COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL AFFAIRS REFERENCES COMMITTEE

Comprehensive revision of the Telecommunications (Interception and Access) Act 1979

(Public)

TUESDAY, 29 JULY 2014

SYDNEY

BY AUTHORITY OF THE SENATE

[PROOF COPY]

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

SENATE

LEGAL AND CONSTITUTIONAL AFFAIRS REFERENCES COMMITTEE

Tuesday, 29 July 2014

Members in attendance: Senators Leyonhjelm, Ludlam, Ian Macdonald, Marshall, Xenophon.

Terms of Reference for the Inquiry:

To inquire into and report on:

Comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the Act), with regard to:

a. the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and

b. recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013.

WITNESSES

BAKER, Mr Stewart Abercrombie, Private capacity

Evidence was taken via teleconference—

Committee met at 09:00.

CHAIR (Senator Ludlam): I declare open this public hearing of the Senate Legal and Constitutional Affairs References Committee for its inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979. The inquiry's terms of reference are available from the secretariat. The committee's proceedings today will follow the program as circulated. These public proceedings are being broadcast live via the web. The committee may also agree to a request to have evidence heard in camera or may determine that certain evidence should be heard in camera. I remind all witnesses that in giving evidence to the committee they are protected by parliamentary privilege. It is unlawful for anyone to threaten or disadvantage a witness on account of evidence given to a committee and such action may be treated by the Senate as contempt. It is also contempt to give false or misleading evidence to the committee.

The committee prefers evidence to be given in public but, under the Senate's resolutions, witnesses do have the right to request to be heard in private session. It is important that witnesses give the committee notice if they intend to give evidence in camera. If you are a witness today and intend to request to give evidence in camera, please bring this to the attention of the secretariat as soon as possible. If a witness objects to answering a question, the witness should state the ground on which the objection is taken and the committee will determine whether it will insist on an answer, having regard to the ground which is claimed. If the committee determines to insist on an answer, a witness may request that the answer be given in camera. Such a request may of course be made at any other time.

I welcome everyone today. Without further ado, I welcome Mr Stewart Baker via teleconference from Washington DC. Thanks so much for talking to us today and for coming online at an unusual hour. The committee has not received a written submission from you. I advise you that, as you are providing evidence from a foreign jurisdiction, your evidence cannot be protected by Australian parliamentary privilege. The giving of evidence is voluntary; however, if do you have concerns that what you say may cause you harm you may make a request to be heard in camera. Do you have any questions in relation to that matter?

Mr Baker: No, I do not.

CHAIR: The whole committee greatly appreciates that you are giving us your perspective. Would you like to make a brief opening statement before we go to questions?

Mr Baker: I am an expert in surveillance law. I am a private practitioner at Steptoe & Johnson in Washington DC. I will give you briefly my background, which may be useful. I was general counsel of the National Security Agency in the early 1990s. I testified to our 9/11 Commission after the attacks. I later was the general counsel and principal drafter of the report of the WMD commission into our intelligence failures in Iraq and then I became an intelligence consumer as the head of policy, the Assistant Secretary for Policy, at the Department of Homeland Security.

CHAIR: Just from the statements that you have already placed on the record, you do have a very strong view about the balance between privacy and security. Do you want to tease out for us your perspective?

Mr Baker: I have been quite disturbed at some of the consequences, not intended and rarely acknowledged, from some of the civil liberty and privacy policies that were adopted in the run-up to the 9/11 attacks. I think we have yet to fully acknowledge the cost that some of these doctrines incur. So I have a somewhat sceptical view of many of the civil liberties proposals because I know they can have costs and we have to look for those costs.

CHAIR: I am not sure how aware you are of the tenor of the debate here in Australia, but it has tracked along, I guess, very similar lines as have occurred in the United States, shaped by events like 9/11 and, in Australia's context, the bombings in Bali in 2002. More recently, I guess, the debate has been shaped by the revelations of Edward Snowden, formerly of the NSA. You obviously have a view that privacy advocates go too far in seeking to protect the privacy of individuals. What do you think is the best balance and what advice could you offer Australia in that regard?

Mr Baker: My broad observation is, I guess, twofold. First, technology is going to inevitably produce more data about all of us and make that data cheaper and easier to collect, analyse and store. For that reason, the idea of having less data is simply not on. It would be foolish to say, 'We're going to let private companies gather that information in order to sell us things that we may or may not want, but we'll not allow governments to use it to protect us from terrorists.' That is the first point. The second is that of course that information tells government an the enormous amount about us and we have to acknowledge the risks that data will be abused, but to my mind the

answer to that is not so much to put restrictions on the front end about what can be collected or the standards under which it is collected but to try to put restrictions on the back end to make sure that, when it is searched, it is searched for a legitimate government purpose and that every search is audited and recorded in ways that can hold the government officials who conduct the search to account.

CHAIR: For you, were there any surprises in the material that was released by Mr Snowden and then published in the *Washington Post*, *The Guardian* and other outlets? Was there anything there that surprised you or is that information reasonably well understood within the community that you operate in?

Mr Baker: I would say the only true surprise was the first revelation, that the government had collected the metadata for every phone record into, out of and around the United States. It was misleadingly presented—the collection was presented and all the restrictions on searching that data were withheld by Snowden and his journalistic allies for about two weeks, in what would have been considered an abuse of classified information if anyone else had done it.

CHAIR: Is it your view that the collection of that material was unconstitutional in terms of search and seizure techniques being turned on the whole American population?

Mr Baker: As a technical matter, no, it is not unconstitutional under existing law, and the courts, with one exception, that have looked at this have come to that conclusion. The constitution has limited application to information in which individuals have reduced expectations of privacy. On the whole, when you give your information to a third party, under existing precedents that data ceases to be yours and becomes that third party's, and it can be obtained in a fashion that does not implicate search but is simply the equivalent of a subpoena, just as a bank may be forced to produce its records about how much money you have in your account without it being a search or phone companies may be required to produce information about, essentially, billing records that they have that are their records, not yours. So it is not a search. It is potentially quite intrusive and deserves to be carefully circumscribed. In fact, as we found out after Mr Snowdon finally and reluctantly released the restrictions that he had also taken from the government, there were very strict restrictions on what searches could be performed on that data.

Senator MARSHALL: In your opening remarks you talked about the contradiction of letting companies take our data and use it for whatever means they see fit. But we will not let the government use it against terrorism, which is one extreme of what we are talking about. Of course, it brings up emotive sort of language, that of course we have to defend ourselves from terrorists. But what about tax evasion? What about kids maybe plagiarising other people's work to use in their essays at university? What about the whole gamut of things that might be seen as theoretically or technically illegal or, sometimes, seriously illegal? Should all that information simply be open to the government to wade through as they see fit, looking for whatever crimes they may deem as important at the time?

Mr Baker: That is a very good question. Remarkably, our debates here and the practice around the world have assumed that that is possible—that is to say, every criminal investigator in the United States begins a serious investigation by going to the phone company and asking for the call detail records of their principal suspect. They ask for that by serving a subpoena; they do not serve a search warrant. The ordinary expectation is that that information can be obtained by subpoena. Only when it was collected in bulk by the national security agency were questions raised and—

Senator MARSHALL: Mr Baker, do we still have you on the line?

Proceedings suspended from 9:12 to 9:15

CHAIR: Mr Baker, have we got you back?

Mr Baker: I am back! I have always aspired to have an unanswerable argument in front of a Senate committee. But I did not think they really had one.

Senator MARSHALL: I am not sure whether you finished your last answer. But let me just pose another proposition to you. I ask my friends whether they think the internet or, more generally, electronic telecommunications is now private. Generally, they do not believe that it is. That poses the question: should it be at all? It is relatively new technology. We have always seen plenty of examples in the newspapers of calls or emails that have been listened to or intercepted by people who otherwise should not normally have them. Given that it is probably not very private and I do not think people think it is very private, should we even have the concept of privacy applied to electronic communications at all and simply let anyone who wants it have it?

Mr Baker: I am not sure I would go that far. I do agree with you that many of the things that happen on the internet are nowhere near as private as we all would wish. But I think there is room for a law to bolster expectations of privacy, that people without any authority should not have access to our communications and if

they gain access they should be punished. But of course much of the problem is that we authorise so many people to have access to our communications. Of course, the government has to have access to some people's communications because some people are criminals.

Senator MARSHALL: We do authorise a lot of people to have access to it without knowing. How many times do we click on that box that says 'I agree' without reading the 20 pages of small print that come up with every app that we buy? In all of those situations, we are agreeing that they can harvest our information and use it as they see fit. But we are not particularly warned or advised that that is what we are agreeing to, either. Who could possibly read all those terms and conditions? After all, we want the app, anyway. So should we be looking at tightening up some elements of that? I think it is an issue: what are people's expectations? What is a realistic expectation and, when we find that or draw that line in the sand, should we then develop laws around that practical line in the sand?

Mr Baker: The difficulty that I see there is that our expectations evolve along with the technology. I often use the example of the right to privacy, which was invented in the United States by Louis Brandeis. He objected to the fact that Kodak had invented a camera that allowed the hoi polloi to take his photo. We have all got used to the fact that our noses look a little bigger in photos than we thought they were. We no longer think it is an invasion of our privacy to take a photo or even put it up on Instagram. Unfortunately, we did take the Brandeis spiel and write it into law and we are still stuck with peculiar laws that seem to think that taking photos of someone is a violation of their privacy.

You do have to be a little careful about saying, 'Let's take people's expectations and write them into law,' because if the technology does not support it, in the end neither will the people, because their expectations will evolve.

Senator IAN MACDONALD: Mr Baker, I see on your website that you wrote a book called *Skating on Stilts: Why we aren't Stopping Tomorrow's Terrorism*. Obviously I should buy the book to get the answer, but basically: why aren't we stopping terrorism?

Mr Baker: You can download it for free, because it is Creative Commons licence, but I would be happy if you bought it. The short answer is that I blamed a kind of unholy alliance of business and privacy activists for making it very difficult, even when you can see a disaster coming, to take action against that disaster until it is upon you. There is just a deep conservatism about taking action based on even reasonable fears about what is going to happen as a result of technological trends. We are seeing that today with cybersecurity, where your privacy invasion has made it very difficult to prevent the people's liberation army from invading all our privacy.

Senator IAN MACDONALD: What would you think United States or world opinion is on the proposition, which I would basically hold, that I would rather be alive and lack privacy than dead and have my privacy intact?

Mr Baker: I actually think that that is a majority sentiment in every country, although less so in the United States where, ironically, the most fervent believers of both the Republican and Democrat parties tend to be sceptical of that proposition, at least when there is a Democrat in the White House. Even here, when you argue about the value of a program to prevent terrorism, a lot of people who are not particularly passionate will agree with you; the problem is that the passion tends to be on the other side.

Outside the United States, governments—whether they are reflecting their people's view or not—are almost uniformly of the view that the United States has exported far too much security and not enough government access.

Senator IAN MACDONALD: With this recent tragedy in northern Europe, are you aware, if there were telecommunications about, there would have been the possibility of that happening before it happened?

Mr Baker: I do not know.

Senator IAN MACDONALD: There is no comment about that?

Mr Baker: I have not seen anything about that at this point.

Senator IAN MACDONALD: Thank you. Would this telephone conversation be being heard by others? It is a public thing in Australia, but would someone be listening to your end of it?

Mr Baker: I find that highly unlikely, because I think it is unlikely that someone would have a basis for considering me a criminal or an agent of a foreign power. But I will say that when you make an international call there are at least two governments that have the possibility of intercepting it, so it is not prudent to assume that international calls are free from surveillance.

Senator IAN MACDONALD: Which are the two governments?

Mr Baker: The government of the calling party and the government of the called party—and, of course, everybody whose territory is crossed by the cable in between.

Senator LEYONHJELM: Mr Baker, I note you said that you are less concerned about collection of data than you are about how it is used. Have I understood that correctly?

Mr Baker: I think it is foolish to try to regulate collection, because that is moving against the direction in which the technology is pushing us.

Senator LEYONHJELM: Do you distinguish between data that has to be collected for just getting things done—such as downloading an app—and data that has to be collected because of a government mandate and for no other reason?

Mr Baker: I take it you are thinking of a data retention requirement.

Senator LEYONHJELM: Yes, but I think also it could apply to phone records. Once the billing has been undertaken and completed, there is probably no further need to retain that data. Is that right?

