enforcement responsibilities at a state and Commonwealth level. Whilst two years may be appropriate for the majority of offences investigated by the Commonwealth and other Commonwealth agencies, such as national security, drug and online sexual offences, states are also responsible for investigating a range of criminal offences, including murders, sexual assaults and robberies, which are often historical or take years to investigate prior to a suspect being identified. The New South Wales Police Force has provided a submission—albeit you do not have it in front of you at the moment, Chair—which outlines a number of case studies demonstrating the complexity of and historical nature of these types of investigations.

I am able to say with some experience from my previous role as Director of Organised Crime in New South Wales and as a longstanding detective, including working with the homicide squad, that there are very few investigations which do not rely on telecommunications metadata. The data is vital to corroborate evidence, identify suspects, eliminate suspects, place movements of suspects or to found affidavits for warrants under the Telecommunications (Interception and Access) Act.

The need for data retention for extended periods is even more important at the moment, as DNA, trace evidence and other forensic science becomes more sophisticated and it is possible to test against older crime exhibits, resulting in the identification of suspects years after offences have been committed. Of the 122,000 requests for telecommunications data New South Wales submitted in the previous year, 4,358 of those requests related to a period greater than two years for retention. Whilst as a percentage this may not appear large, it represents a significant number of offences which may be solved with the access to the information after two years. It is worth pointing out that, of those requests for greater than two years data, the most common offence was murder followed by sexual assault and then robbery.

The New South Wales Police Force is cognitive of the balance of privacy against law enforcement, but would respectfully submit that agencies have thorough and rigorous processes in place to both apply for and manage telecommunications related data. The draft bill, in the New South Wales Police Force's submission, does not focus on content communications, which are rightly governed by a warrant regime under the current TIA Act—
rather, stored metadata which is already available to law enforcement agencies. It is well known by the community that carriers and providers maintain calling records for billing consumer purposes, and there would be a general expectation that these records are not expunged after two years. Similarly, the public rightly expect that police forces continue to investigate and solve matters which are not recent and telecommunications metadata is becoming more critical in that area as technology increasingly makes interception difficulty.

It is the New South Wales Police Force's submission that metadata in the form of CCRs, reverse CCRs and subscriber checks should be available to law enforcement for well in excess of a period of up to two years, particularly when it can be obtained from carriers now for up to seven years and there will be a significant number of serious crimes that go unsolved without it. Thank you for your indulgence.

**CHAIR:** Thank you.

**Insp. Segrave:** I would firstly like to thank the committee on behalf of Victoria Police for the opportunity to appear before you today in relation to your consideration of the issues around the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. Victoria Police considers these issues to be of critical importance to the ongoing viability of avenues of inquiry that police currently routinely rely on in the course of serious and organised crime investigations—that is, access for a prescribed period of time to a defined set of metadata, including call charge records, subscriber information, cell tower information et cetera. In an age where there is an ever-increasing reliance across virtually all elements of our community on telecommunications in its various forms, coupled with increasingly sophisticated telecommunications technologies, law enforcement must be able to stay abreast of the tools of trade or the modus operandi of the similarly empowered and sophisticated criminal element who are always amongst us.

One of the touchstones of investigation that junior investigators are taught is the notion that every contact leaves its trace. In the past, this was intended to draw the investigator's attention to the possibilities of fibres, fingerprints and DNA evidence. In the present, this thinking is just as applicable to the opportunities provided to serious and organised crime investigators by metadata. And, just as in the case of more traditional crime scene analysis, often the lawful access to and analysis of metadata will form part of the initial actions taken at the earlier stages of an investigation, particularly in the case of proactive investigations—such inquiries being intended to help understand how an offence may have been committed; to identify suspects; to eliminate or exculpate persons not relevant to the investigation; to open up new avenues of inquiry; to contribute to applications for more intrusive investigative options requiring judicial warrants, such as search warrants, surveillance device warrants, and telecommunications interception warrants; and effectively to focus the application of finite investigative resources.

An investigation can be considered to be a process underpinned by a series of logical and ordered steps, and the identification, analysis and interpretation of the traces that an offender has left behind in the course of his or her preparatory actions or actual offending will always be amongst the critical first steps that can ultimately determine the success or otherwise of an investigative process, whether such traces are in the form of a fingerprint or a call charge record. Nonetheless, Victoria Police understands and acknowledges the fundamental principle of a citizen's right to privacy and the inherent tensions between aspects of the criminal investigation process and that right to privacy. In this context we note that this bill is not intended to increase the reach of law enforcement in terms of the types of metadata able to be accessed or the circumstances in which it might be accessed and that the bill proposes to introduce new safeguards against abuse by way of the active oversight of the Commonwealth Ombudsman.

It is the view of Victoria Police that the current safeguards in the Telecommunications Interception Act have proved sufficient; however, we accept that the proposed arrangements would appear to strike a pragmatic balance between the sometimes competing imperatives of the right to privacy and the right to personal and community safety and security. However, if there were to be a move to a situation where additional judicial authority was required to access the types of metadata that are the subject of this bill, Victoria Police believes that this would have very significant if not catastrophic implications for investigations for the reasons I have broadly outlined above; would pose very significant logistical problems for all stakeholders involved, including police, lawyers and the courts, by virtue of the volumes involved; and may well perversely drive changes in policing methodologies that potentially result in the use of more intrusive capabilities—for example, physical surveillance, undercover operatives and the cultivation of human sources, in circumstances where they would not currently be deployed.

In conclusion, I appear before you today on behalf of Victoria Police in order to support and reiterate the written submission already provided to you, to reinforce the Victoria Police view that the ability to access metadata in support of serious and organised crime investigations is a critical element in the majority of such
investigations, to commend the notion that there is a need to enshrine the types of metadata and the duration of retention of such metadata in legislation and to further assist the committee in its deliberations as you see fit. Thank you.

CHAIR: Thank you. I think Andrew wants to fire away first.

Mr NIKOLIC: Gentlemen, thank you for your contributions. There has been some evidence to the committee asserting the need for a warrant or judicial process not just for content of information and telecommunications information but for metadata as well. I will try to paraphrase the logic behind some of those submissions. It is that metadata information is as compelling from a privacy perspective—what it reveals about an individual—as the warrantable content information might be. So my question is in two parts. Do you have a perspective on the operational impact of introducing a warrant or judicial system for metadata, not just for content? Second, could you provide some insights on the way you use metadata and the intensity of intrusion in personal information as it relates to metadata? What do you use that information for versus the level of intrusion should you need to seek content through a warrant?

Mr Dickson: I will answer the second part of that question before I answer the first part. By way of example, in a police submission where an individual was murdered, we had no suspects of that murder. Then we identified who that person had been in contact with. We had his mobile phone or knew where that mobile phone was. There were certain contacts which occurred between certain parties in the 24 hours before his death. Obviously that came as metadata. That is how we obtained that information. That led to us identifying, once we had that information, who those individuals were. Then we were able to get further intelligence which led to those people being suspects, and ultimately they were convicted of his murder. It related to a drug rip-off. That is just a very simple example.

Metadata is really just about where the communication occurred, when it occurred, place, time—those sorts of issues. As you quite rightly say, it does not actually relate to the content of that metadata. Often, when we seek that metadata, we are just looking for information because we do not really have much else to go on. We are using that information tool to find out what contact, what communication, the suspects or the victim have had and to then go and speak to those individuals to find out what is the relationship and just going through that process, as any good investigator should do. Really it is an intelligence tool to provide us with information to assist us with that investigation. Often the metadata does not get us anywhere because it is not relative to the investigation.

The first part of your question in relation to—as you are fully aware, the stored communications warrant is a warrant process we go through, but under the legislation the metadata that relates to the warrant has to be 'reasonable and necessary' in relation to a criminal offence. In South Australia we have two levels of authority: the first level is a senior police officer who authorises that metadata is to be collected and the second level is the authorising officer, who is the superintendent, who provides that authorisation. So we do have our own internal requirements that are not part of the legislation; we do have a process in place. From a policy position, five years or more is the penalty provision. That is how we have designed it; other law enforcement agencies could be the same or could be somewhat different. You have just heard about the impact from the New South Wales police. We have about 4,000 a year. New South Wales police would have a significantly higher number than that. The ability to obtain that information, going through a warrant process for that information, would be a significant drain on the investigation—and not just our resources but also the resources of the judiciary and courts and whatever. I think it is quite a big ask.

At the moment we are audited by the state ombudsman twice a year and the Commonwealth Ombudsman once a year. I would have thought the issues that came up about us not doing the appropriate things in relation to metadata or TI applications would become a red rag in relation to those audits that are conducted.

Mr Byrne: Did you see the front page of *The Australian* today, when you say that?

Mr Dickson: Yes.

Mr Byrne: So while you are saying that—and that was referred to an ombudsman. No reflection on anything, but I am just saying that you can say use the term 'red rag'; but there is a very serious incident that has occurred there that apparently was referred to an ombudsman. I do not want to prejudge the outcome, but I would be careful about what you said in terms of that.

Mr Dickson: All I am saying is that we do have a process of audit in place.

Mr Byrne: Sure.

Mr Ruddock: Describe 'senior police officer'.

Mr Dickson: It is inspector or above.
Mr Lanyon: It is the same in New South Wales, Mr Ruddock.

Mr RUDDOCK: Do they have particular qualifications, or is it just any inspector?

Mr Dickson: You are quite right, it is any inspector, but the ultimate decisionmaker is the superintendent in charge of our ISP who is ultimately in charge of our TI section.

Mr NIKOLIC: Did you have anything to add, Assistant Commissioner Lanyon?

Mr Lanyon: Just quickly, if I can I would liken metadata more to intelligence purposes, generally it will commence an investigation, we would look for the metadata. It would be very difficult to found an application for a warrant for the basis of metadata to start a investigation because we really do not necessarily know what we are looking for. If I had been murdered, the first thing we would do is to look at my phone to see who had contacted me, who I had been in contact with and to look for persons who potentially could have been contacted. It would be impossible from an investigative perspective to identify what we were seeking to get out of that telephone data, who we thought the contact would be between when it is clearly an intelligence touch point to start with. And probably just to support again, for the 122,000 applications last year, the operational impact on the time delay in investigating matters, and certainly the first 24 hours in a homicide investigation is critical, a significant time delay to go under a warrant regime would significantly impact on both the effectiveness and certainly the efficiency of criminal investigations.

Mr NIKOLIC: thank you, if I have the figures right and if I have copied them down quickly, Assistant Commissioner an end to you talked about 122,000 requests, of which 4358 requests were greater than two years and Assistant Commissioner Dixon you talked about, in the last five years, 17,000 requests, of which 60 percent were older than 12 months. One of the features of evidence presented to this committee, using overseas research information in particular, is that this is some sort of quantitative consideration because such a small number are longer than 12 months, ago they are less important. Clearly, those ratios do not apply as far as South Australia Police are concerned. Do I take it from your comments that the 4,358 cases in New South Wales older than two years and the 60 per cent in South Australia older than 12 months were complex cases or people reporting crime like sexual crime well after the event? Can you give me an insight there?

Mr Dickson: From the South Australian perspective, I think it is a bit of both. It would be complicated matters where you may not have a suspect for a long period of time, especially within some of the OMCG type investigations where it is very difficult to get people to talk to you because of extortion and those sorts of things. What happens is your suspect might come up 12 months or 18 months into the investigation and that is the time that you need to get this level of detail which we are talking about. That is probably one of the main reasons. It is around when we identify who the suspect is. So that is one issue. Then it is also about the complexity of the matter as well. You may have a rape investigation where, again, the suspect becomes known quite a long time after the event, or it might be historical sex offending where the young person who is the victim of the matter reports two years after the matter. You then have to try to go back two years for investigative purposes. So all those difficulties are there, but the detail that is provided is gold for the investigator.

Mr Lanyon: It is a similar position with New South Wales offences. As I indicated, murder, sexual assault and robberies were the key offences for which those 4,350 were requested. Again, they are often historical. We have had a number of royal commissions and commissions of inquiry into child sexual offences. So there have been a lot of reports for which a suspect was never known and an offence was never know up to a certain period. We have an unsolved homicide squad in New South Wales and we have approximately 650 unsolved homicides for which, as you work through, suspects are often unearthed by advances in forensic science and by changes to information provided by source. The ability to then go to metadata to confirm and corroborate is absolutely essential.

Mr NIKOLIC: Can I deal with the issue of responsiveness. You have described what I can only picture in my mind as a Sara Lee approach to oversight. You have talked about some oversight at the tactical level within your own individual organisations—an inspector making a recommendation; ultimately, someone at the top of the organisation deciding you would seek metadata. There are Ombudsman processes and there are privacy principles being applied and . Then, nationally, if you look at it, you have Ombudsman and IGIS and this committee. As that relates to responsiveness, can you give me a sense in the early stages of an investigation where you have said metadata is important?

Mr Lanyon: Essential.

Mr NIKOLIC: You mentioned you being killed. To what extent do existing processes allow you to be responsive? Do you consider them about right? Do you think they slow you down? Give me a sense of what these layers of oversight do on your ability to do your job?
Mr Lanyon: I would say the balance at the moment is quite appropriate in terms of metadata. As I said, internally there are checkpoints that we need to go through to get there. There is external oversight—and I can have Superintendent Kopsias talk in terms of the telecommunications interception act and Ombudsman, Commonwealth and state, overseeing. In the initial stages of an investigation, it is really about gathering information as quickly as we can so we can try to narrow down suspects, try to identify communications and found the investigation and the direction we are going to go with it. If a significant layer of bureaucracy is put on top of that, that will significantly impede investigations. I would think that they are appropriate, and I certainly take note of Mr Byrne's comments before. But when you look at the significant number of inquiries that are made for metadata each year and the way that they are handled compared to the response we do get from both the state and Commonwealth Ombudsman, I think we have the processes very appropriate.

Mr Dickson: I fully support those comments of the New South Wales Police. Also, I think it would be very difficult from the initial part of that murder investigation to actually get the detail to obtain a warrant to get that metadata. Often you have quite a cold scene and it is very difficult to have any information, so you have to work through that. This is an investigative tool which provides us with intelligence and that is all it is at that point in time: intelligence to give the investigators some lines of inquiry. Then at a subsequent time that may turn into evidence. But it may not; it might just be the intelligence which allows us to move forward.

Insp. Segrave: The Victoria Police endorse that as well. I alluded in my opening to what could be characterised as the potential for unintended consequences around this idea that there needs to be a judicial authority for the access to metadata. I would like to reinforce that point, and it has been raised by other witnesses before you. If we were to move to that type of regime, one of the questions that arises is: what would be available at that point of an investigation to put in an application to be made before a judicial authority for that type of warrant? The reality is that, if you look at where metadata is normally accessed in the course of an investigation, quite often the answer is not a lot. So, if the view is taken that a particular target is worthy of further focus in relation to that issue, you need to deploy other resources that are effectively more intrusive, I would suggest, than obtaining the metadata—for example, physical surveillance, human source or, potentially, undercover operatives. I think on any assessment that type of approach would have to be considered to be more intrusive than the accessing of the metadata. I think that is a worthwhile point for the committee to consider as well.

Det. Supt. Kopsias: From a New South Wales Police Force prospective, the volume of our metadata requests if we put a warrant regime on top of the metadata scheme would—I will make a bold statement—virtually cripple our organisational capacity to effectively deal with organised crime and serious crime. I would make that statement to you. It is not just responding during business hours; it is also after hours. We respond to kidnappings and other serious crime after hours and on weekends. You would need after-hours people to do that type of work. Just the sheer volume of metadata and TI requests would hamper our investigative capacity.

In terms of oversight, I do not think a warrant scheme would add more to due diligence and to the accountability and oversight process currently in place at the moment. As Mr Lanyon told you, we have enough internal processes and accountability schemes in place to ensure governance and equitable practices are adhered to at all times in compliance with the legislative practices that we adhere to.

The enormous, I suppose, intent of our investigative charter does differ from Commonwealth law enforcement agencies, and this is why we are fairly unique. If I could paint a picture of our need to retain data for longer than two years, we have an unsolved homicide unit with 650 cases on its books right now. Pre-1960, we have 12 cases; from 1960 to 1969, we have 15 cases; from 1970 to 1979, we have 80 cases; from 1980 to 1989, we have 150 cases; from 1990 to 1999, we have 210 cases; and, 2000 to 2009, we have 120 cases. At any given time, a particular investigation would need some sort of metadata once it is activated. We would need some sort of metadata to get the process on foot, start the investigation process and then work out whether we need other resources, electronic evidence or physical surveillance to enhance that investigative capability. So, without it, we would be hampered, but on top of that we also have a royal commission into child abuse right now. We have provided that body with 191 cases—referrals. At any given time, they would need to access metadata. Again, those cases go back to pre-1950.