Mr Baker: Absolutely. I do agree, and the governments of the world have struggled with two possibilities. One is to require the phone companies to hold on to that information. This is a development of cheap telecommunications. It used to be that every call helped to determine what your bill was going to be. Now it is all more or less free and therefore there is no need to keep detailed records for any length of time about who you called and how long you talked. That information is still used, because the switch still has to deliver your call, but it may get rid of it much faster than phone companies used to. But it is enormously valuable in determining your social relationships, the people you are doing business with and the like.

There are two solutions for that new technological trend. One is to have the phone companies or the ISPs keep this data; and that was the European solution and still is, although obviously the European courts have begun to restrict that. The other solution, that the US adopted—at least the National Security Agency and the government believe—is that collecting the data and storing it in one place and watching it carefully was a more prudent approach. Both have their disadvantages and their advantages. It is clear in the US that the government collecting this data has turned out badly because it was done in a classified environment and in a way which was then exposed in a fashion designed to create a bad reaction. But there certainly are objections to it, on the theory that letting the government keep this data means that abuses are easier for the government than if it had to go to the phone companies and ask for it. But having the phone companies keep it raises the problem of: one, they don't want to; two, they may not have the same kind of security interest; and, three, you have to go to them for every search so it is actually hard to search the data except in very predictable ways. You could go and say, 'Here's a name; tell me what calls he has made,' but you could not as easily say, 'Tell me everybody who placed a call from the site of this crime at the time of the crime' without having to go to each carrier and ask for a different sort of search. There are disadvantages to both of those solutions. I am a bit agnostic between the two. On the whole I would probably say that having the government keep it is more prudent—if people are willing to trust the government, which is a bit 'if'.

Senator LEYONHJELM: That is quite a big 'if'. Do you distinguish between data that is collected for a commercial purpose—such as a voluntary exchange for a service or a product or something like that, and the company then retains the customer information—and data that is collected under a government mandate for no commercial purpose? Do you distinguish between them or do you think they are both the same?

Mr Baker: I find it hard to believe that the second category could exist without a substantial amount of publicity, so that at that point it is known that if you use this service, if you carry out this activity, records are maintained. At that point, it is not much different from knowing that your pharmacy keeps records of the drugs that you buy. I am not sure I would distinguish greatly between closed-circuit cameras placed by the municipality in public places and closed-circuit cameras placed at the front of business by the business. At the end of the day, both of them are taking my picture and both of them will be used by the police to investigate crime.

Senator LEYONHJELM: Say the data is retained as you are suggesting, and we are not too concerned about the fact that it is being collected but we are concerned about it being used, so the focus is on access to the data and what it is used for. Do you have any thoughts as to how that could be used for the right purposes—in other words, to catch criminals, and not for what we hear all the time: police looking up the addresses of pretty girls or catching their neighbours out doing something and that kind of thing?

Mr Baker: I think actually that kind of abuse is much easier to catch today than it was 20 years ago, but it requires some money and some will. Yes, every search that is done in a database can be logged and it can be subject to audit. It would not be extraordinarily difficult to pop up a little box when a search is done—maybe every 10th search; maybe every third search—that says, 'We see you are doing this search; would you please

record your reasons for this search in a sentence or two for later audit.' I think that is much more likely to prevent the kinds of abuses you are describing than turning it into a felony and occasionally sending a police officer to jail. A regular process in which people are disciplined for misuse, and maybe disciplined pretty severely, and which relies on the ability of our increasingly sophisticated computer networks to keep track of all of that is well within the capability of existing IT.

CHAIR: We are running very close to time. I have one final question and then we will let you go. Australia borrows a lot of its legal and cultural norms from the United States. We do not have your bill of rights, but we have, I think, benefited from the development of that in the United States, as have many other countries, and the balance that has been struck in recent decades in terms of state intrusion into the life of the individual has been that it needs to be targeted and discriminate, and it needs judicial oversight, and so the balance has been struck with a warrant. That is a tradition that Australia and many other democracies have adopted. You have already indicated that you believe it is legitimate for the state to effectively set that aside, for metadata snooping in particular. The courts and that judicial oversight has been entirely bypassed. Do you support the fact that that decades-long consensus has been set aside? And for what reason do you think we have moved beyond that balance?

Mr Baker: It has been set aside, I think. When we are talking about metadata, there really has never been a judicially-created restriction on access to that metadata, except in real-time—immediate access to content. That has emerged from tradition, and the tradition was: this is not even the subscriber's information; it is the information of the telephone company, and if they can be compelled with a subpoena to produce their revenue figures, they can also be compelled to produce subscriber information. And the courts have generally not been particularly good at making fine-tuned restrictions on that information. So even in the United States, with all of the litigation and the constitutionalism of our political debates, the vast majority of the restrictions on government access to this kind of data has grown out of legislative restrictions, not judicial restrictions. I guess I would say that we have pioneered a little the idea that you can set rules for how the data is searched, not just how it is collected, and then have a neutral magistrate enforce those restrictions. So you certainly can have a role for courts by asking them to make sure that the rules that have been drafted for searches are actually carried out.

CHAIR: Thank you, Mr Baker. We greatly appreciate you taking the time at an unusual hour to lend us the benefits of your experience.

Mr Baker: My only regret is that I did not get to come to Sydney.

KELLOW, Mr Philip John, Registrar, Administrative Appeals Tribunal

[09:35]

CHAIR: We now welcome Mr Philip Kellow. The committee has not received a written submission from you. The Senate has resolved that an officer of the Commonwealth or of a state shall not be asked to give opinions on matters of policy and should be given reasonable opportunity to refer questions asked of the officer to superior officers or to a minister. This resolution prohibits only questions asking for opinions and does not preclude questions asking for explanations of policies or factual questions about how and when policies were adopted. Officers of a department are also reminded that any claim that it would be contrary to the public interest to answer a question must be made by a minister and should be accompanied by a statement setting out the basis for the claim.

Would you care to make an opening statement before we proceed to questions?

Mr Kellow: I thought it might be useful if I just try and paint a brief outline of the role of the Administrative Appeals Tribunal, which may set some parameters around the assistance that I can provide to you. I have to give a slight disclaimer in that I am not a nominated or authorised person under any of the relevant legislation so I have had no personal experience of dealing with the warrants. Similarly, because of the secrecy provisions, there is not a lot of information disclosed by members as to the actual content of their deliberations when they are asked to consider them. So in that context, there are some limitations.

The AAT members undertake work under the relevant legislation in their personal capacity—the persona designata type role—which is an extension of that which was originally established for our judicial officers to undertake that role. At present there are 33 members around the country who are nominated under the telephone interception and access legislation. They are located in every state and territory except for the Northern Territory where we have no members. There is a slight gap in Hobart at the moment because the deputy president who had that nomination's term has ended and we are just waiting on government appointments to come through.

The tribunal, as an organisation, has no formal role or responsibility in the persona designata work of the members. But over time we have assumed a fair bit of organisational support for them. The tribunal as an organisation facilitates the nomination and authorisation process. It is the contact point between the relevant officers in the Attorney-General's Department and members to make sure they complete consents and provide other information that is relevant to that process. Once members are nominated then the tribunal facilitates access, so provides the initial contact point for the law enforcement agencies seeking a warrant. That is generally through district registrars and includes an after-hours service. The tribunal also provides facilities such as offices and secure spaces for those discussions to happen; it arranges for the remuneration of members who perform those functions; prepares various guides and internal resources or try and leverage off those sorts of resources that may be developed by other law enforcement agencies. Over the years it has had access to material provided by the Commonwealth Director of Public Prosecutions or the Australian Federal Police, which really is an outline of the legislative framework relevant case law or other factors.

The tribunal organises training. It would be fair to say that with the appointment of Justice Kerr, the tribunal has tried to strengthen the training and support for members exercising their role. I think the context there is that the majority of members do not come from a criminal investigation background; they are generally appointed for their expertise in administrative law, merit review or particular areas of civil jurisdictions, for example, tax, social security, veterans' entitlements and so on. To try and ensure that there is a greater understanding of their responsibilities under the telephone intercept and similar legislation and how to undertake them, the tribunal has provided training. A full-day seminar was conducted in late 2012 which tried to cover a range of areas from stepping through the investigation process through to how information obtained through these sorts of warrants is used in the criminal process through the courts.

In recent years, the main way the tribunal has measured the workload is simply in appointments. So an appointment with a member may involve a number of applications and each application may involve a number of warrants. So the tribunal does not drill down into the actual number of applications and warrants; it relies on the Attorney-General's annual report. The tribunal does not provide statistical information to the department for that purpose but obviously it does have an interest in data—I will come back to that in a minute.

The tribunal's workload is couched in appointments. Over the last three years it has had well over 2,500 telephone intercept appointments each year so all up a bit over 7,500. The bulk of those are in New South Wales. About 1,700 each year are made in New South Wales. That has meant that, as the tribunal has increased, appointments can disrupt our core business of conducting merit review by having to take members offline to deal with those requests. In New South Wales that has led to arrangements where basically an afternoon each day is set

aside and a member is available to deal with those requests—but it is an impost. It would be remiss of me not to mention that the costs of paying the members to do this work and to provide the support exceed the fairly modest supplementation the tribunal got in 2004-05 when it first started to have a major role in providing these sorts of authorisations.

In recent years the members have become increasingly sensitive to media reports which tend to coincide with the issue of the Attorney-General's report. The data is at such a high level it really does give a fairly black and white yes and no type of count. On that sort of count it generally looks like most requests for warrants are granted by AAT members and, for that matter, the other nominated officers. The tribunal has been in discussions with the department about the desirability of providing more consistency and some greater granularity in how work is measured. To that extent, both in the tribunal's annual report last year and in the Attorney-General's annual reports there were some case studies to try and illustrate the things that may happen prior to a grant being made. I guess the three main things that can occur are: requests for further information, which may have to lead to supplementary affidavits being provided—so it is testing some of that evidence; the imposition of conditions; and, on occasion, not granting the warrant for the length of time that may have been in the original request.

So there are various things that do occur which indicate that members do take the role seriously, that they do explore the issues and the appropriateness of issuing the warrant but it may not necessarily result in a blanket 'no'; it may lead to some refinement to make sure there are adequate protections or that the nature of the investigation or the warrant is proportionate to the matters before the investigating authorities.

It would be fair to say there is a large number of law enforcement agencies that can now rely on the legislation. Flowing from that is a wide range of practices and quality in the nature of the requests and the supporting material.

The tribunal has raised with the department the desirability of having a more uniform approach to some of these things. I understood, from the secretary, that you were interested in the Public Interest Monitor. I can give a few comments but it might be better to leave that to questions.

My final point is Justice Kerr as president has raised for consideration with the department the possibility of conferring the powers under the legislation on the tribunal rather than as individual persona designata functions. That would allow some greater scope and greater recognition for how that process could be managed and supported.

CHAIR: How many more people would that allow to undertake those functions?

Mr Kellow: It is in the criteria set out in the act as to who is qualified to undertake that role. I think in broad terms the numbers are probably adequate; it is more just this year's impost in not having that recognised. From an organisational point of view, we see it as something we have had to accommodate within our core functions. If it was recognised then it would provide a slightly stronger framework for the allocation of that work—and picking up on the point I made about inconsistencies in form and structure—not the actual content but how it is presented. Trying to streamline things in a more consistent way would open up the opportunity for the president to give some guidance to law enforcement agencies as to how we would expect requests to be made and how affidavits should be structured and so on.

CHAIR: That consistency seems very important to me. What is precluding you from providing that guidance at the moment?

Mr Kellow: It is because the functions are performed in a personal capacity so there is really no authority for the president. We could suggest or have discussions. In some instances where law enforcement agencies have raised some concerns about their relationship with particular registries, we have tried to look at ways of enhancing that. One solution in New South Wales, given the volume, was to try and make it clear that we would always have someone available every afternoon to undertake that work and so on. We could do it but there is no structure for that to happen.

CHAIR: That is interesting. Just to be very clear, you do not have any visibility of the warrantless meta data requests that are 100-fold higher than the material that you deal with?

Mr Kellow: No, I am not aware of that.

CHAIR: We might set that aside just for the moment. Is the vast majority of the material that crosses your desk from New South Wales over the odds per capita or is it just that it is the largest state?

Mr Kellow: There are probably others better placed to comment on that. My own view is that it is probably a reflection of it being the largest state, and having different law enforcement practices as to the role of those invasive tools in the investigatory process may alter it between jurisdictions. Queensland is a recent entrant under

the scheme so we do not have a lot of experience there. And it has the Public Interest Monitor, which we also think may have had some impact on the numbers that come through.

CHAIR: That would be rather instructive if that were the case. Will you spell out for the committee the role the Public Interest Monitor is playing and whether you would venture a view on behalf of the AAT as to whether you think that is a useful addition having that Public Interest Monitor there. My understanding is they provide something of an adversarial ingredient to the process: do you really need this warrant? Do you really need it to be that far reaching? Is it your view that that is actually suppressing the number of requests that are coming out of Queensland?

Mr Kellow: I think it might be a factor. The public interest monitors are now operating in Queensland and Victoria—Victoria is a slightly more recent jurisdiction to introduce the monitor. I think it would be fair to say that our experience was that the number of requests did drop in the early days of the monitor being there as the law enforcement agencies had to get on top of how the monitor was going to operate and provide that devil's advocate, testing, filtering process.

We have discussed internally with members how they have found the Public Interest Monitor. I think in broad terms they feel it has improved the quality of the requests and the supporting material and that, on occasions, when the monitor has taken a fairly active role in helping test some of the assertions and the need for the warrant or its breadth, the members have appreciated that assistance. I think it comes back to my earlier point that a lot of our members do not have a significant criminal investigatory background, so it is of assistance to have someone generally drawn from the criminal bar or with other appropriate expertise to be able to test things that the law enforcement agencies may be putting up. I think it assists the process in that sense.

From our early experience with the Public Interest Monitor in Victoria, because it was a novel scheme and everyone was learning, we found it made the process a bit longer. Now that the public interest monitors are more assured about their role and how they want to perform it and how the law enforcement agencies engage, I think that has gradually become more streamlined. We have seen the numbers gradually starting to increase again.

CHAIR: In the meantime, it did streamline the amount of work coming across your desk?

Mr Kellow: I think it has improved the general process from our members' point of view.

CHAIR: I think it is broadly agreed—maybe for very different reasons—from the Secretary of the Attorney-General's Department down, that the T(IA) Act needs substantial renovation, if not burning down and rewriting from scratch. What would be your top picks for reforms to the legislation and the way it operates?

Mr Kellow: Personally, I do not have any great expertise or knowledge about the act. There are certainly things that we have raised. Any simplification to make the factors that have to be considered easier to have regard to and so on would be a good thing. I think we have had some discussions from time to time around the appointment provisions. In terms of the T(IA) Act, it has probably been more around some of the administration, where it can take quite some time to have members nominated and put through that process. There are certainly inconsistencies. At last count we have coming up to about a dozen pieces of different legislation where we have members authorised to perform particular functions. I think almost all of them have slightly different qualifying criteria and different appointment processes. It would be good to have a harmonised approach to those sorts of administrative affairs.

We have had issues around whether the identity of members who have issued warrants can be disclosed and in what circumstances. There are obviously often very serious offences and people who may be undesirable to expose risks, so we would like some protections there. I guess the prima facie identity is not disclosed unless there is good reason and it contributes to the judicial process if it gets to that point.

CHAIR: We are a little short of time, but feel free to point us to any case law or any particular instances, if you like, on notice rather than here at the table, where that did present a problem.

Senator IAN MACDONALD: For the record, what do members dealing with warrant applications have to be satisfied of?

Mr Kellow: I do not have the detail. It is in the legislation. There are provisions about the factors that they have to have regard to. There are various factors as to the nature of the investigation and the contribution that the warrant might make to it, and then there are issues around privacy, protection of personal information, impact on third parties and those sorts of factors.

Senator IAN MACDONALD: Are applications to members normally five minutes, 10 minutes, an hour, half a day?

Mr Kellow: It does vary a little bit between members. As in most things, we notice that the longer members have been doing it, the slightly quicker they seem to get through the work. As always, there are some who may take a slightly longer time than others, for reasons that may be just about their personal comfort and how far they want to explore. It ranges from very straightforward ones, of maybe 15 minutes, through to a couple of hours. There are certainly ones where it is a bit of a stop/start, where a member reviews material and then wants clarification or additional material. Sometimes that can be provided fairly quickly; other times that may require effectively an adjournment, to use that expression, to allow the law enforcement agency to provide that additional information.

Senator IAN MACDONALD: I should know this, but, for the record, when the principal application for the warrant is made on the papers, supported by affidavits, is it normal for the member then to have a discussion or examination of the applicant?

Mr Kellow: There are slightly different arrangements with different law enforcement agencies. Some let you effectively provide the deponent or the investigating officer will have the carriage of the request. I think New South Wales police send a representative whose main job it is to liaise with the various members and obtain warrants. Then, if there are queries, that person has to try and contact the investigating officer to provide the additional information. I think it is a volume issue—and obviously location too. There will be times when the investigating officer may not be located in Sydney, Melbourne or wherever.

Senator IAN MACDONALD: Is there a standard of proof for the member? Do they have to be satisfied beyond a reasonable doubt or on the balance of probabilities, or is it just based on it probably being a good idea to issue the warrant? What is the standard?

Mr Kellow: I do not know. I suspect it would be balance of probabilities rather than beyond reasonable doubt.

Senator IAN MACDONALD: Thank you. I will read section 46.

Senator MARSHALL: I was going to ask how long it takes, too. You said you do not collect a lot of data about the percentages of applications that might be accepted, rejected or modified. Do you have a ballpark figure? The Public Interest Monitor, I think, is a very interesting idea, but does it run the risk of encouraging law enforcement agencies to ask for more than they actually want on the basis that it becomes an adversarial thing where they think, 'Let's pitch high to get what we need'? I would have thought that in this space we would actually want to encourage law enforcement to say, 'This is exactly what we need and why we need it.' I would not see 100 per cent acceptance, therefore, if that was the attitude they were taking, as anything untoward at all, but the minute we get the adversarial nature in there you would expect 80/20 or 50/50. If it was not that, where do we go with that? Do you see that as creating problems? From what you have indicated so far, you probably see the reverse, but I just wonder why.

Mr Kellow: Again, I have to emphasise it is anecdotal and second-hand, but certainly the comments from our Queensland members, who have been dealing with the Queensland Public Interest Monitor, have been that, in fact, the requests by the law enforcement agencies have been much more realistic and less ambit, knowing that they are going to be tested. So, in a way, it has provided a bit more of a framework for them to think seriously about how long they actually need to have the warrant in place, what the breadth of it should be and so on. So I think in that way—

Senator MARSHALL: I guess it logically follows, therefore, that prior to that there were ambit requests being accepted.

Mr Kellow: Or that the members had to try and draw those parameters themselves.

Senator LEYONHJELM: You said a large number of law enforcement agencies rely on the legislation and take advantage of it. I think of ICAC in New South Wales and New South Wales police as accounting for the predominance of New South Wales requests or applications for warrants. Do you know who else applies for them? Is there a relationship between ICAC, the Crime and Misconduct Commission and those sorts of organisations and the number of warrant applications, or is there some other source?

Mr Kellow: In terms of the number and who they are, it is probably best to refer to the attorney's annual report that does set out—

Senator LEYONHJELM: That is published, is it?

Mr Kellow: No, the New South Wales Crime Commission has capacity to seek warrants under the investigation. In general terms, I would say that in New South Wales the bulk of the work comes from the New South Wales police. With ICAC and other agencies it tends to come in waves, and I think it coincides with how many investigations they have on foot and what point those investigations have reached and what they might be

needing. It is sheer conjecture, but I imagine where there are joint investigations that may involve a number of law enforcement agencies there is probably a lead agency nominated to seek those sorts of permissions.

Senator LEYONHJELM: My alarm bells went off when you said there are a large number of law enforcement agencies that rely on the legislation and that the functions are performed in a personal capacity. So there is no inherent safeguard, I suppose. It depends on how the member approaches it individually, so there is potential for substantial variation. Do you think there is substantial variation?

Mr Kellow: That is not my sense. All members take the role very seriously. We know that over the years the involvement of judicial officers has declined, in this space, so the members are very aware that they do the bulk of the applications and they do take it seriously. When we conduct training and provide guidelines—I mentioned that when we have had some access to externally prepared guidance we have done a lot of work ourselves to try to provide some sort of quickstep guidance to sit on top of it, to make it a bit easier to navigate, because it can be fairly dense material. In broad terms, the figures show that applications are ultimately granted, albeit they may be subject to conditions or not applied in the form of the original request.

CHAIR: That is a very important question and is potentially something that we might make a recommendation on. How do you ensure that there is consistency across the range of people apart from the training and induction that you obviously need to do? How can you be sure that some people are not being unnecessarily permissive and others restrictive?

Mr Kellow: We cannot guarantee it or be absolutely sure. We have a warrants committee comprising very senior members who have significant experience in undertaking that role. That really covers the main jurisdiction where the work arises, and they are in contact with the members and try to monitor how things are going. Ultimately, we have no official oversight as to how those functions are performed and to detect if there are particular trends or issues.

Senator IAN MACDONALD: You could ask the same question of the judiciary, I might say.

CHAIR: Unless others have urgent questions, we might let you go. I am very grateful for your time and expertise this morning. It has been very useful.

ALTHAUS, Mr Chris, Chief Executive Officer, Australian Mobile Telecommunications Association

FROELICH, Mr Peter, Industry member, Australian Mobile Telecommunications Association and Communications Alliance Ltd

RYAN, Mr Michael, Industry member, Australian Mobile Telecommunications Association and Communications Alliance Ltd

STANTON, Mr John, Chief Executive Officer, Communications Alliance Ltd

[10:04]

CHAIR: Welcome. Thanks very much all for talking to us today. We have received your submission as submission No. 16. Do you wish to make any amendments or alterations to your submission?

Mr Stanton: No.

CHAIR: Would any or all wish to make a brief opening statement before we take you to questions?

Mr Stanton: Yes we would. Thank you very much for the opportunity to appear today. We certainly welcome the work of the committee and we agree there is a case for reform. We are supportive of some of the recommendations that have come down from the PJCIS, but at the same time it is fair to say we are wary of the nature of some of the proposals that we are seeing put in front of the committee. I would like to start with a couple of comments around simplification, streamlining and deregulation, which many of the recommendations go to, and then my colleagues will cover other aspects of our submission.

The communications industry is certainly supportive of the present push by the government for red tape reduction and deregulation. We are making great progress in our portfolio on reforms, and that is very heartening. At the same time, we are concerned with the swath of proposals that we are seeing advanced or contemplated by law enforcement agencies and the Attorney-General's Department that have the potential to drive that red tape initiative deeply into negative territory. We have spoken to the PJCIS in the past about the potential costs of data retention being more than $500 million, substantial costs that may be involved in the proposals for a new scheme around network infrastructure security and potentially high costs for industry around online copyright enforcement. These have the potential to dwarf the entire red tape reduction achieved across all portfolios.

A number of the proposals—and we will go into more detail on this—tend to be, in our view, an exercise in shifting to industry costs that will ultimately be borne by consumers. In our submission we have emphasised the principle of cost recovery from law enforcement agencies, which we feel should be enshrined in any reforms partly because that also acts as a natural curb against excessive requests for activity by law enforcement agencies and encourages them to target their activities.

And it is not just the shifting of costs we are worried about; it is also obligations to service providers who at the end of the day are not police and can sometimes struggle to deal with requests if they are required to process issues in which, frankly, they are not trained.

I move to some of the recommendations. We agree with recommendation 3, that there is scope to rationalise and reduce the reporting requirements that presently exist. Our submission spells out how that could happen. We also see merit in recommendation 10 and believe that the minimisation of references and warrants to internal carrier or service provider processes will allow savings. Equally, recommendation 9 has some merit in its focus on streamlining legislation, and we have spelled out the various areas of duplication and ambiguity between the Telecommunications Act and the Privacy Act. We think there is some scope to do some good simplification there.

We were a little struck by some of the comments that were made by David Irvine to the committee recently. He talked about data retention helping law enforcement agencies to deal with very considerable procedural and time-consuming bureaucratic processes. If in fact that was a reference to processes within ASIO or law enforcement agencies, we would certainly support an attack first on streamlining those processes and removing the difficulties rather than relying on over-the-top solutions to what ought to be a root-cause solution.

I would like to now hand over to Mr Althaus.

Mr Althaus: Thank you. I wanted to make a few observations. One of the hot buttons in this space is data retention. We have made some comments on this issue over time. It is fair to say that as recently as three days ago a senior member of a carrier that is a member of my organisation said to me lamentingly that he still did not quite understand the defined data set that was being sought. I think that is an issue of concern. Clearly, in this day and age information flows are not only huge but increasing in some spaces exponentially. They are also borderless in the sense that all of us on a daily basis I am sure traverse many websites and destinations outside of Australia.