I am not saying we need a scheme that would need to hold records back to 1950, but certainly we need a scheme of longer than two years. Whether it is more than two years or seven years, I am not too sure, but right now we can access CCRs and reverse CCRs with particular carriers or, actually, across all three carriers for up to seven years. Certainly, from our perspective we would not like to go backwards. We would like to keep the current scheme in place in terms of those particular datasets, but we do support in principle a data retention scheme to consistently standardised this process.
Mr NIKOLIC: What do you say to those concerns expressed to this committee that this is potentially an unacceptable intrusion into the lives of 23 million people? As I hear you talk about your operations at the tactical level, it is about a quick skim across a large dataset to understand connections between individuals and networks, which might then lead you to areas of further inquiry rather than a deep dive. I have heard evidence that metadata could be used to listen to journos talking to their sources or to see what clubs people are frequenting. It seems to be inconsistent with the sorts of examples that you are painting to the committee.

Mr Lanyon: With cell site location that we would normally get with metadata, we would talk about an area, for example if I am in Canberra I might be in Deakin or I might be somewhere—it does not specify. There is not the amount of specificity to say that I am in a particular place. We are talking more about gross data. The data does certainly assist us in terms of time, date and place. It gives an idea of who has been speaking to each other. It is absolutely essential. In terms of privacy, I would think most members of the public would expect that there are billing records kept in relation to their mobile phones. I think most people would be astounded to believe that that was not the case, and I think that most people would certainly expect that if a criminal offence had been committed the police would be able to access that data to assist. Again I was very specific before when I said that we are not talking about content. There is quite rightly a warrant regime around that. It is a limited intrusion but a very valuable investigative tool, and I think that if you look at a comparative weight then certainly the public would see the weight of being able to solve crimes higher than the potential intrusion that we are talking about.

Mr Dickson: I support that. As we all know, it is about balance. It is about a balance between privacy and the ability to protect the community. I think the balance is about right, where it is at the moment.

Insp. Segrave: From a policing agency point of view, we are talking about finite resources and an expectation that those resources are targeted where they can achieve the most good. It is just not open to agencies to engage in the sort of activities, routinely, that perhaps some of the commentary suggests. Where that does occur I would suggest that it is generally going to be within the purview of misconduct, and there is a whole regime of legislation and process around that particular aspect of police misconduct.

Senator FAWCETT: Assistant Commissioner Dickson, could I also take you to the table you have provided in your reply to questions on notice which indicates that, pretty consistently over the last five years, over 60 per cent of your requests have been more than 12 months old. Does that apply predominantly to telephone information or do you also deal with IP addresses in terms of internet communication?

Mr Dickson: It is everything. It includes IP addresses, it includes cell dumps, it includes CCR and reverse CCR. We do not calculate it by particular type of metadata, so that is the entire time out. From my experience the greatest amount would be CCR kicks and reverse CCR, because as an investigator what you would need to know is: who has that person been in contact with, or who has contacted them—especially around the issues of serious assaults, murders, drug trafficking and those sorts of offences where it is very important to have an understanding of the criminal network and the nexus between different parties.

Obviously with that there would be a lot of work also around live CADs and those sorts of things, where you need to track someone. From that perspective that would be a minority. Most of them would be around the CCR kicks.

Senator FAWCETT: We have had a number of witnesses use the examples that have been provided to us by law enforcement agencies where metadata has successfully led to a prosecution and they argue that the existing system is working and therefore no change is required. Again I would take you to your case studies, where there was a murder and four days after the murder you put a request in. The particular carrier kept data for only seven days; and, in that case, you resolved the case and you successfully prosecuted. But you then go on to quote a case later where again, a fairly short period after the event, you put a request in but the data was not available. How frequent are those events where you only just get it in time or, in fact, you request and it is not there? The reason this is important is because it demonstrates the fact that the existing system is not sufficient in many cases.

Mr Dickson: There are a significant number of investigations where, because different carriers keep data for different periods of time, it is a bit hit and miss from an investigator's perspective as to whether you are with Optus, Telstra or Vodaphone, because they all have different lengths of time that they keep that metadata for.

Going back to your question, there are a number of examples of where I have heard investigators talk about the fact that they put in a request for metadata but were not able to receive it, which impacted on their investigations in that if that metadata had been available it would have assisted them. I go back to my opening statement. The main issue I see here is the importance of it for law enforcement. To have a consistency of approach is very important for us, because then we will know what the period of time is that that metadata is going to be stored for.
Mr Lanyon: I support that. I think I spoke in my opening remarks as well about IP data that we had requested in New South Wales last year. There were only about 1,100 requests, of which conservatively 80 per cent failed to yield a subscriber from the other end because, without the legislation, carriers are not required to keep the proposed datasets.

Similarly, on metadata call charge records, investigators get very skilled at knowing which carriers they can get data from and which they cannot. They know very well, so the level of requests that go to carrier A, knowing that they only hold that data for four to six weeks, is obviously reduced. There is no point putting a request in if we know the carrier does not hold the data for that long. I think the issue of consistency that we have all spoken about here today is the central key here and the reason why the bill is supported by the jurisdictions. It is because it is essential that there is confidence that carriers are holding information for a particular period of time. We have indicated that obviously we would like it to be for longer, but it is essential that it is held for a standard period of time and that, again, there are consistent datasets so that investigators and certainly law enforcement can be assured that they can get particular information which is relevant to investigate criminal offences.

Senator FAWCETT: This is, again, for SA Police. There was a discussion in your paper that in the five annual reports it is indicated that 146 convictions utilised telecommunications information.

Mr Dickson: Again, that is not just metadata; that is TI information, content information and those sorts of things. It is a very difficult question to answer. In jury matters, it is difficult to know why a jury found a person guilty, as an example. Was it because of the metadata provided? Was it because of certain admissions made? Or was it because of the DNA evidence? It is very difficult to say that metadata was the reason that that person was convicted. Most convictions at the end of the day are because of a whole raft of different things and bits of evidence.

Insp. Segrave: I will make another point there, if I may. The metadata, quite often, is a step in the process for the investigator to get an evidentiary footing. Without the metadata, that evidentiary footing may never be achieved. But it is not actually represented or recognised in the brief of evidence that is put before a court. So it can be very hard to drill down into the brief and into the prosecution to have an understanding of the underlying role that metadata actually plays. But I think law enforcement consistently are saying that, with our understanding of the investigatory process and the application of metadata within that process routinely, it is critical to us.

Det. Supt Kopsias: I will also just add to that. It is hard to quantify. We do not keep a central repository of the effectiveness of metadata, especially involving court outcomes. In our submission, which I hope you will be able to read today, we gauged it as well as we could to parallel the effectiveness of TI because we capture that data annually for the AGD in an annual report questionnaire. We have done that quite well over the years because we have a database and a process for it. I can tell you that over the past four years where we have used metadata and TI they have coexisted. Neither will survive without the other. The best we could come up with is that we had a total of 7,343 interception warrants issued which contributed to 5,093 arrests, 14,016 prosecutions and 5,064 convictions. We are not saying they were directly attributable, but there was some value, some effectiveness or some evidence given in those court proceedings in relation to metadata, including TI. So we are saying, ‘Yes, it is effective. It is a building block. Without it, TI and other electronic surveillance resources that we use would not exist today.’

Insp. Segrave: In relation to that, if we were to move to a judicial warrant situation for metadata, one of the things I think it would throw up in terms of an anomaly is that telecommunications interception warrants, by definition, require metadata within the applications—and quite a deal of metadata—to substantiate the application. We would effectively be moving to a situation where, in a lot of instances, we would need a warrant to obtain the information that we would need to obtain the warrant. I think that would raise a whole range of issues as well.

CHAIR: That is a very good point.

Mr CLARE: With reference to the submission of the NSW Police that was available, it was sitting on our desks here and then it was taken away from us. I am wondering whether the police can authorise us to read your submission or whether we have to wait for the approval of the New South Wales government.

Mr Lanyon: You most certainly can certainly have it now, Mr Clare. I am told it has been officially released to the committee and it is available for you.

Mr CLARE: If that is the case then we might ask the staff of the secretariat to allow us to read the submission. The argument is being put to us that this is urgent and that this legislation needs to be passed and implemented very quickly. Evidence has been given to us by Telstra, Optus and Vodafone that, in regard to the data they hold at the moment for set periods of time, they have no intention of changing the time periods that they
hold that data for. In evidence today, law enforcement has said that they are concerned about the degrading of access to this data. I am interested in whether you can expand on and explain what your concern is and why you think this is urgent.

**Mr Lanyon:** I have several concerns. We certainly get a good deal of cooperation from the carriers; however, they are a commercial entity. One of my concerns with an unintended consequence—and certainly a consequence at the moment—is reverse call charge records. I think I indicated in early evidence that it varies between carriers: carrier A may have seven years and carrier B may have six to eight weeks. Consumer protection is the primary reason that the carriers hold that information, and that relates to billing of customers. There is no billing advantage for a carrier to hold reverse call charge records as it is simply calls in to their service. There is nothing to stop a carrier at any stage—for commercial interests, for the reasons of storage or for the reasons of hardware—from deciding that they are no longer going to hold that there. Without legislation, there is nothing to stop a commercial interest. There are already variances between carriers in terms of what they hold, so there is nothing to stop one making a decision one way and another making a decision another way.

**Mr CLARE:** Is that the nub of your concern—that it is more an issue of consistency of the length for which ISPs hold data, rather than a shift in ISP behaviour and the degradation of access to this data because ISPs are now holding the data for shorter periods of time?

**Mr Lanyon:** I certainly think consistency has been the main message from each of us this morning, but certainly the dataset is equally important—that the carriers are holding the same data which is relevant to criminal investigations.

**Mr CLARE:** So the same data and for the same period of time.

**Mr Lanyon:** Certainly.

**Mr CLARE:** Is it a concern to law enforcement that this legislation, when passed, would not come into effect until two years after that legislation is passed and proclaimed?

**Mr Lanyon:** I think so. We currently operate within an unregulated regime. As you are aware, we exist on the assistance provided by the carriers. We would like to have something in place to ensure that we have consistency and can actually obtain those records when we need to. A regime put in place would certainly be preferable to us, and that would be the reason, I would say, for urgency. By the same token, I think it is very important to all of law enforcement that we get those processes right. We understand that there are industry concerns, and we certainly understand that there are privacy concerns. From a law enforcement perspective, we will certainly push our barrow, but we do understand that there are other things that need to be considered in that process. The faster we could get a regime in place to enshrine what is going to be kept, how it is going to be kept and for how long it is going to be kept, and we have some consistency across the process, that will benefit all law enforcement agencies.

**Mr CLARE:** But you are not making a submission to this committee that we should truncate the implementation period? You recognise that, from the date the legislation is passed and proclaimed, it is another two years before this regime would come into effect, and that is something that law enforcement could live with?

**Mr Lanyon:** Obviously the sooner we have it the better, but I will take on board the submission that you have indicated the telecommunications industry has given—that they do not intend to change the information that they currently provide to law enforcement—as some reassurance that we will continue to get that information in the short term.

**Mr CLARE:** To be fair—maybe just to expand on that and then ask the superintendent to comment—that is the feedback from the major telcos. We have not had all of the telcos, big and small, come through and give advice to this committee. But the advice from Optus, Telstra and Vodafone is that they are intending to hold data for the same length of time they currently do. My question to South Australia, Victoria and New South Wales is that, at the moment, the legislation this committee is considering, and that the parliament would consider, once passed and proclaimed would not become operational for two years, and given that law enforcement, particularly federal law-enforcement agencies, have told us that this is urgent, I am wondering if you want to make recommendations to this committee that that period should be truncated, otherwise the inference this committee will take is that that two-year period is okay.

**Mr Dickson:** From the South Australian perspective, where we are going here is that if from, say, 1 July this year this legislation came into place, my view, and what I would be seeking, is that from that point in time data was kept, as best as could be, for two years previously. That is the magic number we are going to come with. Some telcos will not be able to comply with that because they have already destroyed it after six months, or whatever, and that is fine. We just have to live with that because there is nothing we can do about it. But, then,
have that as the practice moving forward, so that in two years' time you will have all data at least two years old. That would be my recommendation to the committee.

**Mr Lanyon:** As well, I think the importance of why we would like to have this in place as soon as possible is as you have indicated: the major carriers may indicate something but the minor providers, completely unregulated, provide what they like, and store what they like and hold it for as little time as possible. So it is a matter of the sooner we have that sort of surety in place. I agree with Mr Dickson.

**Mr Kopsias:** I not too sure if a certain matter concerning a customer billing record and a record that is currently accessed by law enforcement has been clarified with the committee. Take, for example, a call charge record. The customer's records are different to what we as law-enforcement personnel get for call charge records—and reverse call charge records. It is probably about two-thirds. We will not be getting a replica call charge record under an exemption if we call it like the bill has, where the carrier would keep those records for customer billing and ATO purposes. This is why it is important that a regime is put in place that standardises, and we get exactly what we get today. We get a location—where the person who made the phone call called from. With certain carriers we get the B-party location, too. We get time and dates. We get an IMEI number—a unique identifier. Sometimes we actually get a little sample from particular carriers saying that there is picture here or an SMS—it does not tell us what it is—which prompts us to get a stored comms warrant, or another process. What we are saying is that the current CCRs and reverse CCRs we get are vital to our criminal investigation process. Going back and accessing traditional customer billing records probably will not suffice.

**Mr Lanyon** think that probably again builds on the question that you asked before. After two years, as this bill proposes, there is not a requirement, and carriers are entitled to keep records, as they would normally do. Obviously, consumer protection would require that. The reason that New South Wales has asked for that period of two years, particularly with call charge records and reverse call charge records and subscriber checks to be longer than that period is that there is nothing to stop a service provider keeping for commercial purposes what are only billing records, after two years. At the moment, for seven years we get what I would call law-enforcement records. So we will have a number of pieces of data. After two years, according to the bill, the carriers are entitled to keep information, obviously as they would under consumer protection. That level of information is not at the same detail as that which we would currently get. If it were cheaper to store it that way there would be a commercial reason why a carrier would not want to do that. That is one of the main concerns I raised earlier in terms of the two-year period.

**Mr CLARE:** You made the point in evidence that you think the two-year period, as defined in the bill, is insufficient and should be well in excess of two years. Could you explain for how long you think data should be retained.

**Mr Lanyon:** When my commissioner gave evidence in front of this committee, probably in 2012, I think he indicated that it should be for as long as possible, up to seven years, which we currently have. I did not want to prescribe a number, but we have it for seven years at the moment. We still run into a problem with that but at least if we had that data. Call charge records and reverse call charge records and subscriber details to my mind are not intrusive records. To introduce a bill that would go to two years and the allow carriers to keep records only as they see fit, or as required by consumer protection laws, would downgrade what law enforcement currently has, which is a retrograde step that I certainly do not support and New South Wales cannot support.

We make a significant number of requests for metadata. Currently we are fortunate to get that back for seven years. If we went to a two-year regime and then had less data provided from that point on that would obviously significantly impact our investigations.

**Mr CLARE:** Can I ask South Australia and Victoria whether you support two years or seven years, or something in between?

**Mr Segrave:** We certainly endorse a longer period, for similar reasons. Again, I endorse the view that access to these records is not anywhere near as intrusive as actual communications. I reiterate the points I made earlier in relation to the importance of this material being available in the course of the early stages of most investigations.

If we are looking at an investigation that may be afoot three, four, five or six years after a communication, almost invariably it is going to be an investigation of great significance. Law enforcement is not going to take on an investigation for an incident that occurred that long ago, unless it is a homicide, a sex crime, a crime of significant personal violence, a counterterrorism inquiry or something of that nature.

The other point I would make, and I think it has already been borne out in other evidence before you, is that the reality is that the bulk of these types of inquiries are made when this data is relatively new. Minimal inquiries are made further out. But, again, they are ones that pertain to investigations that are probably of greater import.
Mr Kopsias: For the committee's recommendation, and to perhaps clarify that this is not just rhetoric, we have records on our books at the moment that justify data in excess of five years. Whilst they are minimal, as Mr Lanyon alluded to—minimal in terms of the volume of requests that are handled up-front in the first six to 12 months—we have nearly 1,000 cases involving most serious fraud, unsolved homicides, historical sexual assaults, and a lot of clear-up armed robberies. They are fairly complex crimes in that batch. Those crimes, we can justify, are five years plus. Whether they are five, six, seven, eight or nine, I am not sure, but certainly we get to the five-year mark.

Mr CLARE: So is it arguable that seven years is not enough.

Mr Kopsias: All I can say is, the longer the better. But we would not want to being going backwards from what we are accessing today.

Mr Dickson: I support both my Victorian and New South Wales colleagues on this. I think the issue is that we do not want to go backwards. At the moment we have the ability to obtain CCR records from seven years ago. If we go to two years, from an investigative perspective that is a retrograde step, especially when you are dealing with more and more historical offences, be they murders or historical sex offences, which do require that information. All of us around the table here would understand that the reliance on and use of electronic devices such as those we are talking about is not going to go away. It is increasing. So we will become more and more reliant on this sort of technology in the future.

Mr CLARE: Have you brought your concerns about this to the attention of the federal government or the Attorney-General's Department? If your argument about the CCR data, which you can currently access for seven years, is that this legislation will in effect reduce your access to that data, have you brought this to the attention of the Attorney-General's Department?

Mr Kopsias: I have, in my capacity as a delegate before the Interception Consultative Committee meetings we attend, and national TI forums. It has been brought up over the last three or four years that our desire was for a longer retention period. We made it quite known to A-GD and other delegates at that forum. Whilst some of the agencies had differing views, which were respected, we always were of the view that we wanted a longer retention period.

Mr CLARE: And there was no feedback about how that concern might be addressed in this legislation?

Det. Supt Kopsias: No, I cannot say that.

Mr Lanyon: Previous submissions have been called for, as you are aware, over the previous few years in relation to changes to the redrafting of the TI Act. The New South Wales position has always been consistent in terms of the seven years.

Mr CLARE: If I understand what your evidence is, you are saying that, unless this issue is addressed in this legislation, it could reduce the access that you currently have.

Mr Lanyon: Correct.

Mr CLARE: So this is a fairly serious issue. What you are saying is that this legislation could reduce the effectiveness of your law enforcement capabilities unless it is fixed?

Mr Lanyon: Correct.

Det. Supt Kopsias: Correct.

Mr CLARE: So this is a major hole in the legislation that needs to be addressed, is that correct?

Mr Lanyon: That is correct.

Det. Supt Kopsias: Just for the record—and I am not too sure if it has been raised by other agencies or delegates—when a court proceeding comes up, whether it is a trial, a hearing or a committal, somewhere down the track, whether it is two, three, four or five years, we get requests from the DPP and from the defence in terms of alibis, in terms of checking out a particular witness's statement, a particular location or a particular subscriber. So we get after the fact type requests for metadata. I cannot quantify that right now, but I am trying to. We do get requests from the DPP and there is an expectation that we can access data that is two, three, for five years old. And that is what we are doing today. We are able to access the data today. Under the current regime, if the legislation is enacted in its current form we will be hampered. We will not have the same unrestricted rights that we have today.

Senator FAWCETT: I want to clarify something. My understanding is that the intent of this bill is to put in a common data set and a common mandatory detention period of two years. Those who currently retain data for up to seven years do so because of their own business practice. The passage of this bill, we have heard from telcos,
will not make them change their business practice in terms of reducing things necessarily. As they have indicated, that may be more expensive than continuing to retain the data. So the passage of this bill will not in itself reduce that period. It will only be if they decide they are going to upgrade their systems and it is more economical to no longer retain seven years. They may do that in the future. All we are doing is putting in a floor and saying that, as a minimum, you must retain two years of data. But that is not going to force or, indeed, encourage anyone to reduce from the seven years they already have.

Det. Supt Kopsias: But there is no guarantee they will keep those records in the current form. As we move to an internet based regime, with the introduction of the internet, national broadband and 4G, carriers and ISPs are changing their billing processes to bulk-billing their receipting data, as distinct from who called whom and from where. In terms of those unique identifiers that we are getting today, I think we will be hampered down the track because we will not be getting those same records.

Senator FAWCETT: I understand that, but my point is that that is a function of changing business practice and changing technology, not a function of this bill. The only way this bill would achieve the outcome you are looking for is if we say that seven years is the period we will mandate that the data has to be retained for. But the bill itself will not actually bring about what you are saying.

Mr Lanyon: As I think I said before, that is what we call an unintended consequence. If we mandate—and, again, that is a matter for government to decide—two years as the period, you are then basically saying to carriers that we expect them to comply with this for two years. There is nothing to stop them from maintaining records after that. If you put a compliance burden on at the start, and there is a cost at the end, it is only logical, with commercial interests, that there is a reason why you would want to do that. I agree with you 100 per cent that the bill itself does not do that, but I would ask the committee to consider that that is a consequence of the bill and certainly one that would be negative, certainly for New South Wales and other law enforcement agencies.

CHAIR: Just to clarify that: it is an informal arrangement at the moment that gives you access to the seven years? There is no formal legal arrangement that requires you to do that?

Det. Supt Kopsias: It is just a practice that we have in place—whether it is an MOU or an agreement. There is no legislative basis for the current arrangements. It is purely based on commercial agency—

Mr DREYFUS: You seek access from telecommunications providers, to telecommunications data, under the Telecommunications Interception and Access Act. It is a warrantless regime. In what sense is that informal?

Det. Supt Kopsias: It is informal because it does not set a time frame. Under the Telecommunications Act they provide reasonable assistance to us—whether that is in telco data, a TI process or some other form of data—but there is no retention period defined anywhere.

Mr Lanyon: There is no retention, there is no dataset.

Mr DREYFUS: That is good. I just want to clarify this. So you are not suggesting it is informal that when you seek access from—


Mr DREYFUS: Perhaps we can put the term 'informal' to one side. There is no presently legislated requirement—not formal or informal, there is no requirement at present—that imposes any obligation on any of the 600 service providers to keep any data at all?

Mr Lanyon: That is correct.

Mr DREYFUS: Right. So that is not a matter of informal or formal; there simply is not a law of Australia which requires them to keep data?

Det. Supt. Kopsias: To correct the record, I never alluded to 'informal'. That was raised by someone else.

Mr DREYFUS: I know. I am trying to clarify with you because you are here before us.

Mr Lanyon: There is under consumer protection legislation—

Mr DREYFUS: Sure. There are other—

Det. Supt. Kopsias: There are obligations on the carriers to retain data for us but there is no retention period defined anywhere in the legislation.

Mr DREYFUS: Other than that, as the assistant commissioner has very correctly pointed out to, there might be in other legislation such as in the consumer protection code under the communications ministries legislation, which is one reason why some of this data exists.
Senator FAWCETT: Can I also clarify with SAPOL: on the basis of your verbal evidence and your written submission, some telcos get rid of the data you need within seven days. So in fact this bill would at least establish a base line of two years, which is a step ahead of where you are at the moment, with some providers.

Mr Dickson: You are 100 per cent correct, yes, and the two years would be far better than what we have today from the policing perspective and especially from SAPOL's perspective. I think the discussion we are now moving to is that this practice and considering where at the moment we can get information which is a lot older than that. So it is really about a decision for government to make a determination as to where that number is. I fully accept that two years would be great, but is that the best is a decision we are now having discussion about.

Senator FAWCETT: Two years is not as good as the best of the current crop but it is a lot better than many of the current crop.

Mr Dickson: I agree 100 per cent.

Mr NIKOLIC: Are you arguing for a no-detriment clause to exist in practices? I think the bill currently contains a no-detriment clause from the time it is passed to the time it is implemented. Are you arguing for an extension of that to say that these favourable existing arrangements you would be seeking to preserve to the extent you were able?

Mr Dickson: I think the only difficulty with that is that different telco providers have differing regimes. So telco A may have seven years and telco B may have four years, six weeks or 14 days. That would be quite problematic to do what you—

Mr NIKOLIC: But would you need to standardise? Would you say that in grandfathering existing arrangements, which you find favourable for a variety of purposes, given what they do now which is inconsistent, that that aspect of it would not need to be standardise?

Mr Dickson: Yes, you could consider that.

Mr CLARE: Maybe I can assist. My understanding is that under the TCP Code there are obligations on certain telcos to hold certain data to six years. Is that right?

Mr Lanyon: You ask that question before and what I have tried to explain is that there is a difference between what I will call a customer billing record and a law enforcement record. Under the consumer protection, they are required to hold customer billing information obviously for a consumer issue. That is very different from what we currently get. My concern is that, if we went to two years holding the dataset we are asking for and then carriers are required to hold, as they are required under other legislation for an extended period, the current level of information we get and the current level of specificity in it we could lose. There is no reason why a carrier for commercial interests could decide not to hold the same level of information or data. That was my concern.

Mr BYRNE: Would you then seek a data preservation order on data currently held by the telcos, what they have at the moment? I hear what you are saying, that you are worried they will whack out the information they have, which might specifically be tailored for you. Are you saying that what you are worried about is that they will destroy that data in setting up their system so that you will not be able to access it almost retrospectively?

Mr Lanyon: No. I think we would be talking about a future period where, if there were a cost or a burden applied by having a two-year period, there was an opportunity commercially. If the bill only specifies 'hold records as required' there is nothing to stop you holding records after that period. There is consumer protection legislation which requires only minimal information to be held. My concern is that practices could change to reduce the level of information we currently receive.

Mr BYRNE: What I am saying is that the telcos are saying that it imposes some cost. Notwithstanding what you have just said about legislation, you are obviously getting metadata outside of that that is useful. That aspect of the metadata that you are seeking could then become not accessible to you if they start implementing this data retention scheme.

Mr Lanyon: No, not immediately, because the datasets proposed by the data retention scheme would cover the two years. They would be required to hold it for that period. Outside that two-year period, there would be no requirement—
Mr BYRNE: But you said you are going back seven years at the present time, so you will be losing some form of—

Mr Lanyon: Absolutely. If they decide to make a decision at that stage that they will only hold billing records—strict billing records as opposed to law enforcement records—yes, there is an obvious risk that we could lose that information.

Mr CLARE: You gave a very good example of the use of metadata with respect to a murder and then checking someone's phone records to identify who they have been speaking to. I am just interested in getting the views of law enforcement about the importance of web browsing—what websites people might have clicked on, for example.

Mr Dickson: My understanding is that it is not suggested under the bill. I certainly support that. Again, it goes back to the principle. The information is about time and place of contact as opposed to what is actually in the contact. I think you are now moving into the content of that communication. While you could argue that sometimes it would be good to have that, there are other opportunities you may have to get to that information through a warrant and those sorts of things.

Mr CLARE: But would that not be of interest to law enforcement? You would not want to know—

Mr Dickson: I think it is about where the balance is. I think the balance is, at this point in time, the metadata. We are now talking about privacy principles. If we were to have access to all the web browsing at an IP address, I would say that we had moved not a step too far but certainly a lot further than what the bill is about. I think at this point in time it is important to keep to what the bill is seeking as opposed to the actual content of the communications. It is about the metadata to get information as opposed to getting the content of communications. I think your question is going towards the content of communications.

Mr CLARE: I am just trying to understand how the law can assist law enforcement. You gave the example of being able to check the records and see who that person rang before they died. I would have thought that law enforcement would also want to have a look at what website they might have clicked on. That might help them to work out where they need to go to investigate the murder.

Det. Supt Kopsias: That is important, from our perspective, but at the moment that is content. It is defined as content. The other problem is that when people are using smart phones out there it is hard to get IP addresses because the carriers do not keep records. That is because external IP addresses are handed out and they roam from phone to phone. They do not collect that data. You can go to wi-fi hotspots. Telstra are actually rolling out certain hi-fi areas where you can go and log into your account and virtually remain anonymous because we cannot trace your IP address. Your IP address is actually traced back to your computer, not to your smart phone. So we have a gap there in the process that we are trying to tidy up. That explains the business about going dark in the cloud and the encryption problem we are having with over-the-top applications. That is affecting our metadata and interception capability to identify who is using a particular service at a particular time at a particular location. These things are important, yes.

Mr CLARE: Is this power something that you would like to see in the legislation?

Det. Supt Kopsias: I would have thought with the reform process and the comprehensive review of the T(IA) Act that the data and the T(IA) Act would perhaps merge into one proceeding, otherwise down the track we might be doing this again. I was just saying this to my boss. I said, 'We might be doing this again in 12 months in relation to the TI review.' There would be similar practices and issues we would be raising before a similar committee because they go hand in hand. Metadata and TI coexist. They are interlinked. The metadata will fall under the T(IA) legislative regime as it stands anyway. It always has. I apologise, but to me it does not make sense to be having separate proceedings, but I do respect these proceedings.

Mr CLARE: There is logic to that. You could argue that we are putting the cart before the horse because we are doing metadata before TI. I am just trying to get a sense from state law enforcement about, in this piece of legislation which does not include web browsing, whether that is an issue from your point of view and whether that is the sort of thing you think should be addressed in the future.

Insp. Segrave: From a Victoria Police point of view, if we were to look at this solely from a law enforcement perspective without considering all the surrounding issues which obviously this committee and the community more broadly need to consider, the answer would probably be, 'Yes, we need that. That is fantastic.' But, like all other stakeholders in these proceedings, we need to bring a degree of pragmatism to these discussions. As South Australia Police have already alluded to, we acknowledge the tensions between law enforcement and privacy. We understand the need to try to find a balance. I think the view of the Victoria Police would be that, although that is something that would be very nice to have and very beneficial, if it raises a level of concern in the community.
around the bill and the proposed regime generally we are prepared to say we can live with the proposed arrangements and do the best we can under that regime.

**Mr Lanyon:** I appreciate your question. We have been talking about data retention today and one of the key points that we have all made is that we wish to retain what we currently have. For us, that is certainly a step along the line. Certainly in any reform of the T(IA) that is something that we would like to consider. In terms of data retention, it is more important for law enforcement that we are actually able to retain what we currently have so that we can facilitate our criminal investigations. Down the track, that is certainly something we would like to look at. I could give a wish list of things that would be outstanding for law enforcement but obviously would be very difficult for other parts of the industry and would impact on privacy. I think it is most important that we stay, from a law enforcement perspective, in the game—and that is that we really want to be able to retain what we currently have and ensure that we have consistency across the board with carriers and providers so that we can best carry out the investigations we are charged with.

**Mr Dickson:** Just on that, the information that you are talking about we can gather through a warrant. So it is not as if we cannot get it. We can get it if we go through the warrant process which is appropriate in the circumstance. I think it is all about balance, as the others have said.

**Mr CLARE:** Detective Superintendent, you mentioned the issue of going dark and also wi-fi in public places and the current problem that creates for law enforcement. This is an issue that my colleague Mr Ruddock has raised in the examination of a number of witnesses. It came up most particularly yesterday from the Australian chapter of the Internet Society. In their evidence they expressed a concern about this. They talked particularly about municipal wi-fi networks in public libraries, airports and public rail networks and indicated that this is a potential big loophole in the legislation that creates an opportunity for people that you might be seeking to investigate to go dark to avoid detection. Can you just expand upon that from a law enforcement perspective for me.

**Det. Supt Kopsias:** It is a pretty broad topic but it is also very close to my heart as I have been the TI commander for 15 years. I have been doing interceptions for 15 years. I have managed thousands and thousands of intercepts. But, in the last four or five years, the phrase 'going dark' has come about in terms of the strong encryption out there, lots of over-the-top providers providing apps, the online process. The advent of the internet, if I could explain it to you, has actually degraded our interception capability to the point where we are receiving a lot less than we used to receive.

When I went to the TIB, I used to apply for the warrants. I used to go before Federal Court judges; in those days, we did not have AAT members. I used to go down with a request for the warrant, the same warrant that is served today, and present it before the member, present our case with the affidavit, come back with a warrant and serve it on the carrier. In those days, we had the luxury of one carrier. We would get all communications related to Mal Lanyon, say—everything. It was not a problem. It was easy. Any words spoken were what was said over the phone. The audio was easy to work out. But with the advent of the internet, although it is the same warrant today to the same member, there are about 600 or 700 potential ISPs and carriage service providers out there; and, when we serve the warrant, I am not getting the content, the communications, I used to get, to the point where we have to do other things—I cannot disclose those things in this forum—to complement the TI process.

So we are exploring alternative methods of operational deployment and other forms of electronic surveillance services to fill in the gaps. There is a gap there. Encryption has become mainstream now, with the Snowden impact; we have over-the-top applications and the smartphones out there: all those things are impacting on us. I am not saying they are bad for the global community. I think there are some good things in there, but for us it is hard just to keep abreast. That is why we need to very quickly reform the TIA process—to get a level playing field for policing, I suppose, or a creeping-up in terms of our powers to intercept and more comprehensively acquire and collect the data that we once used to collect. So it is a growing problem for us.