Industry has long had a concern about the level of information that is retained by itself for commercial purposes versus information retained for other purposes. We also underscore the fact that there is a long and deep partnership that already exists between industry and law enforcement agencies. We are keen to be part of the solution, not part of the problem, but one of the large concerns that Mr Stanton has just alluded to is this cost-shifting exercise whereby a large quantum of cost in this law enforcement and national security space is ending up within industry.

To give you a picture: data volumes in the mobile space alone are predicted to increase by a factor of 10 between 2013 and 2019. Should we have to build a system to retain data for a lengthy period, it is not just as simple as pushing a button or tapping an existing resource; in actual fact we would have to duplicate the data. That duplication would be required because this data comes from a multitude of IT systems within carriers. To be helpful to law enforcement agencies, it would need to be duplicated and aggregated. Then we have to store it. I am sure there is a vacant suburb somewhere where we could build a data centre! Then we have to manage it and be able to interrogate it. There are the privacy and security issues that go with that. All of these things are very considerable issues to address; and, as Mr Stanton also observed, we are not a law enforcement agency. We are a telco. We are an industry.

Typically, staff are not trained. Typically, our staff are not covered by the same legal protections that, for example, members of the law enforcement community would have. Five hundred million dollars is a large amount of money, and it would be interesting to see what that wold do in the broader law enforcement world. We do have concerns about the efficacy of such a large data retention pool. Clearly, the UK has grappled with this recently, and one thing we draw a big black line under when we talk about the UK is that the government in the United Kingdom funded the system and the agencies that use it pay for their use of it. That paradigm does not seem to be in our thinking here.

So there is a huge amount of resource, a huge amount of impost and efficacy we have a question mark around. Similarly, in our submission we go to the issue of attribute based warrants. Once again, we are not confident of the definition of this new approach. The intuitive concept of being able to take a thin slice of data to be more efficient and effective is appealing, but for us we would have to capture and hold everything to enable that slice to be found and processed. Similarly, attribute based warrants are once again passing a responsibility into telcos to interpret, judge and react to warrant requests in a more forensic way than simply downloading the data and handing it over. These sorts of transferences of responsibility, cost and performance to us present a significant dilemma. I will stop there because I know we want to get to question, but data retention and attribute based warrants are two very glaring examples of some of the challenges that we face. I underscore the fact that we want to be part of the solution, not the problem.

CHAIR: Thank you very much for your opening statement and for your evidence. Let's start with the cost estimates—the half billion dollars. I understand that is going to be an approximation, but at least you have had a stab at it. That is either passed on to industry and then you have to pass it on to your customers or it is, as you say, absorbed by the agencies, which is then charged back to us all as taxpayers. So there is kind of no avoiding it, is there? People are going to need to pay for this one way or another. Tell us what the $500 million buys us. Is that set-up costs only? What does that actually look like? Where does that money go?

Mr Althaus: We have looked at set-up costs. It is an estimate, as you say. It is also an estimate based on what we understand is the task. There is some further clarification required there, but certainly, when we did the back of the envelope, we were looking at set-up and operational costs. Suffice it to say there is some great concern around definition. So it is difficult to be precise, but it was not long before we were in the hundreds of millions. Then, when we start looking at volumes of data that are projected, that number began to escalate. My colleagues might want to add to that.

Mr Stanton: I think the other point about this ultimately being borne by the taxpayer is fair enough, but I think the difference is that if it were to be included within the budget of the agencies then the agencies have to fight for those funds, and that puts a natural discipline on them They have to justify it. It will tend to rein in the expansiveness of the sorts of requests, systems and facilities they might want to have in place. I think it has some internal rigour which is attractive.

CHAIR: Okay. I guess it is attractive from a commercial point of view as well. Between you, you collectively represent everything from the very largest to the very smallest players in these markets. A Telstra—very large institutional capacity, very strong technical background—can potentially absorb some of these costs. Are you concerned that, if the burden of paying for these systems does need to be absorbed by the industry, that is going to hit smaller players much harder than larger ones?

Mr Stanton: I think it would tend to hit them differently depending on their size. A large organisation like Telstra, sure, has capacity, expertise and all of that but also a vastly larger number of databases that it has to interconnect and be able to interrogate. If you go down to the smallest of players, you have a simpler task, but they may be in a position where they end up doing this effectively manually. So the unit costs could end up being higher for a smaller player, but the capex could be much less because it is effectively an opex-type exercise rather than a capital one.

Mr Althaus: Notwithstanding the size and dimension, quite a number of the tasks here are, as we have alluded, moving us outside a typical business service environment even for those that are already servicing agencies substantially, particularly in the data retention context.

CHAIR: With regard to the system as it stands at the moment before we even start talking about data retention: there are something in the order of 320,000 or 330,000 warrantless metadata requests being sent to your members every year. That number is also growing quite rapidly. Talk us through how that looks from your end process-wise. I understand what happens at the agency end—they fill out about a four-page application that is ticked off internally. How are these things delivered to your members, and what happens when they are?

Mr Ryan: You talk about a warrantless application; we tend to refer to them as 'lawful requests'. We ask the agencies. It is not just agencies but also police forces as well.

CHAIR: Local governments, the RSPCA—we know they are there.

Mr Ryan: They all try, yes—including the ACMA, too. They all do it under such sections as 284 or 287. Some send them electronically. Some fax us those applications.

CHAIR: Faxes still exist?

Mr Ryan: Yes. It is a bit of a concern going forward, but anyway. They send us those applications and we will then extract the information. It falls generally into two areas. One is personal information. So, Senator, they may send us your phone number and they want your name, address and possibly what the service is. That information is extracted out of an industry system called the IPND, the Integrated Public Number Database, which was set up in about 1998 to service both law enforcement and emergency services. That is where the majority of those what you call warrantless requests, and we call lawful requests, are received to fulfil.

CHAIR: I guess the reason I make that distinction is that some of the requests that you get for more intrusive surveillance are warranted—they have been through either the AAT or a judicial process. That is why I make that distinction. Maybe for the AMTA folk: there was a bit of reporting, maybe three or four weeks ago, about the use of tower dumps here in Australia, where, rather than going after a particular record, someone will come to you and say, 'We want all the traffic off the cell tower within a defined period of time.' How do those requests come to you and how hard is that to provide?

Mr Ryan: I am not saying that all carriers or ISPs actually respond to those sorts of requests.

CHAIR: That is a very interesting thing to say. What lawful power do you have to resist such a request when it is made?

Mr Ryan: From our perspective, we look at it as: are they reasonable or not?

CHAIR: What is your test for reasonableness? Where is that written down?

Mr Ryan: We use both the T(IA) act and the Telecommunications Act to make those decisions.

CHAIR: So these are requests, not demands?

Mr Ryan: Yes.

CHAIR: That is very interesting.

Mr Ryan: Generally they are not requests for tower dumps, or cell dumps, as you suggest; they are actually single requests for location.

CHAIR: The location of a particular handset, for example?

Mr Ryan: Yes.

CHAIR: I understand that, but I understand also that you do get requests sometimes if a car accident or a particular awful thing happens within an area covered by a particular cell tower—or a crime is committed—and you are asked to provide all the traffic that transited through that point at a period of time.

Mr Ryan: We request the agency to supply us with the handsets that they are after.

CHAIR: Just talk me through how that would work.

Mr Ryan: We are not too sure where they would get that information from, but they may investigate as to what handsets are in that location at that particular time and then give us the telephone number of those handsets.

CHAIR: How commonly are you having to have these—maybe 'arguments' is a slightly strong term; these negotiations with agencies? How frequently is that happening?

Mr Ryan: Not very often.

CHAIR: Okay, but it does happen.

Mr Ryan: It does happen.

CHAIR: With most of what we have heard thus far, it sounds fairly streamlined: a warrant goes through the appropriate process; it is served; you provide the information; the crimes are solved.

Mr Ryan: Yes.

CHAIR: This sounds really different.

Mr Ryan: But the warrant itself is usually related to one or two handsets rather than many handsets. We do not like, I suppose, the agencies fishing for information. We are very prescriptive in when we respond.

CHAIR: Sure, but then you are providing a public interest function quite separate to your role as an industry. I guess that is a statement rather than a question.

Mr Ryan: We try to make sure we stick within the law.

CHAIR: Yes, but it is quite a big call, because that kind of assumes that you believe that in some instances the agencies themselves are not, and that is why you are having to perform that function.

Mr Ryan: No. We do not believe they are not within the law. We prefer them to be within the law and more easily, from our perspective, to respond to their requests.

CHAIR: I am sure other senators have questions, so I will come back later if there is time.

Senator IAN MACDONALD: Mr Althaus, you mentioned a suburb might be free to store all the data. Can you give us some guess—it may be better than a guess—or some concept of what sort of space you are looking for to store all this data?

Mr Althaus: The technology around data storage is improving and changing all the time. Data centres are the fundamental bedrock of cloud services around the world, and data centres underpin all of the industry's operations. Certainly the numbers of data centres and the capacity within them—multistorey buildings chock-a-block full of servers, with huge air-conditioning units et cetera and power redundancy are common the world over.

In terms of a suburb, yes, there are more and more facilities required to be geographically located. The volume of data is increasing at huge rates. The other important point is when organisations within the industry look at the best commercial arrangements there is an enormous amount of data that is stored offshore. In terms of the location of information, the physical assets of data centres are certainly numerous here but equally there is an enormous amount that do not call Australia home.

Senator IAN MACDONALD: Could you identify a big data centre in Australia where data is currently stored?

Mr Althaus: There are many. In fact, there are quite a number of commercial enterprises that specialise specifically in addressing the task of supplying information storage management solutions that are selling their services to all manner of the IT industry.

Senator IAN MACDONALD: I am just trying to conceptualise it. Would it be a building as big as this one we are in? How many storeys?

Mr Althaus: Bigger and more numerous. I think the physical size of buildings depends on who is investing and whose services they are seeking to support. It is simply a matter of the facility will be built with the technology and the equipment to do the job.

Senator IAN MACDONALD: Are they usually in a remote area, in the centre of the city or wherever you can get land cheaply?

Mr Stanton: They are always close to good fibre connections and strong backhaul. In Sydney, for example, one of the primary data centres is down on the harbour near Darling Harbour. To look at it from the outside you could imagine it was a university building. It is a long building about four storeys high. It is very substantial. At least as big as Parliament House.

Senator IAN MACDONALD: If someone put a bomb under that and blew it up—

Mr Althaus: That would be a bad thing.

Senator IAN MACDONALD: It would, but what impact would that have? Would that data be gone forever or would it be stored somewhere else as well?

Mr Stanton: Typically, you would expect sensitive data to be replicated in a geographically diverse place and you would expect the data centre to be on a self-healing fibre loop, if you like, so that you do not physically take a piece of the network out. You would hope that the redundancy provisions kick in almost immediately and that the data is still available. What that means of course is you have incurred a lot of additional cost in replicating data and facilities to give yourself that security and that is what feeds into the sorts of high numbers that we talk about when we look at what data retention could mean.

Senator IAN MACDONALD: Is there an alternative though?

CHAIR: Paper.

Senator IAN MACDONALD: Paper? Now you are really talking! Some data has to be kept.

Mr Althaus: The short answer is: no, not at present. Cloud services are what we commonly see now as the way of the future in terms people not holding as much data themselves and their data is in the cloud or in a data centre somewhere. The speed and performance of networks enables access and management of those data resources to occur in an efficient and effective way. We are still struggling in this day and age with not only the volume, especially in this data retention context, but also the ability to store, manage, interrogate and protect privacy and security. Those things are all germane to the overall bill here. In the data retention context, as we said, to a large degree it involves some duplication of what is already going on.

Senator IAN MACDONALD: I will finish there, Chair, but you have just deflated me. When I log onto my cloud, I do not know quite what it means, but I always thought it was something in heaven that looked after my stuff.

CHAIR: It is building in an industrial park somewhere, Senator Macdonald.

Senator IAN MACDONALD: That is a disappointment.

CHAIR: It is not quite as romantic as it sounds.

Senator LEYONHJELM: You refer to this huge borderless data issue and you have talked about the fact that a lot of the data in relation to Australians, if it is stored, if it is retained, it would actually be stored offshore. Does the reverse occur? Do you face dealing with inquiries for data from countries, the UK for example, that already have data retention requirements? How do you deal with them if you do?

Mr Froelich: I suppose, strictly speaking, industry members do not deal with foreign agencies. All foreign requests would be filtered through the Australian Federal Police generally under the provisions of any international mutual assistance agreement. So strictly speaking, no, we do not deal with foreign agencies or intelligence groups at all.