**Mr CLARE:** Most particularly, on that issue of public wi-fi, if somebody who is up to something nefarious is communicating using public wi-fi, will this legislation not capture them?

**Det. Supt Kopsias:** Probably not. It will not go all the way, but we will be able to do other things, other investigative processes, to enable it to be rendered intelligible. I remember, when Mr Blunn AO reviewed the T(I) Act back in 2005, one of his recommendations was that the telecommunications carrier and the carriage service providers should be responsible for rendering all product intelligible and readable to law enforcement agencies, and those costs should be borne by the carrier. They were that man's recommendations but, sadly, they have not been enacted as yet. I am waiting for the day when we will have some legislation in place where encryption will not be a huge problem for us. But that is where we are heading; it is huge problem for us.
The legislation is part of the process, but it is a pretty broad area we are talking about here. Certainly, there is a lot of enacting legislation that needs to come from other state and federal areas too. But, with that, we need to be collaborating more with agencies. That is what we are doing now. We are working internally and externally with overseas partners to find a common theme here, because the problem does not just rest here in New South Wales or Australia; it is a global issue, and I think all agencies are in the same boat at the moment.

**Insp. Segrave:** If I could just make one point: I think the issue with those wi-fi hot spots is that they are a vulnerability in terms of law enforcement and, by extension, the community; and history shows, across a whole range of areas, that serious and organised crime actors are very quick to identify those vulnerabilities and exploit them. So it is clear, certainly to me and Victoria Police, that there are risks associated with those arrangements. That argument has probably been put to the committee before now, but I just draw your attention to that.

**Mr CLARE:** Thank you.

**Mr RUDDOCK:** I raised it in the context of internet cafes because it was an exemption, and now I understand it is much wider and goes to wi-fi providers in railway stations, shopping centres and the like. Presumably there is a reason they have been exempted—a practical reason in terms of implementation. Have you turned your mind to that to offer any advice to the Commonwealth as to how the shortcoming may be adequately addressed?

**Insp. Segrave:** To my knowledge, Victoria Police has not had that discussion. I am not sure whether that discussion has occurred at some of the national forums that I have not been a party to. Without meaning to sound flippant, from a law enforcement point of view, I would have thought that that is self evident: ie we have got areas within our community that persons can go to and engage in communications where they are less likely to come under notice or be discovered, the persons in our community who wish to or choose to do that because they are undertaking criminal activity, or actions that they do not want to come to the attention to law enforcement, will naturally gravitate to those areas.

**Det. Supt Kopsias:** Those issues have been raised in forums, but I am not sure that they have been well documented. We have raised them too in our submission in the review of the TI Act, to some extent, and we have raised them at national TI forums. We have a forum with the Australian Crime Commission now where all agencies get together and talk about exactly what we are talking about now, and those things are raised in that particular forum. AGDs are also aware of our concerns and the process in terms of the gap in the legislation.

**Mr RUDDOCK:** So your recommendation to us would be that, if it can be amended to remove the exemption in relation to internet cafes and wi-fi bodies, that should happen?

**Det. Supt Kopsias:** If it could happen, yes; that would be our recommendation. I know it is a big thing to happen, but it is that one job where you are trying to get that communication—it is the one that we will not be able to get, and it will affect us because it will be a serious crime.

**Insp. Segrave:** I think, at a minimum, the committee and the community need to be conscious of the fact that it is a vulnerability and it carries risks with it.

**Mr DREYFUS:** Thank you for coming, gentlemen. It is of great assistance to the committee to have the benefit of your view from the coalface, if I can put it like that. You would have been heartened to hear Telstra, Optus and Vodafone tell the committee yesterday and today that none of them have any intention of reducing the amount of data that they keep. I was certainly heartened to hear that. As was put by Mr Epstein, who was here for Optus this morning—I do not know whether you heard his evidence—the three of them carry the vast majority of communications in Australia.

I want to start by saying that all three forces understand, I take it, that this bill does not prevent access by any state police force to telecommunications data—no part of this bill prevents you from obtaining access. Is that clear?

**Insp. Segrave:** Yes.

**Mr Lanyon:** Yes.

**Det. Supt Kopsias:** Yes.

**Mr DREYFUS:** That is because this bill is, in fact, not dealing with access by state police forces. What it is dealing with is the data that will be there for you when you go asking. Understood?

**Insp. Segrave:** Yes.

**Mr Lanyon:** Yes.

**Det. Supt Kopsias:** Yes.
Mr DREYFUS: It has the potential—and I am just confirming that this is all three of your force's understanding—to expand the telecommunications data that is available over what is there now.

Insp. Segrave: Yes.

Mr Lanyon: Yes.

Det. Supt Kopsias: Yes.

Mr DREYFUS: Which, as I understand from the evidence you have already given—and I am trying not to go over the same ground—you all think is a desirable thing.

Insp. Segrave: Yes.

Mr Lanyon: Yes.

Det. Supt Kopsias: Yes.

Mr DREYFUS: And that would be particularly so from the point of view of the standardisation that this bill has the capacity to produce, because one of its aims is to not only require that all of these 600-odd telcos keep data which, in some cases, they do not now keep at all, but to also require them to keep it for two years and in a standardised form.

Mr Lanyon: Correct.

Mr DREYFUS: I do not want to get confused here. I will ask questions regarding New South Wales first. You said, Assistant Commissioner Lanyon, that you think the current balance is about right. Just for clarity: you are talking about the current situation, not the bill?

Mr Lanyon: I was asked a number of questions. One of them was in relation to the current application process, which I certainly agree is about right. Regarding the seven-year ability for us to access through some of the carriers—and you mentioned earlier that it is certainly heartening that the carriers have agreed to hold what they do at the moment—the problem is that one of the carriers we have spoken about currently holds it for a lesser period than the bill would specify. I think we have all been very clear. From New South Wales' perspective, I support the intent of the bill. I certainly support what the bill is trying to achieve and what the outcomes will be for law enforcement.

The point I have tried to raise from a New South Wales perspective is simply that, in terms of some of that data, we are enriched by what the bill is going to achieve. We will get more data than we have ever had before. My concern is that, regarding some of the data which I feel is least intrusive, if I can put it that way, and would be of concern, we have the potential to have it for a lesser period of time than we currently do. My submission to the committee was that we could consider expanding that period or keeping that period as it was for that data, which would be an extension of what the bill is currently proposing.

Mr DREYFUS: That is why I at least was heartened to hear that Telstra, Optus and Vodafone were not going to keep it for a lesser period.

Mr Lanyon: One of those carriers does not keep it for even the period in the bill at the moment.

Mr DREYFUS: Understood. This is a question directed to New South Wales initially. Could you outline, as briefly as you can, how the process of access by your force works now? You have said that there is an authorisation by inspector or above, but presumably it comes from lower ranking officers. I am not talking about the process for telecommunications interception; it is the non-warrant process—Detective Superintendent, if you are going to answer it.

Det. Supt Kopsias: All of our inspectors and above—we call them commissioned officers—

Mr DREYFUS: How many of them are there, approximately?

Mr Lanyon: There are probably at least 1,000 commissioned officers in the New South Wales Police Force.

Det. Supt Kopsias: They are all authorised under the act—I think it is section 5AB. They are authorised officers to approve metadata requests under section 178 of the TIA act. They are in the field, say, at a particular location. Someone puts the request up to the inspector. They call in the boss. They discuss it—a particular crime has just been committed or is about to be committed—and there is a process in place. There will be discussion. There is a cost involved too. The constable or the detective will need to talk to the boss to make sure that everyone is happy, and costs will obviously be paid for the metadata. They look at the privacy aspects of the particular crime and the safeguards. There is a process on the computer called our 'I Ask' system. They log in online. They put down a narrative of the brief and so on. It goes through to the 'I Ask' system at Parramatta where it is approved. That system then talks to the carrier's system and it is vetted by 'I Ask', which is done by another inspector. There is more supervision and vetting, and the data is obtained from the carrier. At the local level, the
inspector will approve that particular request. They will look at all the safeguards, facts and circumstances to justify the request, and so on. It goes to 'I Ask'. There is another vetting process at 'I Ask', and then the carrier accesses the records back to the officer who requested the data under the process.

Mr DREYFUS: It is a pretty standardised process, I take it.

Det. Supt Kopsias: It is standardised, accounted, documented, recorded—

Mr DREYFUS: There is, in effect, a form sent by email to a carrier? You are not one of the police forces still using a fax?

Mr Dickson: I think it is more an issue with the carriers as opposed to the—

Mr DREYFUS: We were a bit shocked yesterday to hear that some of this takes place by fax. Does New South Wales—

Det. Supt Kopsias: One carrier still uses a fax process because it has not really come on board with the electronic delivery process. The other carriers have come on board. One carrier still uses a fax.

Mr DREYFUS: Perhaps we had better not ask you to name them. It might embarrass them.

Mr Lanyon: We use an electronic process internally.

Det. Supt Kopsias: We use an electronic one called—

Senator FAWCETT: Don't put the accusation to the police.

Mr RUDDOCK: I still have a fax machine.

Det. Supt Kopsias: What I am saying to you is that it is recorded, it is documented, it is discussed, it is transparent, it is objective, it is checked, it is balanced, it is all sanctioned—it is all good. The process seems to work. We have never had any adversity or any criticism levelled at us by any authority in relation to data processes and how we keep and manage data. We thrive on data because it is intelligence. We have thousands of police who access data. We have a data management policy. We have a communications policy. There is a screen up there and when you log in it tells you—it is in your face—what to do and what not to do with the data and to look after the privacy interests under the personal protection information act and so on. We are bombarded with the legislation, regulations and codes of conduct. Our own code of conduct tells us how we deal with that particular data too. The process is working. If it was not working, I would not be here telling you that—it is working. To give us another layer with another warrant would just about cripple us. It would add no more due diligence or accountability to the existing process.

Mr DREYFUS: On that, the questions that were asked by my colleagues went to a hypothetical and judicial warrant process. Some of the submissions we have had have acknowledged the slowness, expense, time, effort of a judicial warrant process and have said, in recognising that, this committee and the government ought to give consideration to, say, a much less formal tribunal process or even a ministerial process. Have you given any thought to that?

Mr Dickson: I think we have alluded to this previously. The main concern that we have with obtaining a warrant as an example for metadata is that at that initial stage of the investigation we would not have the information to support the warrant. We treat this as an intelligence. We need to get this information so we can actually then identify who may be involved, where the communication nexus is between the victim and the other parties if it is a murder type investigation. That will then give us opportunities to look at different individuals. Quite often it might remove them as a suspect or whatever. It is about having that process in place. As was previously alluded to, often when we do provide the warrant for stored data, we require all this information—that there has been contact between person A and person B. We would never know that unless we have the metadata. It is almost a circular argument to some degree as to how we would achieve that. I think it would be very difficult, and we would have to change our investigative practices significantly, if we needed a warrant to get the metadata. I do not think there would be that many occasions where we would actually have the justification at that point in time. While it is very important for the investigation—and do not get me wrong—we need to have the reasonable cause to suspect, and that is what we would be lacking at that in time.

Insp. Segrave: If I could just make a point on that too. I think there is potential for some observers to misconstrue this idea of law enforcement using metadata in terms of intelligence. It needs to be tied back to an understanding of the investigative process. The point that I made in my opening address tried to do that. It is important for people to understand that in most instances metadata is used at the early stages of investigation when police are trying to get an understanding of a whole range of things in relation to the circumstances under investigation. I think that is what we mean when we talk about it being used in an intelligence sense, not that it is some broad fishing expedition because we have nothing better to do. It is part of a process, but it occurs at a point.
in the process where we are unlikely to have sufficient information to make a formal application to a judicial authority. If there were steps taken to require that of us, that has very significant implications for the process as a whole, for the veracity of that process, for the outcomes of that process and for the viability of that process. It is really important that that point is understood and that, when we use the term ‘intelligence’, it is not construed as some sort of broad based fishing expedition.

Mr Dickson: The legislation talks about it being reasonably necessary and relevant. To me, if person A is murdered, who has had contact with that person in the previous 24 hours, 48 hours, seven days or whatever is quite relevant to that murder investigation, and that is what we are asking at that point in time. It is this same with a drug trafficker: whom that person has had contact with is relevant to that investigation.

Mr DREYFUS: That is helpful. Just taking New South Wales, it is very much a standard. With 122,000 requests, that means that a request is being made in a lot of cases. It has become a standard as a preliminary, early stage investigative tool for certainly all of your officers investigating serious crime?

Mr Lanyon: There would be very few criminal investigations for serious or organised crime that would not involve the use of metadata early in an investigation. It is a valuable tool to us in an investigation. One of the questions in relation to that is the utility—putting another layer of scrutiny over the top. The example I gave earlier is if I was murdered. If I had my phone, we would want to scrutinise it. We already have a system in place where we have to record which criminal offence it is tied to and the reasons why we are seeking that metadata, and that is recorded. If I had a judicial officer or a tribunal member looking at that as well, they are really only going to be rubberstamping what has already been done. I really do not know that it affords any greater scrutiny at that particular stage, because of the type of information that we are getting and we are looking for with metadata.

Det Supt Kopsias: It would not make sense because it is just as Mr Lanyon was saying. There is metadata, you get a warrant, TI get a warrant, surveillance devices get a warrant and covert search warrants get a warrant. It would just about cripple us. Another layer would really hurt us right now because, you are right, it is a preliminary aspect of the investigation. If that were the attempt within the TIA act, I am sure you would have a warrant already in place for metadata, because metadata sits within the TI process, and that complements the TI process—it advances and enhances it—and there is a process in place where you do get a warrant within the TIA act but not for the person using the service. It tells you to do your own inquiries and checks to get that data. It does not tell you to go out and get a warrant. The current process, from our perspective, is quite fine, and it does work.

Mr DREYFUS: It has become more useful over time, I would suggest, compared with 1979 when the current form of the regime was created—1979 being a point at which you would have got the call, the number rung, the number from, the time of call, the date and the duration; that is it. Now you get a lot more information.

Insp. Segrave: Could I make a couple of additional points? The numbers that have been put before you today, in terms of the applications, reflect the uptake of the broader community of the communications technologies that are available. Obviously, they have increased exponentially over time and the law enforcement figures just reflect that. The other point that I would make in relation to those numbers, certainly from a Victoria Police point of view—and I would be confident that that extends across other law enforcement agencies—is that it should not be interpreted that, if we have made 60,000 requests in a year, that is 60,000 individuals. A lot of the organised crime figures that are investigated and where these tools are utilised routinely drop phones and roll phones over, so there are multiple requests in relation to that. There may be multiple requests in relation to call charge records over periods of time, and so on. Another aspect that needs to be understood is that, if you were to drill down into those figures, the actual numbers, in terms of the individuals that are the subject of the applications, are much less than the bottom line figure—

Mr DREYFUS: Can I reassure you, Inspector, on behalf of myself and my colleagues, that we have been given, in closed hearings, by the Australian Federal Police and ASIO, multiple examples of exactly what you are talking about. I am not disclosing anything here. For major investigations, there will be hundreds of requests for telecommunications data for a single investigation—

Insp. Segrave: Indeed. That is the experience across—

Mr DREYFUS: Possibly only covering a dozen or a dozen individuals, but nevertheless there are hundreds of requests. So, take it from me, and I think I can speak for my colleagues: we are not assuming—it is quite the reverse—that the 60,000 requests from your force or the 122,000 requests from New South Wales describe a number of persons. Far from it.

Insp. Segrave: It is also important to get that on the record in terms of other observers and other commentators to the proceedings.
Mr Dreyfus: Absolutely. Part of this exercise, part of what you do, part of what we do is build in confidence in our law enforcement agencies in the system. I want to finish on the stats. The committee sent you, all three, and to the other state police forces and the Australian Federal Police quite a detailed questionnaire. Thank you for ending the tantalising 'now you see it, now you don't', New South Wales. The purpose of sending the questionnaire was very much to provide as much opportunity as possible to publicly make the case for data retention. In other words, because the framework in which this question of the mandatory data retention has been considered elsewhere in the world by reference to statistics, allowing for all of the problems of looking at statistics—that was the purpose of the questionnaire. Your three forces have been able to provide broad level statistics as to the raw number of requests over the past five years, the percentages in time periods for which they are sought and that is really helpful. So thank you for that, but in answer to the questions—and I think this applies to all three forces—as to whether you could give statistical information as distinct from anecdotal information about the instances where historical telecommunications data had been used to prevent a serious crime, instances of historical communications data being used to prevent a terrorist attack, that is something on which the data is simply not available.