Senator LEYONHJELM: All right. On the assumption that only the Americans can claim extra territoriality of their laws, if Australian data was stored and the data centre was in a lower cost country than Australia, which would almost be inevitable you would think, how would you deal with that in that case? Would you only be obliged to search the databases stored within Australia?

Mr Froelich: It depends on how a particular lawful request is formed to the industry member. For each group, if you have things hosted in a different geographic location then obviously you are subject to the laws of that geographic location. If that information traverses Australian networks or Australian territory, then under the rules in the Telecommunications Act and the Telecommunications (Interception and Access) Act we are obliged to provide that material under a lawful warrant. We would do so; we would respond to any lawful warrant.

Senator LEYONHJELM: In theory then, another country could say that the data is stored within their borders and so they could stop you from doing that?

Mr Froelich: Strictly, yes. You would be subject to the laws of the geographic location, but we would respond to anything that meets the obligations under the Telco Act or the TIA Act.

Senator LEYONHJELM: Okay. I do not quite understand the comment that you do not like phishing in relation to Senator Ludlam's question about tower dumps and you also included cell dumps. How do you decide what phishing is? What are you referring to there?

Mr Ryan: When we receive a lawful request, we like a telephone number or a name—so fairly standardised and succinct. This is so that we do not have to step into the role of a policeman to try to decide what is relevant and what is not. If you send us a telephone number, we will get the information on that telephone number and

send it back—end of story. So we have responded to that warrant. Or if it is a name or handset information et cetera. We do not try to decide what you do and do not want. If we get a phone number or a name, that is it.

Senator LEYONHJELM: So if somebody asks for all of someone's friends on Facebook, that is not your cup of tea?

Mr Ryan: No. We would not even know where to start.

Senator LEYONHJELM: That is fine. Thank you.

CHAIR: I might put this to our next witnesses as well, but since we have the mobile industry here, can you help us out? Included in the Attorney-General's definition of metadata, which is the working definition across the various agencies that you deal with, location records are fair game: the location or the approximate location of a handset at the time of a particular event or call or whatever. From an industry point of view, what is the range of accuracy? Assuming that the GPS on the handset is not turned on, so just from the triangulation of the cell towers, how accurately can you determine somebody's location at any given time?

Mr Froelich: So I guess specifically that answer varies according to the geographic locations. For example, in a country town there may only be one cell tower that has what we call an omnidirectional antenna propagation. You can tell the distance from the antenna, but without the GPS turned on the phone assisted GPS location function is not available to you—I think the parameters you set around it was around not having GPS on. When you get into an area like where we are now, in central Sydney, you would be able to triangulate, and triangulate implies that you have three towers, to measure the distance from each tower to get a relatively accurate approximation down to 10 metres to 50 metres, in that sort of range, whereas in a country town it might be a doughnut shape of perhaps 100 kilometres.

CHAIR: One hundred kilometres? So within the range of the particular tower, you have a distance but not bearing?

Mr Froelich: Yes, you have got a distance from the tower only. You have set the parameter in the question around having GPS turned off, so the accuracy would not be that great, no.

CHAIR: Obviously for billing purposes or even for the call to function you need to record that, you need to know that information, otherwise the system does not work.

Mr Froelich: The billing function is based on the tower that you send your signal through. If you were making a call that was a distance of 500 kilometres from Broken Hill to Sydney—whether it was 500 kilometres or 600 kilometres it would not really matter in the billing function because you are still connected to the same tower.

CHAIR: And what is the range—you were talking before that in a regional town there might only be one tower providing that service. What is the approximate range? How far can you get from that tower before the signal drops out?

Mr Althaus: It depends to some extent on what frequency you are operating on. There would be a range depending on the network parameters that you are dealing with at the time. We can give you a range. We can take it on notice if you like and give you an estimate.

CHAIR: If you like; just industry estimates. To my mind, the geolocation included in the definition of metadata is one of the more invasive reasons why I want this material to need to be accessed via warrant rather than someone stamping a piece of paper and serving you with it. The vast majority of Australians probably live well within range of two or more cell towers at any given time. So that material is all being logged. How long is that held for across the industry? Is there an average, or is it just up to individual company policy?

Mr Froelich: I think specifically for that information it is quite transient because it does not necessarily form a billing function. The structure of the storage of data in the telco industry is such that under the structures of the privacy legislation we only keep information for as long as we have a business need for that. So that location information is particularly transient.

CHAIR: Days? Weeks?

Mr Froelich: Perhaps here and now really.

CHAIR: Really?

Mr Froelich: It is where you are at that point in time.

CHAIR: It just goes straight through and it drops off.

Mr Froelich: Yes, there is no reason to keep that information.

CHAIR: Well ASIO believe they do have reason for you to keep that. That is part of our half a billion dollars I presume.

Mr Froelich: If you want to retain that, yes, it forms part of the—

CHAIR: No, I do not. I think it is a terrible idea!

Mr Froelich: If the law enforcement community wanted to retain that, yes, you would have to create structures to actually do that rather than the transient nature of what the data is at the moment.

CHAIR: Say you kept it for a couple of hours—or under data preservation notices is it correct that at the moment, if they are tracking a particularly bad line, they can serve your members with a notice that says: 'Don't throw that away; we might need that. We might come with a warrant later.'?

Mr Froelich: No, for transient data—we do not see the application of a preservation notice; we only see the application of a preservation notice for stored communications. This does not form a stored communication such that—if I could define stored communications as communications that come to rest on our networks, like email perhaps SMS and MMS. Those types of stored communications can be preserved, but we would not accept a preservation order for transient data.

CHAIR: Truly? How difficult would it be to do so? To my mind I can actually see a legitimate reason why that might be quite valuable for law enforcement purposes and, if it was targeted and discriminate, why it might be quite useful to trap that material for a period of time. How difficult is that to institute on a very targeted basis rather than across the entire population?

Mr Froelich: In a strictly engineering answer, because that is the part of the business I come from—

CHAIR: Yes, if you like.

Mr Froelich: we can build anything with time and money. Anything can be built—

CHAIR: Apart from safe nuclear power! Sorry.

Mr Froelich: I do not work in that industry so I will not comment, but I take your point. Given sufficient time and money, we can build any system that is required, provided it fits within the structures of the legislation.

Mr Ryan: Industry is building a project now, it is getting towards completion in, hopefully, September or October, to deliver your location in emergency to emergency service organisations. We are building the capability within the network—it is called push MoLI—the legislation is under the emergency call service determination to capture your location when you call 000. Along with your call we will capture your location. As Mr Froelich just said, depending on the cell tower, the number of cell towers, we will capture your location to send along with that emergency call to 000 and then onto the emergency service organisation. But that is a defined need, if you like, that the community has asked for.

CHAIR: Now imagine that I switch on the GPS function on my handset. How accurate does that become from the back end point of view? I know how accurate it is for me, but as far as the service provider is concerned.

Mr Froelich: It takes you down to the 10-metre range in terms of using assisted GPS is embedded signalling functions within the network. It will take you down into the 10-metre range of accuracy.

Senator LEYONHJELM: Not if you are inside; only if you are outside.

Mr Froelich: Yes. The GPS requires a link to satellite access.

Mr Ryan: That is assuming that each carrier actually has access to that layer of information.

CHAIR: That is my next question. How much of that GPS data resides on the handset and how much of it is transmitted back through your networks to be stored for arbitrary periods of time?

Mr Ryan: I cannot speak for all carriers. Some carriers just do not currently have that access. If I go back to the push MoLI project, that is something we are looking at the future. That is the next phase of it, if you like.

Senator IAN MACDONALD: You are calling it 'push molly'?

Mr Ryan: Because the network pushes it to the emergency services organisations. Rather than using, say, a 287 request they request the carrier to pull it from the network.

Senator IAN MACDONALD: What is the molly part?

Mr Ryan: Mobile location information, sorry.

CHAIR: That is all right. I don't think any of us here is an engineer; please bear with us. Just explain for me again in words of great simplicity how from the carrier's point of view the GPS functions on these phones, which I expect most people wander around with switched on so they can use maps or whatnot, that operates for people

using smartphones from a back-end engineering perspective. Can that material lawfully be accessed for good reason by intelligence or law enforcement agencies?

Mr Froelich: If required, yes. Assisted GPS signalling functions within the network are available within that host network, if you will. By host network, I mean the underlying access network that you purchased your phone through. At the carrier aggregation level—the connection between carriers—it is not necessarily translated across carrier borders. There is no reason to hand off a customer's location information once you have changed from one carrier to another. That information is useful perhaps in a marketing sense to the host carrier, where you might want to perhaps direct that person to their nearest pizza shop or something like that. We would not necessarily translate it across carrier borders, no.

CHAIR: When you say carrier borders, you mean if a Telstra handset rings an Optus one?

Mr Froelich: Yes.

CHAIR: But that material could potentially be within the dragnet of data retention. It is there. What I am trying to understand is that it is not simply isolated on this phone; it is being transmitted back and forth.

Mr Froelich: Yes. That comes down to the statement made by Mr Althaus before that within the data retention dataset we are unsure at this stage as to what that looks like.

CHAIR: Me too.

Mr Froelich: If that was included in the dataset we have to build systems to do that.

CHAIR: Just to be very clear, then I think we had probably let you go and call our next witnesses, it is entirely technically within the range of possibility and has probably already been done that you could be tracking somebody from that information. You could be tracking somebody around a live map—in fact, very many somebodies simultaneously—everywhere they went, every time they sent a text message, every time they made a call, purely on the basis of metadata alone. It is not content data under any legal definition.

Mr Froelich: No, that is not beyond the realms of possibility.

CHAIR: I guess I am asking you an engineering question rather than a legal one. We will get to the legalities later.

Mr Froelich: Yes, you can do it.

CHAIR: I do not have any other questions.

Mr Althaus: What we have been talking about demonstrates that on our side of this discussion there is an enormous amount of expertise and experience. To the best of our ability and awareness of what is coming in technology terms and service and application terms we would love it if there were a much clearer and more pragmatic dialogue between agencies and industries to talk about their needs and our capacity in a pre-emptive way rather than our being constantly in a reactive mode to proposals that are potentially quite problematic and in some cases are not that well thought out or whatever. I guess as a closing comment, some more dialogue would be a helpful thing.

Senator IAN MACDONALD: Along that line, is anyone speaking to your groups about a possible change to this act and what needs to be in it? Are you having discussion with any government department?

Mr Althaus: Yes, we are. One of the things we find problematic is that it is often the case that ideas and concepts are formed and are well advanced in an agency's mind, and perhaps an earlier and ongoing discussion with industry would be beneficial.

Senator IAN MACDONALD: This is not really part of this inquiry, but you should make sure and if we can help—I cannot, because most of what you are talking to me about I have no idea about; that is not your presentation but my capacity—it is important for the nation and for the government that if this act is to be reviewed that it is done taking into account the experts that actually make it work and can see where a little bit of extra time might make it better for everybody. It is important, as I say, that you use us if you can, but it is important that your views are taken notice of even if they are not adopted.

Mr Althaus: We certainly agree and we put them forward at every opportunity.

CHAIR: Are you presently in discussion with the Attorney-General's Department or anybody else around data retention proposals in any kind of formal way?

Mr Stanton: At the association level? No, there is no active consultation about that at the moment. We have been in discussion very recently about the TSSR proposal—that is the infrastructure security proposals that AGD have been putting forward.

Senator IAN MACDONALD: What is TSSR?

Mr Stanton: It is a framework that the Attorney-General's Department wants to put in place to provide greater surety around the protection of critical infrastructure in the telecommunications industry.

Senator IAN MACDONALD: What does it stand for?

Mr Althaus: Telecommunications security sector reform—we live and breathe acronyms.

Senator IAN MACDONALD: You are not as bad as Defence.

Mr Stanton: On data retention right now, no, nothing in particular.

Senator LEYONHJELM: You were talking about $500 million for data retention, is that based on each ISP doing its own data retention? Have you looked at some kind of pooled system? Is it feasible or not an option?

Mr Stanton: That number was based on market-share-based extrapolations of each major player putting in place their own system.

Senator LEYONHJELM: Doing your own thing.

Mr Stanton: Yes.

Senator LEYONHJELM: Okay. Does that make more sense than having a pooled system? I will make my position clear: I do not want any system. But if you had one, would it be cheaper or more efficient to have a pooled system or for each organisation to do its own thing?

Mr Stanton: I think you would have to start from the basis of the dataset requested and look at the issue in that light. You would have to take into account interoperability and privacy issues. I cannot give you a simple answer to that question.