Mr Lanyon: I do not think there would be a police force in Australia that would keep that sort of data and, as Mr Dickson alluded to before, one of the issues is that it is rarely a single source of data that is responsible. For example, metadata might identify a source for us and might contribute to the way we go with the first steps of an investigation but there would be a number of other contributors. So to say that it was simply purely as a result of metadata would be a very problematic statistic to keep and I do not know of a police force which keeps that sort of information.

Det. Supt. Kopsias: It is pretty hard to keep those figures.

Mr Dreyfus: I do not think the questioning was intended to be where historical telecommunications were the only reason that conviction occurred or the only reason that crime was prevented. I am just checking that there is just not that level of breakdown available. What you have done, all of you to some extent, is provide some examples.

Mr Lanyon: If telecommunications metadata was stored hypothetically for an infinite period, there would not be one historical murder, sexual assault or robbery for which metadata would not be sought, not one. It is simply that crucial because it allows us, if nothing else, to put persons in places, to put contact into perspective, to identify whether people are talking to each other and where they were at a particular time. It can eliminate a person, get them out of an investigation very easily. So I can say hypothetically that if there was an infinite data storage period there would not be one historic investigation that would not use metadata.

Det. Supt. Kopsias: It also has the ongoing disruption element, too. When we investigate, we identify and we interview criminal gangs and associations, it has that disruptive element. That is why it is hard to quantify these outcomes which we are seeking in that questionnaire because it is hard to quantify that particular source of information—other than anecdotally, yes it is effective and without it we would not be able to function the way we function to day.

Mr Dreyfus: Lastly, I would say to Inspector Segrave that your force has attempted to answer our question about the discrepancy between ACMA figure and the reported figure to parliament under the T(IA) Act. We have had a pretty acceptable explanation yesterday, which, speaking for myself but not for my colleagues, I am satisfied with.

Insp. Segrave: Thank you for that.

Mr Clare: I want to pursue that little bit more, in terms of understanding the limitations of historical metadata and look at it in the context of the events that occurred in Sydney late last year to get some feedback from New South Wales police in particular. My impression, looking at that, is that this legislation—or access to historical metadata and its use by police—would not stop an event like that from having occurred, but I presume law enforcement agencies would now, after the event, look at that data and be able to exploit it to find out who that individual was talking to or communicating with. As opposed to that, a preservation order on somebody who has been identified as a potential risk to the general public—if the correct person has been identified and the notice has been put in place with the ISP, and law enforcement is looking closely at what that person is doing as a result—would be a more effective way of trying to disrupt or stop a potential attack like the one we saw in Sydney. Would you care to comment on that?

Mr Lanyon: Again, as a hypothetical, with the nature of Sydney itself and where law enforcement would benefit from metadata in relation to, say, the Sydney incident, it most likely would not have prevented the Sydney incident. At the time, metadata could have been essential in trying to identify any other persons who may be
engaged in a group or involved in that type of offence. Historical metadata could still benefit police down the track to see who that person has associated with in terms of a cell or, if they have been radicalised, where they come from. The preservation order you have spoken about would certainly be beneficial in that way, but metadata would have a range of benefits to law enforcement to prevent subsequent incidents.

Det. Supt Kopsias: Those preservation orders would be fairly important to us because they work in similar instances to the stored communications preservation orders in place, so we could actually go and apply to the carrier to retain that data for us for perhaps a more defined period. That early piece of information is pretty important. This is why it is good to standardise the current regime—to make sure that internet data or the rest of the data in terms of who called who is there, including cell dumps. It is important to find out who is in that particular location or another location and who called who, so you need those unique identifiers to be able to start the investigation process. Whether it is at that particular time or three or four months down the track, it is all part of the investigation process.

Mr CLARE: I presume NSW Police would be making a submission either in writing or orally to the NSW coroner and, potentially, to the federal government's inquiry into the events that occurred in Sydney. Would that be correct?

Mr Lanyon: We will mostly investigate the incident on behalf of the coroner. So, in terms of the critical incident, we will certainly report to the coroner on that side of things. If it was identified that there would be useful amendments that could be made or recommendations for amendments that would assist us, then that would certainly form part of that process. Similarly, if that forum was not the most viable for it—and, arguably, whether a state coroner would be is a question—there is certainly a capacity through Superintendent Kopsias for us to make national representations of what could have benefited law enforcement out of that example.

CHAIR: Maybe you can take these questions on the record or answer them now, but Mr Ruddock has named one exemption which is in the legislation regarding public wi-fi, and we have heard evidence today that you think the committee should look at. Are there any other exemptions that you think we also should have a look at? I am happy for you to take it on the record.

Det. Supt Kopsias: I was looking at the oversight arrangements in the bill, where we have the Commonwealth Ombudsman overseeing the metadata scheme. From a state perspective, if I can use the current model, we have a state ombudsman that looks after interception warrants under the Commonwealth interception act, then we have a Commonwealth Ombudsman who looks after stored communications warrants per se. So we have two oversight bodies looking after our warrants: one body checks a couple of thousand warrants and the other one checks a few hundred, so to speak, but there are different practices for one and different practices for the other, and different rules apply. Having two oversights in the one process, to me, seems a little bit ineffective and inconsistent. It leads to confusion in terms of trying to operation at best practice to ensure compliance. With this scheme here, you will throw—sorry, my words—the Commonwealth Ombudsman again into the loop to do our metadata. So we will have the Commonwealth Ombudsman looking after metadata, the Commonwealth Ombudsman looking after stored communication warrants and the state ombudsman looking after TI warrants. I think we would like to see one oversight body looking after the whole process, especially when it falls under one legislative scheme. To me, it makes better sense from a state perspective. We have not discussed this with our state partners here but certainly from my perspective—

Mr Lanyon: We will take that on board and respond back to the committee. I have not really considered the exemptions in the way you are asking at the moment. We could respond back, if there were any other information.

CHAIR: Good. Also, we have had this discussion about seven years, two years et cetera. The evidence we have heard is that potentially there may be an issue here. If you could think about how this may or may not be sold in a practical way or whether it could be, if you could come back and provide us with some further evidence around the discussion we have had on that topic, that would be extremely useful as well.

Mr Lanyon: We could certainly do that. As I think I have indicated, from a New South Wales perspective we would be looking for only a limited number of data sets to go to that seven-year period that we currently have—three particular sets.

CHAIR: If you could set that out for us and if there was, say, agreement among the lot of you et cetera to give us a little bit of a potential guidance on that matter, I think the committee would find that incredibly useful as well.

Mr Lanyon: Thank you.

Insp. Segrave: Chair, could I take you back to the issue of exemptions. There is one area Victoria Police would like to put on the record. It is in our written submission—that is, VLR, visitor location register data. The
intent of the bill, as I understand it, is explicitly around data that arises out of communications, which VLR does not. VLR is effectively the handshake, as it is anecdotally referred to, between the phone and the tower as the phone passes the tower, even when there is no actual communication occurring. That has what I would suggest are fairly obvious benefits for law enforcement and within the Victorian jurisdiction we have had one recent very high profile homicide which caused high degrees of community concern and which VLR was instrumental in resolving, certainly in the time frames that we were able to do. Victoria Police would like it to be put on the record that our view is that VLR should also be part of the datasets that are considered in this legislation.

**Det. Supt. Kopsias:** We would also endorse the VLR because carriers have a similar capability and we would like some standardisation and some consistency in that particular arena.

**Mr Dickson:** Can I ask for a time frame for the advice you would be seeking?

**CHAIR:** If we could get it by the end of next week or may be in 10 days time, if that is reasonable.

**Mr Dickson:** We will do our best.

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

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

Mr Moraitis: Thank you. I think my colleague Deputy Secretary Jones made a presentation in our first hearing in December. You also have the benefit of our submission, which you have, so I leave it at that for the purposes of this session.

CHAIR: Okay.

Mr Lewis: I have an opening statement which I would like to share with the committee. Thank you for the opportunity of being here this afternoon. The shocking and what I regard as terrible acts of violence that we have witnesses in Australia, Canada, the United Kingdom and most recently in France emphasise the gravity of the threat that is posed by terrorism. These tragic events as well as the turmoil that we have seen in Syria and Iraq illustrate the disturbed world in which we security intelligence and law enforcement agencies are currently operating with regard to the terrorism threat. We deal in this case with people with no regard for the law, no regard for community and often, I might say, no regard for human life.

ASIO is the only Australian government agency that is legislated to both collect and assess intelligence. Our routine business relies on capturing and verifying numerous sources of reliable intelligence. The functional information provided through telecommunication interception is one such source. It is a source of intelligence which we consider to be a fundamental building block for intelligence led investigations. It is a fundamental building block for ASIO to provide the security protection and the warning which our Australian community expects.

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 that we are discussing today is a critical piece of legislative reform aimed at ensuring that Australia's security intelligence and law enforcement capability remains relevant and effective. Access to historical communications data is vitally important in ASIO's effort to identify threats to security and to keep Australia and Australian interests safe. I want to stress that ASIO is not seeking new powers to ensure access to this information; rather the aim is to ensure legislation is in place that will enable my organisation to keep pace with the inexorable modernisation and standardisation of access in what we know to be a rapidly changing communication environment. Again, this legislative reform is critical to ensure that ASIO remains able to gain an intelligence insight to keep ahead of the people who would wish to commit acts of terrorism, espionage and politically motivated violence and to protect against people with no regard for Australian law or community values.

The historical communication data has proved essential in the resolution of a majority of ASIO's high-priority investigations. That includes the prevention of terrorism attacks. Some ASIO counterterrorism investigations where Australian authorities have prevented the loss of life in Sydney and Melbourne are well known and have been out there in the public arena for some years. Less known, of course, is the way in which historical communication data has been of assistance to us as we tackle the problems of counterespionage. We provided a submission to the committee which you have all seen, and I know one of my colleagues gave evidence in a closed session the day before yesterday.

In the bill it is proposed that historical communication data be retained for two years. ASIO supports this provision. However, I would like to point out—and this is important—that I regard the retention period as a
pragmatic compromise. Ideally ASIO data needs would be better met if there were a significantly longer retention period, but I want to stress that, with the competing interests—we do not operate in a vacuum here—of the triangle of privacy, business efficiency and security, I accept that a two-year retention period is an acceptable minimum.

I want to say a few things about accountability because I know that is of interest to the committee. ASIO's role is to investigate and provide advice on threats to Australia's national security, and we take these responsibilities very seriously. In doing this work we are very mindful of the importance of using the least intrusive methods of collection proportionate to the level of threat. When an individual comes to ASIO's attention, there are a range of methods that can be applied to establish whether that person's activities are relevant to security or not. Requesting historical communication data is often one of the most useful as well as one of the least intrusive methods of establishing those matters of fact. In many cases a simple subscriber check on a phone number is sufficient to determine that there is actually no investigation required and the matter can be put aside. This data that we are talking about is collected lawfully in all cases. I as well as my officers understand the sensitivity of these holdings. The holdings are strictly controlled. They are well managed, and access is highly accountable. In my organisation we strictly adhere to the need-to-know principle, and in addition we have numerous internal accountability mechanisms to ensure the protection of the data.

We use more intrusive collection methods only where there is a warrant and where it is warranted by the level of threat to Australia's national security. In these cases ASIO is careful to ensure that the level of intrusion into individual privacy remains proportionate to that threat and in accordance with the guidelines that were provided by the Attorney-General. It is not and will not be the case that ASIO automatically requests the maximum amount of data available. Should this bill become law, ASIO will continue to request access to historical communication data needed only for the purpose of carrying out our function, regardless of the length of time that data may be available for. We abide by the law.

ASIO's work is also highly accountable through, as this committee knows, a range of external processes. Your own committee is one such process. The Senate estimates process is another. We have internal processes within our organisation with which you will be familiar, and I note that ASIO's internal processes are open and regularly reviewed by the Inspector-General of Intelligence and Security, who I understand gave evidence to you a short time ago.

In summary, I would like to invoke some of the words that have been uttered by international figures around this particular question. International figures who have stressed publicly the need for continued access to metadata or historical communication data include Chancellor Merkel; FBI Director Comey; and my opposite number in the United Kingdom, Andrew Parker, the head of MI5. We are not alone in a global situation here. This is an international issue, and we are of course addressing the Australian aspect of that.

So, in summary, I want to reiterate four things. First, access to historical communication data is not a new power. Second, it is a power and authority that is critical to our work in protecting Australia. Third, it is essential to maintain this capability in the face of what I describe as rapidly changing communications landscapes. Finally, we already have what I regard as a strong accountability regime. We have demonstrated—and this has been admitted by the IGIS in her evidence—that we are diligently complying with that regime. Thank you.

CHAIR: Thank you.

Mr Ashton: Thank you for the opportunity to be here today. We have just a brief opening. Commissioner Colvin appeared here on 17 December and made a lengthy opening statement. We bring his apology that he could not be here today. He is certainly keen to continue. I think he has offered to present here with the police commissioners at some opportunity next month, and we greatly welcome the opportunity to do that.

The statement today is brief. It is simply to reiterate Commissioner Colvin's previous address and to add to that that we were very appreciative the committee took the opportunity to visit the AFP headquarters earlier this week. We were able to make a number of presentations to the committee in camera. For the purposes of the public record: those presentations covered a number of different types of cases, including large-scale drug trafficking importation, child sexual abuse, public sector corruption, murder, large-scale fraud and counterterrorism. The efforts that were made at that time in presenting you with those briefings were really to describe the nature of matters and the varied nature of matters for which metadata is used not only by the Australian Federal Police but by our partners who have already spoken here today and are present in the room and the way in which it is used to try to identify, investigate and prosecute crime.

One of the key points that we sought to describe to the committee in presenting those cases was not only the nexus between metadata and the actual investigations and the serious nature of those investigations but also that,
importantly, metadata is often used at the very early stages of an investigative process. It often forms the mortar that sits between the bricks of investigations. Without that mortar, often you cannot build a case in which to prosecute. I think that, in describing what happens to metadata in terms of how it contributes to prosecutions and crime, in our opening today we would also make the point that it plays an integral role in that. It is often hard to quantify like to the role that it plays. If you have an analogy to motor vehicle seatbelts, we know that seatbelts save lives but often cannot quantify how many lives seatbelts save, because it is part of a whole range of safety equipment that is in a vehicle. Metadata is similar to that when we are investigating large-scale crime. It plays a critical role and plays it in partnership with a whole range of other technologies, powers and investigative techniques, but it is absolutely critical. Thank you.

CHAIR: Thank you, and on behalf of the committee I thank you for your hospitality and for the informative briefing that you did give us. I think every member expressed to me that they were extremely grateful for the hospitality, so thank you very much. Andrew, do you want to kick us off?

Mr NIKOLIC: Can I resolve what appears to me on the face of it to be something of an inconsistency in the evidence presented to the committee by previous people reflecting on your evidence and what you have said today?

I have heard Mr Lewis quote access to historical telecommunications data as crucial and that two years is a pragmatic compromise, noting that long and complex investigations potentially require more. A number of submissions have expressed divergent views on this issue. Some have said to us that you already have what you need; others have said that one year is more than sufficient. The Human Rights Commissioner, in fact, proposes a one year data retention regime for the first three years of operation, but the Privacy Commissioner in his submission has referred substantively to evidence put forward by Australian enforcement and security agencies, stating:

…evidence put forward by Australian enforcement and security agencies, provides some evidence to suggest that a data retention scheme with a retention period of up to one year may be necessary…

It goes on to say in paragraph 37:

…evidence provided to the Committee at the hearing on 17 December—

Which has been referred to—

states that telecommunications data that is less than one year old is used in a large proportion of investigations.

And, at paragraph 38:

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

I raised this yesterday. Can I, with finality for the record, understand that what you are saying unequivocally—what I understand Commissioner Colvin said on 17 December—is that, in your words, Mr Lewis, two years is a pragmatic compromise?

Mr Lewis: At the risk of repeating myself, could I just reinforce the fact that two years is not only a pragmatic compromise but it is a minimum—it is the floor below which we could not go and still produce the kind of protection and the kind of analysis that we need. If you were to offer more, or if the result of the legislation produced a longer period of retention, you would get no argument from my organisation, but we recognise that we do not operate in a vacuum and that there needs to be some form of workable compromise. There are a number of very vital interests at stake here, and we think that will do it.

I would also make the point—picking up on the Privacy Commissioner's issue—that while much of the data that we utilise may be short term, that is something that has only been in existence for six months. A point that was made by one of the previous witnesses here was that the data we pull from deeper into the time period is quite often the most important because it will be some critical piece of a major inquiry. I would also—and this is a particular and peculiar requirement for ASIO—reinforce the point that counterintelligence investigations have a very long sine wave. The backcasting and the forecasting around those investigations is very long, and so I would be unhappy at any suggestion—and I do not know where the Privacy Commissioner heard that one year was being suggested, but it has not come out of my organisation to my knowledge. It is certainly not my position.

Mr NIKOLIC: I take it from your comments just then that this is not a quantitative argument—it is not about saying X number of data retention requests are much more plentiful in the early stages under a year, ergo the smaller number of longer term ones are less important. That is the point you are making?

Mr Lewis: Almost the reverse.

Mr NIKOLIC: Finally, the Human Rights Commissioner calls for an independent judicial or administrative authorisation system not just for the content of communications but for an additional warrant process for
metadata. I wonder, from your perspective, how workable that is and what, from a tactical operational level, the implications are of adding an additional layer of judicial warrant approvals up-front and what it might do to your operations.

Mr Phelan: When I last gave evidence on 17 December, I think I described that it would cripple our organisation, and I do not resolve from that position. I listened to the evidence of my state police colleagues, and the AFP’s position would be exactly the same. We must remember, as we said, that metadata is one of the building blocks that we use as an investigative technique that helps build the picture for us to use those more intrusive powers and, therefore, require a warrant.

To be quite frank, I would find it quite difficult sometimes to actually meet the minimum thresholds required for a judicial authority under the current regimes that exist to obtain a warrant for that type of material, because there is simply not a lot of background there—it is the first building blocks that come from the very infancy of an investigation, whether it be information that comes from an informant or from offshore, whatever that information is. With the time it would take, it would cripple the organisation in terms of man hours to be able to do it.

Mr Ashton: To briefly add to that, if I may: what complements that is that, at the other end of the process, there is now—which we think is entirely appropriate—an increased oversight role of the Ombudsman, a very specific inspection oversight role which attempts to address some of those concerns. We will need speed, we will need to be nimble at the front end in getting this material, and then we understand at the back end, where that urgency is not there, there can be a much more intrusive inspection regime that sits up the other end of it.

Mr Lewis: I spoke in my opening remarks about the laminates of accountability that we currently have in place—the internal ones and the external ones—and the fact that our internal processes are absolutely transparent to the IGIS. To have yet another laminate on top for what I would describe as the ‘quick turnaround processes’ that this particular problem—the historical communications data—presents, would be an unacceptable impediment to progress. I think we would just get bogged down. If you have a look at the volume of requests that would go through, I think it would quickly become unmanageable, and, if it drops back into a situation where it is not timely, it is of almost no use. There is a perishability around the request and the desire to get hold of the information.

Mr CLARE: Mr Lewis, thanks for your written submission and your oral submission today. I want to pursue this concept of a pragmatic compromise a little more, and you have made the point that, from ASIO’s point of view, the longer the information is preserved and retained, the better. I am interested in understanding the mechanics of how this pragmatic compromise was arrived at. Is it true that ASIO made the argument within government for a longer period of time but is willing to accept the two-year minimum?

Mr Lewis: No, I do not think I would characterise the process like that. We have, even within our organisation, a variety of views on how long information should be shared. There are enthusiasts who would want to see it held for long periods of time, and there are others who can satisfy themselves with shorter periods of time. I think your characterisation that the information is better with age is not what I am saying; what I am saying is that, in those cases where we have long, drawn out and very complicated but usually very serious investigations, quite often the nuggets of information will be in the longer-held databases. That is the point I am making.

The issue of parochial compromise is that, within my organisation, there is a high recognition of the fact that there are competing interests at stake here. Each one of those interests is legitimate—I mentioned the triangle, and each point of that triangle is a legitimate interest—and I think that something which is workable for all of those interests and meets all of those interests is the two-year mark. As I said, I would be very unhappy about anything less. If the committee was minded to consider something more, then you would not get any complaint from me, but I am conscious that this needs to be an acceptable position for our wider society.

Mr CLARE: Did ASIO provide any advice to the Attorney-General’s Department suggesting that the period should be longer?

Mr Lewis: I cannot think of it off the top of my head. We certainly have had discussions about what the length of time should be, but I do not recall at any point giving him specific advice. I will just ask for confirmation on that, but I am pretty sure that is the case.

Mr Moraitis: The process—and Ms Harmer agrees—is a process of iteration with our agencies and the portfolio AFP/As and we have a very close, productive working relationship. We as a department look at empirical evidence and there is evidence of that in our submission. It actually quantifies the period in a qualitative and quantitative way, to address Mr Nikolic’s point. I am sure the shorthand, pragmatic compromise that Mr Lewis alludes to is us as government having a pragmatic, good faith take on which way this should land. And a
two-year period, to allude to discussions previously by the state police forces, is a floor—it is a minimum period that we think gets us as close as we can—

Mr CLARE: I appreciate that; I am conscious of that. I have a little bit of experience in the operations of the department and the agencies that are before us.

Mr Moraitis: I am sure you do.

Mr CLARE: I also note that, from time to time, those agencies might provide you with advice, either written or oral, about their own views about the development of a proposal that might go before the Australian cabinet. Therefore, I am interested in how that pragmatic compromise was arranged—not in shorthand but in longhand? My question to you is: did the Australian Federal Police or ASIO or any other law enforcement agency provide any advice, either orally or in writing, to you suggesting that that two-year period should be longer?

Mr Moraitis: I will ask Ms Harmer to answer that.

Ms Harmer: The AFP and ASIO have both engaged extensively with the department in the development of this legislation. As this committee is aware, we have naturally been considering the policy issues for some time. This committee has previously made some recommendations around the retention period, so it would be correct to say that ASIO, AFP and indeed other agencies have expressed views in the course of development of the data retention measure on the appropriate retention period. That has included the views that agencies have provided to this committee on the appropriateness of the length of the period and that agencies would value a lengthy retention period.

Mr CLARE: That is a very, very good answer. But there is enough in it for me to interpret from that that those agencies provided you with advice that may include that it should have been longer than two years. My question then is: who decided that it should be two years?

Ms Harmer: Those agencies did, as you say, provide advice, as I indicated before. Again, the committee has also expressed some views on a retention period and in the development of the measure it weighed those issues, considered the views of agencies, industry and also the views that this committee itself has expressed on the appropriateness of the retention period. A number of witnesses to this committee and a number of submissions have reflected that there is an exercise in proportionality to be considered in terms of proportionality as a measure. So the measure will only be proportional in circumstances where it is appropriately directed at a legitimate end. The agencies have expressed views on those legitimate ends being the functions that they perform in protecting the safety and security of Australians, and the enforcement of the criminal law. There are also industry considerations and also privacy considerations. So all of those factors weigh into the proportionality and, through that, through looking at empirical evidence and at agency views we have reached a view and the government has attempted to put forward a two-year retention period.

Mr CLARE: That is another very good answer. Can I interpret out of that that the Attorney-General's Department formed the view that two years is the right amount of time, having sought advice from the agencies and that the government has agreed to that two-year period?

Ms Harmer: That is correct.

Mr Lewis: Mr Clare, could I just clarify the comment I made to you just a moment ago, because it obviously predates my time in this appointment. However, there was earlier discussion about a variety of periods, from two to five years, that took place between ASIO and the Attorney-General's office. I arrived on the scene at the time when two years was in contemplation in my own organisation and I am personally committed to that two-year period. I believe that is a compromise point, which I think is workable.

Mr CLARE: Just to explore that in a bit more detail, I am very conscious that law enforcement agencies consider this information to be critical. We have had that impressed upon us a number of times. You have provided us with some really useful information about the currency of that information. But we have had the New South Wales Police come before us and say, 'The longer, the better; seven years would be better, thanks very much.' The impression I am getting from your evidence is that ASIO has had discussions with the department about a period that might be longer than two years—perhaps two to five—and that the department, based on consultation with your agency and perhaps the Australian Federal Police, have concluded that a pragmatic compromise would be two years rather than a longer period and that that has been agreed to by the government?

Mr Lewis: I think that is a reasonably accurate description.

Mr CLARE: I want to turn to a question that I asked the New South Wales police at the end of their evidence about the events that occurred in Sydney in December of last year. Mr Lewis, you were in the room when I asked that question. I just want to check that you agreed with the evidence that New South Wales Police gave.
Mr Lewis: I am sorry, would you mind running that question past me again.

Mr CLARE: I asked the assistant commissioner about historic communication data and whether this legislation or whether historic communication data would have stopped that event from happening in Sydney. I think the Hansard indicated that it would not prevent it, but it is extremely useful either during the event or after the event to collect information about who that person may or may not have been communicating with. We then went on to have a discussion about preservation orders. I just want to check that you agree with that.

Mr Lewis: I think in the context of the question was asked of the New South Wales officer that was here that that is the right answer. I would, however, say that, for my own organisation, you will recall that I mentioned the rather long sine curve of some of these investigations just now. For Sydney you were asking about a particular situation and I cannot and will not comment further about that for all sorts of reasons. It is not uncommon for our inquiries to be on a very long sine curve, and, in that case, the receipt and the use of historic data at the front end of that process may well change the course of actions that are taken.

Mr CLARE: Indeed. The assistant commissioner made that point as well—depending upon how long that event—in this case the siege—takes place. I also asked him questions about the importance of preservation orders and about where they are in place where people have not been identified as a threat, the value that that presents in being able to potentially prevent events like the one we saw in Sydney. I seek your views on that as well because the hard part is identifying people that are at risk and then being able to put in place a preservation notice or a preservation order on the data of these people.

Mr Lewis: The facility of a preservation order is very helpful. It is something we use and it is absolutely the case that if we were aware that something was likely to happen that you can in fact put in place a preservation order around that particular set of circumstances to understand it better going forward. But all of that of course is prospective. Your earlier question about could we have stopped Sydney is a retrospective issue and retrospectivity is a different set of issues here. But prospectively, yes those orders are very helpful.

Mr CLARE: I make the point because this is very complicated and people often get confused about what we are talking about when we are talking about metadata. There is a difference between historic data and preserving data from a point onwards.

Mr Lewis: I should make one other comment. It is important that that preservation order goes to information which can then only be used by us under warrant—that makes it profoundly different, so it is a different order of magnitude. For us to actually access the information that has been preserved—we can ask for it to be preserved—requires a warrant.

Mr CLARE: But it can happen very quickly if circumstances require. The challenge, of course, is where you place those orders.

Chair: We need to look at the Hansard record but I also think the assistant commissioner from New South Wales did add that, potentially, incidents like that could help stop future events. I think that was clear point that he made. Just to make sure that we have got that there.

Mr CLARE: I think that is a fair point. One of the things he said was identifying a cell or a communication network. I think it is important for us in reviewing this legislation to understand its capacity but also its limitations.

Mr Lewis: I support that point that was made.

Mr CLARE: We do not want to create any unrealistic expectations that passage of this legislation is necessarily going to stop things that will not stop. The legislation, when passed and proclaimed, will not commence in full for two years. I want to seek the views of ASIO that they are content or appreciate that there is a time period there before the legislation is fully operational and whether you have any concerns about that.

Mr Lewis: Yes, we are satisfied. We had a discussion internally about this. From the time of royal assent, there is no—dare I say—backsliding in terms of the data that is being held by the telecommunications companies at that point. I think Secretary Moraitis might have something more to say about that.

Mr Moraitis: That is right. We were listening to the testimony before—that there was no degradation and obligation from the moment of royal assent. I think that provides, again, a further floor and provides a relative degree of assurance on behalf of the operational agencies that have been well aware of that.

Mr CLARE: I am sure you would have heard the evidence of Telstra, Optus and Vodafone that they do not have any intention either before or after royal assent, and that gives us a high degree of confidence.

Mr Moraitis: Yes, that is right. That is practical reassurance we also welcome.
Mr CLARE: That must be a reassurance to you about the risk of degradation. I will move to a series of questions to the department specifically, some of which have come out of the evidence we have heard over the last two days. Firstly, we heard from ASIC, who were concerned they were not listed as a law enforcement agency. They were concerned that if they were simply made an agency by regulation by the Attorney-General that they might find themselves getting caught up in a court process. I am interested in the Attorney-General's Department's thoughts of the evidence given by ASIC.

Mr Moraitis: We are quite satisfied with the situation. I am very aware of the points made by the ASIC. I am also aware of the regime that is in place. Speaking as a secretary, I understand the perspective of where they are coming from and the practical reality of the fact that they would be a supplicant under the new regime. And for all intents and purposes, I would start from the a priori assumption that they have a very positive case to make which should be considered very strongly in that context rather than starting at the point. I will try to answer the point about risk.

Mr CLARE: Before you do that, I interpret from your comments that you are positively disposed to their argument. If this committee were to recommend that ASIC were to be listed as one of those agencies, would it be correct to say that the Attorney-General's Department would not be necessarily opposed to a change?

Mr Moraitis: I will take that one on notice, based on your recommendations. We will see how we go. The point I was making was my mind space is that I can understand the arguments and where they are coming from, so in the context of the regime we have set out—

Mr CLARE: Do you think it is a strong argument?

Mr Moraitis: Objectively, yes.

Ms Harmer: In terms of the specific issue that ASIC raised this morning, as I understand it, they reflected that perhaps a declaration as an agency would put them on a weaker footing than they might currently be at the moment. With respect to ASIC—and we have had discussions with them on this point—I do not agree that that is the case. In actual fact, a declaration puts them on a stronger footing than is currently the case. ASIC’s ability to access data at the moment relies on their ability to fall within that very broadly and non-specifically cast definition of ‘enforcement agency’, which does not identify them by name; it relies on them falling within that broad class of agencies who are involved in enforcement of the criminal law and related functions. A declaration as an agency would actually give very specific certainty that ASIC is prescribed for the purposes of accessing data. And I think if anything it puts them on a stronger footing rather making them more susceptible to challenge on the basis on which they can access the data.

Mr CLARE: On this issue more broadly of the power of the attorney to make such a declaration, we received submissions from a number of different organisations suggesting that the discretion of the attorney in this respect should be should not be as broad as it currently is in the legislation. ACAN and made some recommendations to us about how that might be restricted to agencies that are responsible for investigating serious offences—I think as it is defined under the TI act.

As you know, the University of New South Wales—and we discussed this on 17 December—also made recommendations about how this might be tightened. Yesterday in evidence News Corporation also made the argument that the powers of the Attorney-General, or the discretion of the Attorney-General in this respect, should be more narrowly defined. Has the department had a look at these arguments and have you formed a view?

Ms Harmer: We have had a look at those arguments and we have heard some of the evidence given by those submitters that you referred to. As I said earlier, the test that is now being prescribed for declaration of an agency is one that substantially narrows and puts greater clarity around the agencies that can access telecommunications data. At the moment we have a very broadly cast description into which agencies may fall simply on the basis of their functions and constitution. The declaration process that is proposed in the bill is one that puts quite a high threshold around declaration of agencies. It would require the Attorney-General to have regard to the functions of those particular agencies—the extent to which they would use or require stored communications or telecommunications data in the performance of those functions—and then introduces some new and quite specific requirements in relation to the extent to which those agencies are the subject of binding privacy obligations in relation to how they treat that information. So the new declaration process does actually include quite significant enhancements on the way in which an agency can become a participant in the scheme to access telecommunications data. Of course in addition to that we are introducing substantial oversight for those agencies that do access the data through the ombudsman, which is not currently present in the scheme.

Mr CLARE: Their argument, if I might put it to you, is that under the proposed schedule 2, 110A(4)(f) is that, in addition to all of those things that you have set out, the Attorney-General can consider any other matter they
'consider relevant'. So this gives the Attorney-General lots of liberty in making those decisions that perhaps they should not have.

**Mr Moraitis:** The key word is 'relevance'; it has to be relevant to the purposes, so it is not open-ended.

**Ms Harmer:** I think it is also a matter of administrative decision-making. A minister is entitled to take into account those things that are relevant to the making of that decision. Whether that is specified there or not, that makes clear on the face of the legislation that those matters can be taken into account, but it would necessarily flow in any event that a minister would be so entitled, I think.

**Mr CLARE:** When can we expect the draft regulation in relation to the dataset?

**Ms Harmer:** I assume your question relates, effectively, to the extent to which the data that is to be prescribed by regulation is available?