CHAIR: Have you looked at renting some space at that big NSA data centre in Utah?

Mr Althaus: No, sir.

CHAIR: That is a no, for Hansard. We will suspend the committee. I greatly appreciate your expertise and time. I know you are all busy people. It has been really instructive.

Proceedings suspended from 10:49 to 10:57

DALBY, Mr Steve, Chief Regulatory Officer, iiNet Limited

O'DONNELL, Ms Leanne, Regulatory Manager, iiNet Limited

YERRAMSETTI, Mr Roger, Operations Manager, iiNet Limited

CHAIR: I welcome iiNet Limited to today's hearing. Thanks very much for talking to us today. The committee has received your submission as submission 38. Do you wish to make any amendments or alterations to your submission?

Mr Dalby: No.

CHAIR: If you wish, you can kick off with a brief opening statement, and then we will take you to questions.

Mr Dalby: In this statement there are some illustrations, which probably did not reproduce too well in the submission, so I have handed them around and will talk you through them when we get to them—the slides in a slightly larger format. I was hoping to be able to step you through that on PowerPoint slides, because the slides build, but we will have to just work with the paper version.

As mentioned, we previously provided a written submission in which we elaborated on our concerns with a proposed mandatory data retention regime. Our conclusion in that submission was that proponents of such a scheme grossly underestimated the volume of data to be collected and the consequential costs flowing to those companies forced to undertake the proposed surveillance of the Australian population. On this occasion we offer additional information on the poorly defined but freely used term 'metadata'. Given that various public comments have indicated that the full set of metadata may not be required to be retained, we will illustrate our observations that stem from an apparent requirement for ISPs and carriers not only to collect metadata but also to process the metadata to redact or remove the content from the metadata which appears to be surplus to requirements according to some comments.

It is important for us to note that the contradictory and confusing comments from law enforcement agencies and government sources regarding this subject have led us to base our comments on a range of inputs as well as interpretations and assumptions of those inputs. The documented descriptions of metadata that have been provided lead us to believe that a full set of metadata is preferred. However, public comments have also suggested that a much smaller subset is acceptable. A definitive statement outlining the government's requirements would reduce the uncertainty and enable us to more meaningfully respond to any proposed data retention regime. We like to say it is not 'just metadata'. In an internet protocol or IP online environment metadata is pervasive and extensive. Metadata underlies all communications. It is fundamentally misleading to downplay the degree of intrusion of data retention regimes such as those that operate at the European directive level. A false assertion is that such regimes do not include the actual content of what our customers might be communicating. These inaccurate distinctions are dangerous and inappropriate. It is misleading to assert that such data is 'only metadata' or 'just metadata'. Metadata reveals even more about an individual than the content itself.

As I will expand on shortly, a post or a tweet on the social media platform Twitter is considered to be a very limited or concise form of messaging. A single tweet is only allowed 140 characters, but it is important to understand that as a piece of communication a tweet can contain 40 fields of metadata, comprising thousands of characters. This metadata can be used to extract more information than the content. In May this year David Cole, a professor in law and public policy at Georgetown University Law Center, reported a number of points. He included a comment from NSA General Counsel Stewart Baker, who said:

Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.

He also reported that General Michael Hayden, former director of the NSA and CIA, called Baker's comment 'absolutely correct' and, frighteningly, raised anxiety levels by asserting, 'We kill people based on metadata'.

Conversely, the Privacy and Civil Liberties Oversight Board found that there is little evidence that the metadata program—that is, the data retention program—has made us safer. Caspar Bowden, a specialist in EU data protection and European and US surveillance law, has argued that:

… retention is like having a CCTV camera installed "inside your head" i.e. that it invades the subjective interior space of our thoughts and intentions, because these can be inferred from Internet and other metadata.

He went on to say:

It is incompatible with human rights in a democracy to collect all communications or metadata all the time indiscriminately. The essence of the freedom conferred by the right to private life is that infringements must be justified and exceptional.

Additionally, the EU Advocate General, Pedro Cruz Villalon, in his opinion supported the overturning of the EU data retention directive. He argued that the retention of such data 'may make it possible to create a both faithful

and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity'. He also highlighted the risk that the retained data might be used illegally, in ways that are potentially detrimental to privacy or more broadly fraudulent or even malicious. He went on to express concerns that data retained under the directive is not held by public authorities but by the providers themselves and that it does not need to be physically stored in the EU but can be kept on servers anywhere in the world.

The complex, voluminous, often sensitive and private nature of the data sought under a mandatory data retention regime exposes the hollowness of the claim that communications data or metadata is 'just like the envelope without its contents'. The difficulty with such a poor analogy is that it attempts to compare a piece of paper, the envelope, with a chain of events and multiple links to myriad other data, meticulously described and recorded. In the case of Twitter, this may include who wrote the tweet, their biography, their location, when it was written, how many other tweets have been written on that user's account, where the author was when the tweet was posted, what time it was, whom it was sent to, where the author is normally based and, surprisingly in the case of Twitter, the 140 characters of the content of the tweet as well.

Using faulty analogies to explain complex issues with the frequent use of the word 'just' is risky and misleading. As the ACLU explained in their report on metadata and privacy, a URL is both metadata—that is, a delivery instruction—and also content. It requests a webpage, which essentially means sending a message saying, 'Please send me the page and all the content found at this URL.' A single URL, or universal resource locator, reveals exactly which page was sought and, thus, exactly what content was received. The data generated as a result of our customers using the internet and telephone networks is certainly different in nature and volume than traditional fixed-line analog phone records. This data can reveal even more about an individual than the content itself.

I would like to move to the first page—it has 'Followers on Twitter' at the top. On the right-hand side, in the white box, you can see a screenshot of the original tweet. It has some red boxes over it, but it says: 'Need to catch up? Our complete coverage is here.' Then, in the larger box below that, the metadata, you can see a red box highlighting that the content is in the metadata. So, when people suggest, 'We don't want the content; we just want the metadata,' it is difficult to see how you can separate the two.

Senator MARSHALL: Is that just from a tweet?

Mr Dalby: That is just a tweet, yes. If we go to the next one—

CHAIR: Before you move on, your slide makes it look as though it is dropping off the bottom and fading out.

Mr Dalby: It does, yes.

CHAIR: How many more pages are there?

Mr Dalby: Sorry, that was just for presentation purposes. There is probably as much again—about an A4 page.

CHAIR: So the metadata is maybe 100 times the size of the content itself?

Mr Dalby: Yes. The tweet content is limited to 140 characters. In that case, there are not 140 characters there, but, yes, there could be thousands of characters in the metadata.

The next one is a webpage rather than a tweet. We chose the ABC. Typically, on average, behind a webpage there are something like 90 IP addresses or other URLs. You can see on the right-hand side a screenshot of the ABC website. It has all sorts of pictures and links to other stories and bits and pieces. On the left-hand side, again, there is a screenshot of the metadata behind that page. In that metadata there are all sorts of trivial things like what colour the text should be, the fonts and where it should be placed, but, bracketed in red, there are also a variety of files which live elsewhere on the internet. That is the instruction on how to get that content which sits elsewhere. On the ABC webpage itself, I have put a box around two of the pictures, and the arrow points to the URL that locates those pictures in the metadata elsewhere on the internet. Again, if you have the metadata, you have the content, so suggesting that we do not want the content but just want the metadata is, I think, a little misleading.

Finally, with Facebook it is the same story again. In this case it might be a little bit easier to see that. That is a snap of one of the iiNet Facebook pages. There is a green or teal coloured box with a quote in it, and it shows the link on the metadata page below. That, again, goes much further down the page. The link, which is a very long string of characters there that you can just make out, links to box No. 3, the content box up the page, and that shows that as an image just sitting elsewhere on the internet. Again, it is probably hard to read, but in the URL at the top of that internet page it shows the location. All that is sitting at that location is that green box with that

quote in it. It is a piece of discrete content on its own. There are other linkages there to the author's profile and to another Facebook page, and so we could take that on again. I have tried not to make that too complex.

Senator IAN MACDONALD: That is very good.

Mr Dalby: But you can imagine that, when we are talking about metadata at iiNet, we are not thinking about phone call records with the number being used to originate the call, the number that has been dialled, the time it started and the time it finished. That metadata is trivial to us, and we have done some number crunching on it. In fact, we think we could store the amount of metadata for our telephone traffic on a USB stick. It is trivial. We do not need to build a new building. But we will get to the numbers. Roger Yerramsetti is going to give us some additional numbers shortly.

We could go on and on about showing different examples, but I think it is important to note—before I get back to reading my statement—that we are seeing exponential growth of devices and of computing power and storage. So this is not a 'snapshot in time' issue for us; it is what it is going to be in two years time. We are already seeing wearable devices, with people wearing watches and other devices on their bodies as they train, exercise or just go about their daily lives.

Senator IAN MACDONALD: Dick Tracy used to do that in the fifties.

Mr Dalby: That is right, but I do not think anybody was collecting his data. So we see data from a range of wearable personal devices, home automation systems and security monitoring systems also all generating metadata. Wearable devices measure and record biometric data—such as sleep patterns, pulse rate, temperature and metabolic activity—distance travelled, altitude and GPS coordinates, as well as any calls made or received and photographs taken with that wearable device, all of which will be generating metadata which would need to be collected under this regime.

In its submission to this inquiry, the Attorney-General's Department asserted:

Service providers routinely engage in telecommunications data retention for their business purposes.

We believe this assertion is overstated. Carriers only collect appropriate data for their businesses. There is a world of difference between the data collected in order to bill a customer for their internet or telephone usage and the collection of a mass of data generated by a customer during their sessions online. The data generated by telecommunications traffic massively outweighs the data required for ISPs and carriers to run their businesses. This suggestion of routine collection from the Attorney-General's Department could be likened to saying, 'You're going to the shops to get a litre of milk anyway, so it's no big deal to bring me the whole supermarket.' iiNet has no use for surveillance data, so there is no commercial driver to collect a massive volume of data, indexed to individuals, that we will never use. In the event that a specific data preservation order is received from law enforcement agencies, special steps are required to retain the information specified in that notice.

We note that other reports emphasise the word 'telephone' in comments attributed to government sources. If the requests for metadata are to be restricted to telephony traffic, this limited approach conflicts with previous confidential documents provided to the industry by the Attorney-General's Department, which have clearly spelled out a much broader dataset to be collected. This broader dataset has been described as consistent with that adopted in the European Data Retention Directive and is the data necessary to trace and identify the source and destination of communications, including unsuccessful or untariffed communications, on fixed network and mobile network telephony as well as internet access, internet email and internet telephony. It is further described as necessary for agencies to have access to the data to reveal the daily habits of targets, to enable targeted surveillance. We were also told that the additional data collection results from the use of new technologies such as Voice-over-Internet Protocol and encryption, which increases among agency targets.

The inconsistent and contradictory messaging from government sources is confusing and unhelpful. The communications industry and broader community do not know whether the government is only looking for the data already collected routinely by telephone companies or is actually seeking the full set of data as set out in its briefing paper. Is it the metadata such as that described by the European directive or is it a much smaller subset of metadata which has had the content processed and redacted?

Additionally the Privacy Act prohibits the collection of data beyond that which is required for the service provider to conduct their business. iiNet has worked hard to ensure that it is compliant with this obligation, which I can broadly paraphrase as: if you do not need it, do not keep it. Browsing data; posts to RSVP, Twitter, Instagram, Facebook, Weibo, Google Plus; purchases from iTunes, Netflix, Amazon, eBay, Alibaba; searches via Bing, Google, YouTube, Baidu, Yahoo; and transactions for online banking, ticket purchases, hotel bookings or PayPal are not routinely retained by iiNet for our business purposes. These are private and irrelevant to the provision of our services. If we do not need the data at all, then it logically follows that we do not keep it in the

first place. It only creates unnecessary overhead. We do not build storage capacity for data we do not keep. The company has a formal data retention policy which operates in line with my comments here.

Assumptions have been made about how our business operates which lead to erroneous conclusions. Recent public assertions have been made, for example, that 'the ISP, as they do with their billing system, will be able to match the specific time and date stamp and IP address with a customer account.' These sorts of assertions are misleading, as iiNet and probably most Australian ISPs do nothing of the sort.

CHAIR: Who is that quote attributed to?

Mr Dalby: That was Graham Burke from Village Roadshow. This demonstrates the danger of making assumptions and comments in the absence of facts and the consequent risk of creating a false impression. Suggesting that it is no big deal because carriers are already doing it, when carriers are not doing it, is misleading.