**Mr CLARE:** Yes.

**Ms Harmer:** And on that point the data—

**Mr CLARE:** I guess I am making an assumption. We have the draft dataset. Organisations that have come before the committee that have looked at it have expressed general agreement with it—with the caveat that Optus today, for example, have a number of suggested changes. But there has been a consistent theme in evidence before us over the course of the last few days that there is a hankering to see the draft regulation, not necessarily the substance that would be included in any draft regulation. So the substance of the issue is already—

**Ms Harmer:** A draft regulation would prescribe the dataset; that is correct.

**Mr CLARE:** So it is a simple process; it is effectively a cut and paste of the document into a regulation—

**Ms Harmer:** A regulation would prescribe the dataset; that is correct.

**Mr CLARE:** Is it the intention of the Attorney-General's Department then to prepare that document in advance of this committee reporting back at the end of next month?

**Ms Harmer:** The draft regulation would be the formal instrument through which the Governor-General prescribes the data to be retained. So, in terms of this committee's consideration, the dataset that has been referred to provides the substance that would be included in any draft regulation. So the substance of the issue is already before the committee.

**Mr CLARE:** If this committee were to recommend that, instead of that approach, the dataset should be embedded in the principal legislation that is before the parliament, would that be a major drafting exercise?

**Ms Harmer:** The dataset that is proposed is one that could be included in regulations. It could likewise be included in primary legislation. I think as I said in response to questions from the committee in December, there is nothing procedurally that would preclude the dataset from being prescribed in legislation. It is simply a level of detail that is typically reserved for regulation, but certainly there is nothing technically that would preclude the data from being placed in the legislation.

**Mr CLARE:** Costs. We are keen to see the next report from the internal working group. They are now focused on this issue. We have received some evidence about submissions having now been made by Telstra, Optus and others to PricewaterhouseCoopers. Before we report, it would be very valuable for us to have an understanding of what the costs of this scheme are likely to be as well as what proportion of those costs the government intends to subsidise.

**Mr Moraitis:** As you know, there have been various iterations of PricewaterhouseCoopers' draft reporting. That is still a work in progress. We do not have a final report, and if I did I would not be able to share it with you on this occasion because it is part of cabinet deliberations. To be honest with you, we are still waiting on the finalisation of that report to inform us of the quantum and the reality the Commonwealth bears in terms of the government's commitment to reasonable coverage of capital costs. That is the context in which we are operating.

**Mr CLARE:** We would be keen, when that process is concluded, to have you back before the committee to explain the report and provide us with some more information on it. Are you able to give us a feel for how long that might take so that we know when we might need to bring you back before the committee?
Ms Harmer: Could I ask you to clarify the question? Are you asking for when a decision might be made on the quantum of contribution or when—

Mr CLARE: First, when we can see the report. When the Attorney-General approves the report—

Ms Harmer: PwC's report?

Mr CLARE: Yes. PwC is providing information to the IWG, if I am correct. Is that right?

Ms Harmer: PricewaterhouseCoopers is providing a report to the Attorney-General's Department that we have commissioned to inform the government, not the IWG.

Mr CLARE: Okay. Nevertheless, what I would be keen to get advice on is when we would be able to see that report.

Ms Harmer: PwC's report on costings is, as the secretary said, one that is being prepared for the purposes of government deliberations. It is not a report that we anticipate being in a position to share. Regarding the decision on costings and the decision on the contribution that the government makes, the government has reiterated on a number of occasions that it intends to make a reasonable contribution to the up-front capital costs of implementing data retention, but it would be a matter for government as to the timing of that decision. I am not in a position to advise the committee as to when that might be.

Mr BYRNE: That throws a rather large spanner in the works, doesn't it? If you have looked at previous committee recommendations, that was one of the key recommendations. So what you are telling us is that the committee is now not relevant. That is effectively what you are saying, isn't it?

Ms Harmer: What I have indicated is that the government has made a decision on costs. This committee previously made a recommendation that the costs should be borne by government. The government has taken into account that recommendation and the decision that it has made is to make a reasonable contribution to those capital costs. That advice I can give to the committee, about the approach to preparing those costs. What I cannot provide is advice as to when the government might make a decision on what that contribution might be.

Mr BYRNE: Could I say to you, via your department head, via the Attorney-General, that it would be in his interests and the government's interests to provide the information that was provided to you by PricewaterhouseCoopers to this committee. If it is not, there will be consequences. Just so that you take that on board and we have it on the public record. It is unacceptable to me, as deputy chair of the committee, and the chair. We have had discussions with Duncan Lewis's predecessor, with your predecessor, and for you to come before this committee and say to me that you cannot provide a costing is completely unacceptable. Regardless of the excuse you provide, it is unacceptable to an oversight committee. Duncan, you are talking about the ISC, where they had 12 months. The ISC would have been given this information. It would have been given this information before it deliberated, but you are saying this committee cannot have it. Frankly, I do not care what you say. It is unacceptable.

CHAIR: I do not think you need to answer that, Mr Moraitis.

Mr Moraitis: I will take it on notice.

Mr BYRNE: You can take you back to your political masters, basically.

CHAIR: The deputy chair is—

Mr Moraitis: My Attorney, yes.

Mr BYRNE: I am sure he is listening.

CHAIR: I do not think there is any need for you to respond to that.

Mr CLARE: If I might just add one point, the Australian Federal Police have been very open with the committee in providing in-confidence information which is helping us with our deliberations—ASIO as well. All of that information, which is not made public but is available to the committee, is extremely useful for the members of this committee. It is the information we need to prepare our report. I do not think there is any disagreement around this table about how important this legislation is and we are trying to scrutinise it as best we can to make sure that we provide the best possible advice to the parliament and, for that matter, the government.

But a big part of this is: how much does it cost? How much is it going to cost Australian taxpayers? We are law-makers who need to make decisions on laws, and one question we need to have an answer to is: how much does this cost in total, whether it is ballpark or exact—and it will take some time for it to be made exact, I appreciate—and what proportion of that is going to be covered in the budget? For that reason, I think it is in the interests of the government to provide this committee with that information.
I am not talking here about the proportion of it—I appreciate that that is something that needs to go through the cabinet process. I am particularly talking here about what the report says. If this committee is deprived of the information in that report, I think that would be a mistake.

Mr Moraitis: Thank you. I appreciate that point and I will take that on board and convey that to the Attorney.

Mr CLARE: I just want to move to the issue of the security of data. We have heard from a number of witnesses about that. One of the recommendations that this committee made in 2013 was that it be mandatory that data retained under a scheme such as this be encrypted. My understanding is there is no specific provision in the legislation to deal with this. We did have advice or evidence over the last few days about this from a number of different witnesses to support it, including Optus today, who described this as a sensible approach. This is another one which the department may like to take on notice because it is a policy decision that would need to be made by the government. But I am interested to get some advice on why that recommendation of two years ago was not implemented in this bill and whether it should be.

Mr Moraitis: You mean regarding encryption?

Mr CLARE: Encryption.

Ms Harmer: There are a couple of points that I can make in that regard. As a number of industry participants have reflected in their evidence to this committee, it is already the case that the industry retain a range of telecommunications data and that they are subject to a range of risk based information security obligations which oblige them to provide a certain degree of security, including under the Privacy Act and the Telecommunications Act. Those existing obligations apply to the whole range of their information holdings. Of course, data retention would be just a subset of the holdings that an industry participant might have. We would expect that the standards that the industry apply to their current data holdings would continue to apply to any additional holdings that they might accrue under the data retention measure. I should say in that regard that it is the case that we work closely with industry to manage security risks, including protecting networks. We have had productive and positive engagements with carriers on that particular front.

The other thing that I should add, which I think is reflected in our submission and may have been alluded to in Deputy Secretary Katherine Jones's opening statement in December, is that the government has committed to a broader piece of work around telecommunications sector security reforms and has indicated that it intends to bring forward legislation this year, and prior to the conclusion of the implementation phase of data retention, which addresses broader issues in telecommunications sector security. So the government's approach to the PJCIS's recommendation on encryption takes into account that broad context of the existing data protection obligations that carriers are subject to, the existing engagement that we have with them and forthcoming telecommunications sector security reforms.

Mr CLARE: Which may include encryption?

Ms Harmer: Those reforms are coming forward. They would include, I understand, broad principles in relation to the security of information. One thing that this bill naturally does not do is prescribe the particular way in which carriers must go about their business. Rather, it defines in broad terms the obligations they would be subject to without technologically specifically prescribing how they should go about it.

CHAIR: Is using the word 'encryption', then, too technologically determinative?

Ms Harmer: Using the word 'encryption' does beg the question of what type of encryption and to what standard and in what respect. I think it certainly reflects the intent of this committee, and the recommendation was understood as being about importing a degree of protection for the data. But it is fair to say that, in our engagement with the industry, while some providers asked for certainty and for a prescriptive approach to how to go about doing things, others have been very clear on the fact that being very prescriptive about how a measure should be implemented fetters their ability to run their businesses, which of course are ones that they must run at a profit.

Mr CLARE: That was one example of a lot of recommendations that have been made by different organisations before the committee over the last two days. If you trawl through the submissions, there are a lot of proposals about how the legislation might be amended or adapted. Soon this committee will need to trawl through those one by one and make a decision about whether we agree with those and whether we will incorporate them into our recommendations to the government. I am just wondering whether the Attorney-General's Department might be of a mind to conduct a similar exercise. I am conscious of your comprehensive submission. It is comprehensive and we are grateful for it. But in conducting our work and contemplating whether we agree with those recommendations which have come from a range of different organisations I am wondering whether the
department might go through those same recommendations and, in consultation with the Attorney, provide advice to this committee about its thoughts on those recommendations before we finalise our report.

**Mr Moraitis:** So before the finalisation of your recommendations you would like a checklist of what we think—

**Mr CLARE:** Yes. I think it would be useful for the committee if, before we write our report and say, 'Recommendation 1 is that you should make this change to the bill based on the advice we got from organisation X,' that we have your thoughts on that as well.

**Mr Moraitis:** Okay, yes.

**CHAIR:** Sort of like a collation—

**Mr Moraitis:** Yes, I understand. I just wanted to clarify that you want it before the finalisation of your recommendations.

**CHAIR:** Yes, before.

**Mr Moraitis:** We will take that back with us.

**Ms Harmer:** We have reflected on a number of the issues that have been raised in submissions in our own submission because we anticipated that those would be raised or because we explained the effect of the bill in a particular way. The only thing that I would say is that we would certainly be assisted if the committee can inform us if it is considering particular recommendations. There is obviously a very large number of submissions, and there have been some recommendations which we have dealt with in our submission. Naturally, if the committee and the secretariat are working on a particular list of recommendations, we could tailor our advice to particular questions and particular approaches.

**Mr CLARE:** I was reading through the Optus submission today, for example, and it has some very explicit recommendations about making certain changes to the bill. As I was reading through that submission, I thought, 'We would be assisted if the department could give us advice on its views on those suggested changes.'

**Mr Moraitis:** I guess Anna's point is that it would be useful to have a list of which ones you are focusing on. Is it every single recommendation in every single submission? Are there are 120 or 300?

**Mr CLARE:** That is a fair point. I am sure we can narrow that down to the ones we are particularly interested in.

**Ms Harmer:** The Optus submission is a very good example of where we could readily provide some information that would assist in considering the effect of the proposed amendments, whether amendments would be appropriate and what the consequences of those would be. I think a number of other submissions have made somewhat broader recommendations. Gilbert and Tobin's submission is another that has raised quite specific recommendations. If we could get some guidance on some of the others that you might be considering then we would be happy to provide some comments.

**Mr CLARE:** Thank you for that.

**CHAIR:** We will be happy to have a discussion, and we will provide that guidance.

**Ms Harmer:** Thank you.

**Mr CLARE:** There is one last area I want to pursue, which is the submission by the Internet Society on the issue of public wi-fi and this being a loophole. Mr Ruddock is not here at the moment, but I know he is interested in this as well, having asked some questions in December. When the New South Wales Police appeared before us an hour or so ago, I asked them questions about this as well. They described it as a risk, and Victoria Police described it as a big gap in the legislation and a vulnerability. The Internet Society yesterday said something along the same terms, that this is a gap that we need to be very conscious of. I am very keen to have those concerns satisfied before we finalise our report.

**Ms Harmer:** I think perhaps when we had our earlier discussion in December I may have been at somewhat cross-purposes with Mr Ruddock, so it is probably useful that we can clarify some of the comments made at the time and address some of the risks that agencies have identified subsequently. What the bill does, as I said, is to describe the data retention obligation but to describe it in a way that is a proportionate response to the particular challenges that agencies experience in accessing data. It does not provide comprehensive coverage of the entirety of telecommunications services provided in Australia. Indeed, it includes a number of quite specific exclusions to make sure that the measure is appropriate and adapted to the particular ends that are to be achieved. One of the exclusions that is then made in that particular context is to those services that are provided to a 'same place'.
I think where I may have confused issues in December was by references to cafes. In that instance I was not referring to internet cafes in the sense understood as providers of access to internet services but to more commonly your takeaway venues and coffee shops that might provide internet access that is at their premises and that they provide as a courtesy to their customers. That is an exclusion from the coverage of the scheme. It is an exclusion in the sense that the coffee shop then is not the subject of an obligation to retain data in respect of the service that it provides to the users of the coffee shop. It is nevertheless still the case that the telecommunications service provider who provides this service to the coffee shop is one that would be the subject of data retention obligations. So it is a question of at what point of aggregation the data is accessible.

Without going into too great a detail about the operational practices of agencies, data may be accessible at a different point in the process. The fact that a particular coffee shop is not required to retain data in relation to who it provides its free wi-fi to does not preclude data from being accessed at a different point in the process, so the exclusions are an illustration or a representation of the proportionality of the data retention measure in that it targets appropriate points in the process and provides data for key telecommunications services.

Mr CLARE: If I understand that right, does that mean that, in effect, there is not a loophole or there is not a gap because law enforcement would be able to get the information they need via the ISP that is providing that service to either the council or the cafe or the airport or the railway station et cetera?

Ms Harmer: That is correct. Carriers, carriage service providers and internet service providers will be subject to data retention obligations in respect of the provision of services to their customers, and their customers may include cafes that then offer their services.

Mr Phelan: If I may, how it would work in an operational sense is that, if an internet cafe or a coffee shop has a service provided by Telstra, we would know that that internet cafe service accessed their system from between the internet cafe and Telstra at a particular given point in time, but we would not know which device within that cafe accessed their internal wi-fi router or modem to do it. It is similar to if it is a home; out of the six or seven or eight phones or devices inside, you do not know which one has accessed it. However, it is a gap in that sense, but it does not mean that we do not have other technologies or other abilities to exploit that situation. It is just another investigative technique. For example, we would know that, if a person is in that area, they are using that particular wi-fi network, maybe, and then could use other techniques. So it is not the end of the world but, like anything else—I think the state police gave the evidence—it would be nice to have and it would be great for law enforcement. We have to do the proportionality test as well, though.

Mr CLARE: Pragmatic compromise.

Mr Phelan: This has been a lot about pragmatic compromise and we have given a lot of concessions.

Mr CLARE: Have you given concessions in relation to time period?

Mr Phelan: Yes. Mr Negus when he first gave evidence said 'indefinite' and I think I have come down from indefinite to about seven and then back to indefinite. Even the examples we have put in our submission that are before you, the two out of the four—and we did not selectively choose those, they are random, major operations. For the one relating to child exploitation material, the web site in particular was compromised in 2011. The referral gets to us in 2013—two years has already passed by the time it gets to us to start anything. At a very minimum, the day it arrives you have lost two years.

CHAIR: We heard similar evidence this morning from an organisation of an exact case where it was four years later.

Mr Phelan: Yes. You are actually beholden to when the originating information comes to you not from when the offence occurred. So an offence occurred last year, three years ago, two years ago, 10 years ago but you can only start the investigation when you know about it. That has sometimes been lost on some of our commentators, that they think the offence occurred and straightaway we have access to the information. That is not true.

CHAIR: On this wi-fi issue, this is something which Mr Ruddock has been very interested in. He has asked me to ask of the A-G’s willingness to just look at the evidence that we got from the Australian Internet Society yesterday. They have sought to engage with AGD or at least the Attorney's office—part of the evidence they gave of ways that might be able to assist in this issue. He was very keen for that to be put to you and whether there was a willingness from AGD to engage with the Australian Internet Society—they have made the offer—and to talk to them. I am not sure whether you heard their evidence yesterday, but if you have a look at that, that will give you the background to what they are seeking to do.

Mr Moraitis: Fair enough. Will do.

CHAIR: Thank you.
Mr CLARE: Those are all my questions. I just emphasise once again that I think it would be a mistake to expect this committee to report without having before it information on what the costs of the scheme are. I would ask the Attorney-General's Department to reflect upon that.

Mr Moraitis: Thank you. I hear you loud and clear.

Mr NIKOLIC: Can you recall whether the department provided costings for the 2012-13 inquiry?

Ms Harmer: I do not believe we did on that particular point. The issue that was referred to the committee was one of broad principle which was around broad reform of telecommunications interception legislation including, potentially, data retention legislation. As I think industry have attested to in their evidence, it is difficult to cost and measure until you have specific details and this is the first time that a dataset has been established against which costings could be prepared. So we have not previously provided costings.

Mr NIKOLIC: Thank you, and I did not want to interrupt my colleagues flow, but taking you back to the comments about datasets either in legislation or regulation, I think you said, Ms Harmer, that there is no procedural impediment to having the dataset in either but I wonder what the practical preference for having the dataset in regulation rather than in legislation might be from a departmental perspective.

Ms Harmer: As I said, the level of detail that is proposed to be included in the dataset is one that would be conventionally prescribed by regulation. Typically matters of detail are preserved for regulation with the primary legislation prescribing and limiting the extent to which legislation can be made by delegation effectively. In terms of the practicalities, the key change would be obviously a regulation is capable of being amended somewhat more swiftly in the event that there are technological changes that would require it to be amended. So primary legislation would naturally require a different process. Both require parliamentary scrutiny in slightly different ways. So the key difference would be the extent to which—

Mr NIKOLIC: Are you saying that technological development in recent times requires that sort of agility in terms of reshaping what a dataset might look like?

Ms Harmer: I think international experience suggests that potentially reshaping may be required at a future point. Our international colleagues have reflected on their experience with the EU Data Retention Directive, which took a technologically specific approach to their data set and found that it was very quickly outdated. We have learnt from that in some respects by proposing to prescribe a more technologically neutral data set. But our discussions with industry consistently reinforce the fact that telecommunications technology evolves at a rapid pace. The kinds of services that are available now were not available 10 years ago or even five years ago. There have been radical changes in the technology and the service offerings that are available to customers, who include people who use telecommunications services to engage in criminal acts and other activities. On the basis of advice from industry, we believe technological change is almost inevitable. Regulations would provide a vehicle for potentially making any refinements that were necessary in an expeditious way. That is an advantage of a regulation based approach. Amendment to legislation is naturally possible, but it takes longer.

Mr NIKOLIC: So your preference is linked to the sort of operational necessity you have seen arising from emerging technology in recent years. One of the challenges for us is obviously that the information about telecommunications services and those offerings is information that is exclusively held by the telecommunications industry. They are developing new and sometimes commercially sensitive offerings for the public and we need to be able to respond quickly to that. So, while we expect there to be change, we do not know the direction that change will take.

CHAIR: Thank you very much. I think that is all the questions. We will be in touch with some sort of matrix around recommendations. If there is any evidence that you have heard over the last couple of days that you think also could do with some clarification, we would once again appreciate any feedback. That goes for everyone who is here today. If you feel that there is anything that needs to be specifically clarified, we would welcome that feedback over the next week or so. I thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you. We appreciate your time and, given that we have run a little bit over time, your patience in appearing before us today.
The Privacy Foundation fundamentally opposes the blanket data retention regime embodied in the bill as it imposes an unacceptably high level of interference with privacy that is neither necessary nor proportionate to the objectives of law enforcement and national security. We emphasise—and I cannot emphasise this too highly—that this conclusion has been reached by every court and human rights body that has examined the issue, including the UN High Commissioner for Human Rights and the Court of Justice of the European Union.

There were some comments earlier on in evidence today by a member of the committee who—I have to apologise—is no longer here, who suggested inaccurately that the test for proportionality was 'some chance of success'. That is not the test and it cannot be the test. I would take you, if I can, to the bottom of page 4 and to the top of page 5 of our submission, which has an extract from the relevant report of the UN High Commissioner for Human Rights, and it bears close reading. The UN commissioner says:

Concerns about whether access to and use of data are tailored to specific legitimate aims … raise questions about the increasing reliance of Governments on private sector actors to retain data “just in case” it is needed for government purposes. The report goes on to say:

Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers’ communications and location … appears neither necessary nor proportionate.

That is the correct application of the test and that is the relevant part of the report from the UN High Commissioner.

The bill is disproportionate, and there has been some discussion of the meaning of 'proportionality'. The bill is disproportionate because it requires the collection and, in some cases, creation of what might be highly personal data about the entire population, regardless of whether or not there is a link to serious crime or threats to security. I must emphasise that proportionality is a well-accepted international test and it is not the same as 'pragmatic compromise'. The bill is a sledgehammer that unjustifiably breaches the right to privacy of all Australians who are overwhelmingly neither criminals nor terrorists. The interference is serious because non-content data or metadata reveal at least as much about people as communications content and sometimes more. This is now well established. What has happened is that what this data or metadata can reveal has changed and the legislation has simply not kept up.

It is our submission that the objectives of the bill can be achieved by more targeted mechanisms such as some version of the preservation notice regime under chapter 3 of the act. We do not believe that to date sufficient consideration has been given to the advantages of a more precisely targeted preservation regime. Moreover, the efficacy of blanket data retention is likely to be compromised by the extent to which persons of interest will adopt readily available techniques to hide their trails. By mandating honey pots of personal data, the bill creates risks of uses and disclosures of that data, including unauthorised access.

There are many technical problems with the bill as it has been drafted. It is very difficult for us to form an informed view of the privacy implications of the bill, because simply so much of the detail is left to delegated legislation, including the definition of the dataset but also including who may be subject to the regime and including the definition of agencies that may take advantage of the regime.

The foundation is concerned with the high level of warrantless access to telecommunications data under chapter 4 of the regime, which has emerged in evidence to the committee. Given that metadata is just as intrusive
as—and sometimes more intrusive than—content, we strongly support the introduction of some form of procedural safeguards for access to non-content data. We are not prescriptive about that, but we believe that this should be explored in more detail.

We also support, and this has been consistent in the submissions that we have made to relevant committees, increasing the thresholds for access to both stored content and metadata or telecommunications data such that access must relate to investigations of serious offences—that is, offences in general terms punishable by imprisonment of at least seven years. Thank you.

CHAIR: Thank you. It appears that none of the committee members has any questions. I think your submission is quite substantial, and obviously your introductory statement has also been quite detailed. So, I thank you very much for appearing before us today.

Dr Lindsay: Perhaps I could just add one more point, and it relates to the exemption from browsing history, which is in proposed section 187A(4)(b). The problem with this is that it simply says that this information does not have to be retained, but it does not prevent the retention of this information, and it does not prevent access to this information under chapter 4 of the T(IA) Act. Now, we believe that to say that the bill is privacy protective, because there is no obligation to retain this data, does not deal with the fact that the data may well be retained. And we also point out that in many cases with technology evolving, particularly with what is referred to as carrier grade network address translation, that to comply with the obligations under the bill to retain data it may well be necessary to actually also collect destination IP data, and that is because of the way in which business practices, which you are all aware of, have changed and the way in which the technologies used have changed.

Dr Clarke: Also, if I may, there are many points that arose in evidence today that would have been worthy of discussion. Perhaps I could highlight one: at no stage today has there been any real discussion of the fact that this is mass surveillance that is to be imposed by the parliament on the Australian people. We have skirted around that and never used the word. There has been mention of personal surveillance—the collection of data about individuals who have come to attention and about whom there is reasonable suspicion et cetera. That has been mentioned in passing. But this moves way, way beyond that, to mass surveillance.

Now, that has a mass of consequences, at all sorts of levels, from the philosophical through to the democratic, legal, social and technical. But one that arose today—a conundrum that arose in discussion when the MEAA was before you—is the question of: supposing there was a decision that the media should be exempt—whatever ‘the media’ means. It is inactionable. It is virtually impossible to specify how you can have a mass surveillance scheme which either fails to collect data about designated categories or which enables it to be collected but precludes it from being accessed by law enforcement agencies because somehow, magically, the holder of that data knows that the person to whom that data relates is a member of the media. Once you have moved into a mass surveillance scheme, you do not have any exceptions; you have built that kind of infrastructure that we used to associate with unfree countries.

CHAIR: Thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you. Thank you again for your tolerance today.
COPE, Mr Michael, President, Queensland Council for Civil Liberties, on behalf of joint councils for civil liberties

DE KOCK, Mr Hugo, Member, Liberty Victoria, on behalf of joint councils for civil liberties

LYNCH, Dr Lesley, Secretary, New South Wales Council for Civil Liberties, on behalf of joint councils for civil liberties

[15:16]

Evidence was taken via teleconference—

CHAIR: Welcome. 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 respect as proceedings of the House itself. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of parliament. The evidence given today will be recorded by Hansard. Do you wish to make some introductory remarks before we proceed to questions?

Dr Lynch: We will, but I do appreciate that we are probably all suffering from exhaustion around this topic at this stage. But we want to register quite clearly that we hold a considered position of opposition to the core policy in the bill. We do not support the mandatory mass collection of telecommunications data for most of the population for security and law enforcement purposes. To legislate for the mandatory collection and retention of mass telecommunications data to enable retrospective access by authorities is a very big decision and a very big step for a democracy. We of course accept that there is a real and significant terrorist threat facing Australians, and we accept the need for the government to provide security and intelligence agencies with adequate powers and resources for the best possible protection of Australia's national security—with, as always, the caveat 'consistent with a robust democracy'.

The complex but absolutely essential balance between security and democratic values is at the heart of the necessary and proportionate test that you have been talking about for most of today, one way or another. And we accept the proportionate test as defining how far we are willing to go as a nation in encroaching on our rights and liberties to protect our national security. The proposed regime clearly constitutes a major intrusion into the right to privacy of most Australians, including those who are not suspected of any participation in unlawful activity. It is our view that such a major intrusion into the privacy of the community will have deep, real, significant and negative implications over time for other freedoms and democratic values. It is the accumulation of this that means that, on balance, civil liberties councils consider it a step too far.

We agree with the further observation of the European Court of Justice, and we think this is a critical point about the collection of this data: Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained…

We do not believe that this—though it is acknowledged and quoted in places—has been consistently acknowledged by the government or its agencies. The public assertion that metacommunications data is like information on the outside of the envelope obviously cannot be viewed as a serious contribution to the debate.

We agree with the further observation of the European Court of Justice, and we think this is a critical point about the collection of this data:

…the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance. This means that ordinary people will be more cautious about many kinds of communications knowing they can be retrospectively accessed by authorities for up to two years and without the knowledge of these persons. This concern relates to the effects of both the collection of the mass telecommunications data and the access and use of that data.

A key point for us, which others have raised, is flow-on effects to other freedoms beyond privacy. Most significantly, the regime will create a real threat to free and open journalism. It will make it extremely difficult for any sensitive information to be provided to journalists as it will not be possible to guarantee confidentiality of any kind of telecommunications. This further suppression of legitimate whistleblowers wishing to expose misbehaviour or corruption and bring it to public notice does not augur well for any democratic society.
We accept that telecommunications data is an important investigative tool and that law enforcement and security agencies should have appropriate access to it. While we do not accept that appropriate access should extend to the compulsory collection and retention of mass telecommunications data—unfortunately, the whole population—we do accept that there is justification for a more targeted regime than the one that is proposed in this legislation.

I am jumping here, because I know you are all anxious to get out of here. Our core alternative recommendation is one which has been made by a number of other groups and has been explored widely in other countries, and that is to focus on a properly defined, targeted data surveillance scheme which is more compatible with liberal democratic values, less invasive of privacy and certainly a more proportional response.

We want to flag that this is a very, very live global debate, and that it is a highly and closely contended global debate. We think it is an important and defining debate for liberal democratic societies, and we think it is a long, long way from being over. There is a lot we could say about history and impact, but we will simply flag history suggests that high surveillance states and robust democracy are not good bedfellows. Having stressed our principal position, we of course recognise the government is intent on proceeding with the scheme and it is possible that the committee will support this. Therefore, we have addressed in our submission some of the major shortcomings—and there are many in the bill—and in fact most of the recommendations in our submission relate to these shortcomings. I will not detail them at this stage of the afternoon as I would think all of them have been raised by numbers of other submissions, and they are widely recognised flaws in the bill. It is absolutely essential that, if the government and if the committee recommends that the government proceed with this scheme, these major flaws in the bill are addressed and remedied.

CHAIR: Thanks very much.

Senator BUSHBY: In your opening statement you made the comment that the bill, if implemented, would represent a major intrusion on the rights of Australians. We had the Human Rights Commission here yesterday. They also indicated that—although on balance, with recommended changes, they support the passage of the bill—potentially the mass collection of data would be an intrusion. But when I put to them that the data, which would largely be held in an inert state and never looked at—probably the large majority of it never, ever looked at—was a minor intrusion on rights, they agreed with me. Are you at odds with the Human Rights Commission in that respect?

Dr Lynch: We think that the existence of such a large database with so much incredibly important and valuable personal information, which has the capacity to draw a pretty full profile of a person's life, is in itself a significant factor in terms of the society in which we live. There are a whole range of issues that have been raised around this relating to the security of that data, who and what interest it will attract from a whole range of players including those with a nefarious interest in it. There is the issue of function creep, which is hardly a rare occurrence in these kinds of contexts. There is the issue of access to this data by sources outside the framework of this legislation; there is civil access to it. There is no way there will not be pressure around access to this data—greater access to this data—very, very quickly. But the existence of such a very large, mass database—

CHAIR: Well, it will not be a large database, if it is just information that is generated by providers that they are required to keep. It will be held by a wide range of providers in their own ways. It will not be a central database. But coming back to my question though, you raise a lot of potential issues regarding what might happen with the data that is stored, if it is stored, which we have had a lot of evidence on over the last few days. That is something that the committee will look at, and we will deliberate on those issues. But I guess it comes back to the question that I asked you: the requirement that the data, which in many cases is already held, be held in a consistent manner for a consistent timeline. In the end the Human Rights Commission acknowledged that the retention of data itself was a minor intrusion on rights.

Mr Cope: The fundamental problem with that is that this is the state directing that some people will collect data to be used, made available, for its purposes.

CHAIR: That is right.

Mr Cope: That is quite different from private organisations who enter into contracts, which may or may not be consented to in any proper fashion, collecting data. That is a fundamental difference.

Senator BUSHBY: Absolutely, but I do not think that that is a valid comparison in this context. The opening statement was along the lines that the fact that data will be used and collected without people's consent under this bill will present a problem for a lot of people. The fact is that data is collected and used in exactly that manner now by the security and law enforcement agencies. The only impact of this bill is to maximise the likelihood that, when a law enforcement or security agency seeks particular metadata, that data exists.
Mr Cope: But we have a problem with the current arrangement.

Senator BUSHBY: That is a valid position to hold, but this bill is not going to expand the authority or ability of law enforcement and security agencies to access metadata. In fact, it actually confines it to some degree. The purpose of the bill is to maximise the likelihood that the metadata exists when they seek it.

Dr Lynch: I think that ignores the transformational change in what metadata is, what kinds of metadata there are, and the fact that that extraordinary acceleration in that area in the last few years is not an acceleration which is going to stop. We think it is somewhat misleading to speak about this as if there is no difference in the range and the kind of data that will be accessible through telecommunications metadata—and also, of course, the increasing analytical capacity to draw a vast amount of information out of this.

Senator BUSHBY: I would not use the word ‘misleading’ myself, but I think the law enforcement and security agencies themselves acknowledge that part of the reason they would like this is that there are changing business practices. This requirement would better enable them to ensure that, as technology changes, they continue to be in a position to be able to solve major crimes and to deal with terrorist threats by accessing metadata in very restricted and clear circumstances.

Mr de Kock: I think one of the issues we have raised is that the threshold for access to telecommunications data is so low that it just simply goes far beyond what is necessary for investigating serious crime or terrorism. That is a threshold issue which we have a problem with in the current legislation, which of course gets exacerbated through the two-year data retention period.

Senator BUSHBY: I acknowledge that that is your position and that it is a position of other submitters. Clearly, we have received evidence from others that suggests that it is necessary to continue in that position. I guess that is something that the committee will look at and deliberate on in due course. Chair, I think I will leave it at that point. Thank you.

CHAIR: As there are no more questions, I thank you for giving evidence at the hearing today. You will be sent a copy of the transcript of your evidence, to which you may suggest corrections. If you have been asked to provide any additional material, please forward this to the secretariat as soon as possible. If the committee has any further questions, the secretariat will write to you.

Resolved that these proceedings be published.

Committee adjourned at 15:34