Senator IAN MACDONALD: But don't you keep all that for your own billing purposes—the time, date and—

Mr Dalby: Certainly time and date are important for telephone calls, but we are primarily internet access. We do it for the telephone traffic, certainly.

Senator IAN MACDONALD: Sorry.

Mr Dalby: That is not a problem. A careless approach is unacceptable for public policy development. Indeed, in a recent policy background paper, the Department of Communications highlighted to us that the design of regulatory interventions requires an in-depth understanding of markets, supply chains, revenue flows, technical developments, expected regulatory costs and consumer and end-user expectations. I am almost to the end.

CHAIR: I was just checking, because we are a little bit pressed for time.

Mr Dalby: Shall I just move on to the implications for industry and leave it there?

CHAIR: As you wish, because we are going to turn these folk loose on you, and I am sure they have got lots of questions.

Mr Dalby: Mandatory data retention regimes turn commercial companies like iiNet into unwilling agents of the state. As the Office of the Victorian Privacy Commissioner submitted, the proposal for a two-year data retention scheme is characteristic of a police state. Law enforcement agencies already have the power to undertake targeted requests for data retention—for example, by using an ongoing data preservation notice.

We believe the community and our industry view these vague proposals with a great deal of uncertainty. Descriptions of metadata have ranged from just routine data already collected for the purposes of telephone billing through to the full suite of data covered by the European directive. The telecommunications industry may not only find itself coerced into the onerous requirements to collect, store and protect massive quantities of unwanted data but also have imposed upon it the obligation to process petabytes of data per day to remove content or links to content.

CHAIR: Thank you, Mr Dalby. There are two procedural matters to deal with. Firstly, there is a gentleman here from the media who is just testing the will of the committee that photographs be taken, using the usual courtesies. There being no objection, that is agreed to. Secondly, our colleague Senator Xenophon is now with us, on the phone from Adelaide.

Senator MARSHALL: Mr Dalby, do you think that anyone who uses Twitter, Facebook or a web page as a form of communication has any expectation that these are private communications?

Mr Dalby: No, but I do not think they have an expectation either that law enforcement is stripping out the metadata that is behind it. Most people are not aware of the metadata at all.

Senator IAN MACDONALD: Can I just interpose and say that this was very useful to me. Now I understand what people are talking about.

Senator MARSHALL: And I think most of that is meaningless to most people too. What is the big deal?

Mr Dalby: The big deal is collecting the data on people that are not suspected of any offence.

Senator MARSHALL: Someone is going to know that, yes, you did send a message by Twitter, you did do it at this time, you did do it from this location and you did do it using this device. So what?

Mr Dalby: Personally, I find that unacceptable.

Senator MARSHALL: Why—did you not do that tweet?

Mr Dalby: Yes, I did.

Senator MARSHALL: And did you have an expectation that this was a secret, private tweet?

Mr Dalby: Senator, no, I do not expect that it was a secret, private tweet; it is very public. I generally post on other forums. However, the collection of the metadata is what I object to. The collection of that metadata is far more information than in the tweet itself.

Senator MARSHALL: I have to get the tweet, but I am not allowed to get the metadata that comes behind it?

Mr Dalby: You are welcome to the tweet—that is right.

Senator MARSHALL: I would like privacy from the tweets, to be honest.

Senator IAN MACDONALD: That is easy—you can just turn it off.

Mr Dalby: The point is that we do not see it is our job to collect that metadata.

Senator IAN MACDONALD: Yours is not a philosophical argument; it is a commercial/storage argument.

Mr Dalby: It is both. Certainly from a corporate perspective the imposition of those costs and the additional risks of storing sensitive information are of great concern to us. At a philosophical level, we think there is a civil rights issue here—that people should be entitled to their own privacy at whatever level they deem rather than a level that the law enforcement agencies deem.

Senator IAN MACDONALD: Mr Dalby, doesn't that come down to a question of whether you believe, in this modern day and age, the fight against terrorists or all the bad guys—whoever they are—justifies you doing this? I assume that what you have told us in a simplified way was how the Americans knew where Osama bin Laden was and sent a drone to get rid of him, and could send it to get rid of me right at this moment, I guess.

Mr Dalby: That is an excellent example. I understand that Osama bin Laden operated in a completely electronic-free environment. So the answer to that question is probably no, they did not use that process.

Senator IAN MACDONALD: So they would get me but not him!

Mr Dalby: Yes, possibly.

Senator IAN MACDONALD: But, if I am a bad guy, isn't it in the world's interest that someone be able to find out where I am?

Mr Dalby: Yes, but it is entirely hypothetical and speculative, because there is no evidence, there has been no argument put, that shows that the collection of this data has helped anybody to catch anything. Denmark has been running with a scheme very similar to this for at least five years. The debate is now that we should stop doing it because it has not achieved anything. The crime rate has gone up and the amount of data collected is far too cumbersome and massive for law enforcement agencies to get any value from it.

Senator MARSHALL: On the flip side, if there is nothing useful in this information and it does not help anyone, what is the big deal? Let people have it.

Mr Dalby: Nobody is suggesting there isn't anything useful in it. If I was in the law enforcement agency's shoes, I would be wanting this very rich information as well. What I am suggesting is that all of us here in this room are possibly not targets of law enforcement, so why collect our data? My 12-year-old niece, why collect her data? My 93-year-old mother, why collect her data? It is not right.

Senator IAN MACDONALD: You do not know that until you have analysed the data of your 93-year-old mother.

Mr Dalby: I can vouch for my mother.

Senator IAN MACDONALD: Okay, but you cannot vouch for me or someone with my name, for example.

Mr Dalby: That is not law enforcement's job to target the individuals that are under suspicion..

Senator IAN MACDONALD: But how can they get that if they do not have this wide body of stuff to—

Mr Dalby: How have they got it for the last 100 years?

Senator MARSHALL: The internet has not been there for that long, has it.

Senator LEYONHJELM: First of all, can you tell us how a data preservation order works? I agree with you, by the way, about your civil liberty points. That would seem to me to answer the questions of Senator Marshall and Senator Macdonald in relation to catching a bad guy, in that you want to get information about them. Does a data preservation order do that?

Mr Dalby: Yes. In general terms, a data preservation order is a very specific request for information and it is prospective. So it goes forward and it expires after 90 days. So they will send the order to us—

Senator LEYONHJELM: They cannot ask you to store the data?

Mr Dalby: Yes, they can, but prospectively. So the data preservation order says: 'We've got Steve Dalby in our sights. Here's the service that we would like the information about and we want all his emails or his web browsing history for the next 90 days'—though they do not say for the next 90 days; they just say they want it—and that expires after 90 days. It is specific and it is about an individual, and it is a person of interest to that law enforcement agency.

Senator LEYONHJELM: Who issues them?

Mr Dalby: They will come from a law enforcement agency. The AFP, typically.

Senator LEYONHJELM: The AFP directly?

Mr Dalby: Yes.

Senator LEYONHJELM: Are they subject to a warrant process?

Mr Dalby: Yes, I understand that that is correct. If you like, I could take on notice and provide back a process and show you exactly step by step what happens.

Senator LEYONHJELM: Yes, if you could take on notice how they work. In a way, I understand Senator Marshall's point about the triviality of a tweet, but emails are not trivial and neither are VOIP phone conversations. What is the metadata associated with them?

Mr Dalby: A VOIP, a voice over internet protocol, telephone call is much the same as any other format. In fact, VOIP has been used in the network for a very long time. The metadata is the originating point, the address, typically, a phone number—but some VOIP services like Skype may not use a phone number, they use an IP address; the destination; and the time it started and the time it finished. If we are not billing for that—a customer may have just downloaded an app to their phone or to their laptop—it is just data to us.

Senator LEYONHJELM: Correct. But what I am getting at is this: you said metadata includes content—so it is a lot more revealing than just content itself. In the case of a VOIP phone call or an email, if you get the metadata how much content do you get?

Mr Dalby: On an email, you would get the subject line as part of the metadata and that can be quite revealing; the 'from' address and all the 'to', 'cc' and blind 'cc' addresses. Is there anything else, Roger?

Mr Yerramsetti: Information about how many attachments and possibly even the name of the attachment but not the attachment itself.

Senator LEYONHJELM: I did not know about Denmark and its data retention system. Could you elaborate a little more on how they do it, who pays for it and how much it costs there?

Mr Dalby: I would have to take that on notice. I am relying on news reports on that front that the Danes are now considering that the value of that five-year process that they have undertaken is not delivering what the original expectation was.

Senator XENOPHON: Can I just ask about the interception capability plans you have to submit every year pursuant to the act. Can you explain in broad terms—I do not want the tactical details of your specific ICP—and provide a skeleton outline of that.

Mr Dalby: I will ask Mr Yerramsetti to answer that.

Mr Yerramsetti: Can you clarify specifically a bit more about what it is you want.

Senator XENOPHON: Under the legislation, as I understand it, you are required to provide an interception capability plan to the Attorney's office each year, pursuant to the act. Can you outline what that involves in respect of the requirement under the act?

Mr Yerramsetti: Inside the ICP that we lodge annually we outline the services and products that we offer, some information about the volumes, so how many customers or how many services have we got. We outline our capability to intercept those services and we also specifically outline what we can intercept, how long it might take, how long we might be able to store it for and things like that.

Senator XENOPHON: Do the intelligence or law enforcement agencies have input into your interception capability plans from year to year?

Mr Yerramsetti: They provide feedback on our plans and we do work closely with some to ensure that there is capability for any products of interest.

Senator XENOPHON: Sure. Sometimes you change your interception capability plan depending on that feedback from intelligence or law enforcement agencies?

Mr Dalby: That is correct. In our own case, having grown through the acquisition of many other companies over the years, the predominant amount of feedback we get is: how do we integrate those new companies into our ICP capability? Because there is a technical basis to this collection and interception we have on occasions had to, if you like, dispense with the existing infrastructure and replace it with stuff that is compatible with the broader group. So we have had a fair bit of toing and froing with the AFP, particularly on that issue. We have a reputation for constantly buying other companies. It has been live for the 11 years that I have been in the iiNet Group.

Senator XENOPHON: Can I just go to this issue. iiNet possesses experience in providing phone services as well as internet services. If the proposed legislation were enacted in terms of data retention, is it possible for two people in Australia, one a whistleblower and the other a journalist, to contact each other without law enforcement agencies finding out that they have been in contact?

Mr Dalby: Do you mean electronically?

Senator XENOPHON: Electronically?

Mr Dalby: I would say yes. I think there are devices and services like BPNs and encryption services that would be readily available and would allow people to do that. They might even use a third party to swap information—a dropbox or something similar.

Senator XENOPHON: But with respect to the encryption and the services you refer to, there would still need to be that first contact between a whistleblower and a journalist or, for that matter, a member of parliament that the whistleblower wishes to contact?

Mr Dalby: Yes, that is true. I guess it would depend on how familiar they are with the means to remain anonymous. It is quite possible to use a public phone box, for example, to ring somebody remotely.

Senator XENOPHON: But in terms of electronic communications it would be much more difficult for their anonymity to be preserved, with mass data retention?

Mr Yerramsetti: I would not agree. I think there are many places that have relative public access that you cannot pinpoint an individual—you might be able to see a device possibly, but to determine who the individual was behind that—

Mr Dalby: Public wi-fi is growing as a service across the country. I do not know if that would—

Senator XENOPHON: So you are saying that mass data retention would not necessarily have a chilling effect on whistleblowers going to journalists or members of parliament?

Mr Dalby: I could not possibly comment on that. I do not know. I would argue that it would possibly have a chilling effect, but I do not know.

Senator XENOPHON: Let us just go back a step. Are you familiar with President Obama's review group on intelligence and communications technologies that comprised attorneys and former national security officials? Are you familiar with their conclusion that mass data retention did not actually add anything to catching the bad guys—and I think Senator Macdonald quite rightly put that—and targeted surveillance of data retention or targeted metadata was much more effective in establishing whether a crime had been committed or was about to be committed?

Mr Dalby: Yes, and we would be sympathetic to the point of view that a targeted approach is much more likely to yield results than just mass data retention.

Senator XENOPHON: You say that what has been proposed would cost iiNet in the order of $60 million. Is that a one-off cost?

Mr Dalby: That was our first-year cost, which we calculated the last time I appeared at this committee, which may have been 18 months ago. We have done some maths since then and we have seen the proliferation of metadata on websites and other places doubling every 18 months to two years, so our costs would increase. I know the cost of storage is coming down, but we believe that doubling every two years of the volume of data that would need to be collected would mean that this would be an ongoing increase. We are now talking more in the order of $100 million for that first two-year period of data collection—

Senator XENOPHON: And this is just for your customers, your clients?

Mr Dalby: That is right. We are only talking on behalf of the iiNet group of companies, which represents about 15 per cent of the broadband market.

Senator XENOPHON: What would that mean in terms of an increase in charges for the users of your services? Would it be a 10 per cent increase or a 20 per cent increase? Can you give us a ballpark range?

Mr Dalby: We originally calculated the $60 million to be an increase of about $5 per month per customer if we just passed the costs through. I have tried to make this point today: we are very confused about what is required so it is very difficult for us to calculate what the costs will be. If we are only required to keep routine metadata for telephone calls we can probably pack up today and not speak again. If, however, the confidential briefing paper that was provided by the Attorney-General's Department is to be interpreted the way we have then yes, there will be massive costs. As I said, we are talking now about $100 million for the first two years and growing over time as that data grows. And then there is another potential cost on top. If the suggestion is that content is not required—that somebody will be required to process the metadata that is collected to strip out the content—that would be petabytes of data a day for our own organisation. You would need supercomputers to extract that data. Frankly, we do not want that job. That is not what we do.

Senator XENOPHON: So you are saying that the costs of $100 million every two years would actually increase significantly if you had to do that as well?

Mr Dalby: The cost of storage might go down a fraction, but if we have to store it in the first place and then redact it it is just costs upon costs.

Senator IAN MACDONALD: I understand your commercial obligation, but I want to make it clear that your concern is mainly commercial?

Mr Dalby: Yes.

Senator IAN MACDONALD: I think we have answered most of the questions I had. You have referred to this with Senator Xenophon: what you are seeking is a definitive statement by the government—I think you said this earlier in your evidence—on just what they require.

Mr Dalby: Yes.

Senator IAN MACDONALD: Have you mentioned that to the government?

Mr Dalby: Yes, we have.

Senator IAN MACDONALD: Have you been consulted by the government on what you need to know in the definitive statement?

Mr Dalby: It has been some time since we were approached or invited, other than in this process.

Senator IAN MACDONALD: Again, as I said to a previous witness, perhaps those of us on this committee can help. You are more or less saying that if you have to collect everything you have to collect everything, but at least you want an unambiguous statement about what the government wants and who is going to pay for it.

Mr Dalby: Who is going to pay. We would also add that we are not particularly enamoured of the idea of storing this data. If we were obliged through a change in legislation to start collecting this data, we would prefer to hand it over to law enforcement somewhere and let them build a place up near Alice Springs in the desert and run a power station to power that and tell us what the data feed ought to look like. We will collect it and feed it to them, and they can look after it.

Senator IAN MACDONALD: Is it technically possible to do that?

Mr Dalby: Yes.

CHAIR: That is the US model. Effectively that is what the NSA has been doing.

Senator LEYONHJELM: The NSA is doing that, yes. That is why I am interested in what Denmark is doing. The only other model that I know of is the NSA model.

Senator IAN MACDONALD: All right. Thanks, Mr Dalby.

CHAIR: I just have one or two to wrap up. Can you just confirm for us, as we did with the other industry folk, that you are not in present discussions of a formal nature with the A-G's Department or anybody else on this?

Mr Dalby: No, we are not.

CHAIR: How much can you tell about a person from simply an IP address? For the benefit of all of us here from a non-technical background, just define, firstly, what we mean by an IP address. How much can you tell from that?

Mr Dalby: An IP address, or internet protocol address, is the definition of a location on the internet. The internet is not just a single thing; it is a mesh of networks. In order to operate, we use IP addresses either to set up a service—so you set a service up at my house in the first instance and you make it live with an IP address—or to route traffic, whether it is a telephone call, a Skype session, an email, web browsing or downloading some information. We use IP addresses for all of that for the internet to know where you are going, what you want and

where to bring it back. So when you say, 'What can you find out about a person from an IP address?' the primary thing an IP address might provide is a link to me. In iiNet, in my account, I could take the IP address of the service that has been provided to me by iiNet and link it, through a process of investigation, to my name and address, my contacts, the accounts that I have, all the email accounts that might be associated with that account, any telephone numbers that are associated with that and the billing history. Interestingly, that Attorney-General's briefing paper from 2010, which is still the only piece of documented briefing that we have, also asks for details of drivers' licences, credit cards, passports, banking arrangements—direct debit or credit—and a variety of other material which we generally do not keep but which I understand other companies keep, maybe for purposes of identification. So, at a personal level, the IP address could provide that sort of information. Then, if you had a lot of other IP addresses of where I travelled in my surfing of the internet, you would get access, really, to everything I do.

Ms O'Donnell: It could be your wife doing it on your account.

Mr Dalby: Yes, it could be my wife or my children using my account to do stuff too.

CHAIR: So it does not identify you; it identifies a device.

Mr Dalby: No, it identifies a service.

Ms O'Donnell: It links to a service, not an individual.

CHAIR: So people are making inferences about who is using the service, rather than—

Mr Dalby: Yes.

Ms O'Donnell: That is the issue of where you have an IP address at a university, for example, or at a library. It is not going to link to an individual in that case.

CHAIR: Yes. Finally on security, sketch for us briefly an ISP. You have a number of different businesses within the ionic family but what you do to secure peoples' personal material, that which does exist which you host? How was that material made secure?

Mr Dalby: There are some industry standards. Probably most strict is the banking standard, the PCI-compliant—the payment card industry standards—which means that for things like credit cards we do not keep the record at all. We have a process where the customer supplies it into our system themselves, it is checked with the bank and validated, but if you are talking to is on the telephone we do not get the information or if you are doing a self-service application on the net it goes into an application which, again, is not stored. The rest of the information—which is personal details about name and address and other services attached to that account—is stored again in compliant systems which are compliant with the Privacy Act, for example. For other standards—

Ms O'Donnell: There is a whole range of ISO standards.

CHAIR: I guess where I am heading with my final question is the security implications of creating this vast data store on people going back at least two years and some of the agencies amount talking about five or more. I imagine that is a fairly serious security risk which presumably accrues to you guys as the ones who need to look after it.

Mr Dalby: Yes.

CHAIR: What would you need to do to safeguard it?

Mr Dalby: We do not want to go there, but I guess if we have to we are likely to need to build new data centres to store this. So there are bricks and mortar and communication facilities to link those data centres to the rest of the network. That is where the $60 million, $100 million come in—to build that infrastructure. It would be built to standards with security, privacy and so on. We are not suggesting that we could not do that. We do not want to do that but again, as the previous witness said, you can build anything with time and money and I guess this is the same thing. We can build the security, we can build the privacy, but the question is: how much money do you want to spend?

CHAIR: The reason I am putting this to you is that we asked these questions very directly to Mr Irvine from ASIO the other day and they do not really know.

Mr Dalby: Yes.

CHAIR: And it is all going to be made to your problem.

Mr Dalby: That is right.

CHAIR: I am just putting you on notice.

Mr Dalby: We are clear on that—that he has made that comment and made suggestions about selling BMWs and other things. They are far-fetched comments. I do not think he understands or has had advice which makes it clear to him what he is asking of the industry. There is no way that there is an informed comment coming from ASIO.

Senator IAN MACDONALD: But in the end result, it is either you billing taxpayers through your billing system to pay for storage or us collecting it from taxpayers as taxes to build a storage system. It all comes from the same source in the end result.

Senator LEYONHJELM: That assumes there is a storage system, if there is to be one.

Mr Dalby: Yes.

Senator IAN MACDONALD: If there is one, yes.

Senator MARSHALL: And not all customers pay tax.

CHAIR: Yes. It is either billed to your customer base or to the taxpayer, but somebody has to pay for it.

Mr Dalby: That is right.

CHAIR: We had best let you go. We have taken you well over time and greatly appreciate your time and expertise this morning.

Mr Dalby: Thank you, Senators.

WATERS, Mr Nigel, Australian Privacy Foundation

[11:49]

CHAIR: Welcome. Thank you for talking to us today. Your submission has been received by the committee as number 36. Do you wish to make any amendments or alterations to your submission?

Mr Waters: I do not wish to add anything, but I would like to make a few comments highlighting some of the points in our submission, if that is acceptable.

CHAIR: That is more than acceptable. We invite you to make a brief opening statement and then we will go to questions.

Mr Waters: Thank you, Chair and senators, for the opportunity to appear before you. I have been appearing before this committee for more than 20 years, initially as Deputy Privacy Commissioner but for the last 15 years as a representative of the Australian Privacy Foundation. Most of my appearances have been in connection with various proposals for amendments to, or review of, the telecommunications interception regime. It is very good, and we are very gratified, that you are now having an overview inquiry into the act, because in the past the various inquiries have mainly been about marginal changes to the regime. If I can use the boiled frog analogy, it has always been very difficult to get people to look at the big picture and ask: 'Well, what is this cumulatively amounting to?' There is always a good case that can be mounted by the law enforcement agencies for 'just that little bit extra' and it is very valuable to have this opportunity to take an overview of the system.

I acknowledge the many other submissions you have received. A lot of the points we make have already been made to you, both in submissions and in hearings, by organisations such as the Law Reform Commission, the Council for Civil Liberties, the Rule of Law Institute and the Blueprint for Free Speech, but I would like to highlight a couple of points that might not have come up or to reinforce points that have already been made.

Firstly, there is the question of the scope and context of the inquiry. Whilst the terms of reference refer to two specific reports and to the T(IA) Act in particular, we do not think you can really do the job you have been asked to do without taking a wider set of issues and legislation into account. I know you have been doing that in your proceedings, so we welcome that willingness to look at the wider context. Part of that wider context is the overall level of government surveillance of Australian citizens and residents. We draw attention in our submission, for instance, to the extensive powers and information collection associated with the AML/CTF Act.

CHAIR: We might get you to spell out any acronyms.

Mr Waters: Sorry, that is the Anti-Money Laundering and Counter-Terrorism Financing Act. I notice that the Secretary of the Attorney-General's Department actually made reference to the mutual assistance arrangements under that regime when talking about sharing of information with overseas agencies. It is good that the government agencies are recognising the wider context and it is good also that you are prepared to do that.

There is also, of course, the international context. I know you have already canvassed a number of the parallel reviews, inquiries and developments overseas. Again, it is very important that we do not see this in isolation; it is part of an overall pattern, as we see it, of eventually the whistle being blown on the ever-increasing surveillance state and the importance worldwide that people are recognising of putting some brakes on that where it might have got somewhat out of control.

I welcome the fact that many of the government submissions have started to recognise, in a way that they have not done in the past, the importance of the privacy issues. But there is one glaring exception to that, which I would like to draw your attention to. When I was preparing for this hearing yesterday I stumbled across a privacy impact assessment report on the telecommunications interception act regime that was conducted by the consultants IIS—that is the consulting firm of Malcolm Crompton, the former privacy commissioner. The report was presented to the government in December 2011. I understand it was made public on the Attorney-General's website in August 2012. It is a very detailed piece of work. It contains some very useful analysis of the privacy implications and a detailed set of recommendations about the sorts of safeguards that should be applied to any revised regime, and I think it is extraordinary that the Attorney-General's Department has apparently not drawn the committee's attention to that piece of work, which would I think have been extremely valuable to you.

CHAIR: Well, it still can be, so thank you for drawing it to our attention.

Mr Waters: There is a direct URL, but I only found it by doing a search and just completely accidentally stumbling across it. If you look at the interception act page on the Attorney-General's website there is no reference to it.

CHAIR: Fascinating.

Mr Waters: The access regimes you have canvassed extensively—the warrant regime, the stored communications warrant regime and the authorisation regime. We have just made the point about section 313 of the Telecommunications Act, which in our view is a worrying potential sidestep or loophole that potentially allows agencies to ask for information outside of the legislative regime in the interception act. We are not entirely sure how far that is being used, but I think it is worth asking the questions and making sure that it is not being used to circumvent the intent of the interception legislation.

In terms of the use of the access powers, we have given you some statistics in here, which I know you have from other sources as well, illustrating the growth in the number of authorisation requests in particular. I always like in these contexts to draw attention to an analogy that the UK data protection regulator made several years ago, which is that when you are looking for a needle in a haystack the last thing you should be doing is building a bigger haystack. I think that is worth bearing in mind, because it is quite clear that many of the law enforcement and intelligence agencies are actually drowning under the weight of the information they already have. The problem is not information; it is the way they use information and the way they target and select information. There was a very good question that I think you, Chair, asked one of the witnesses, about how many people are involved in these authorisations, and I think that illustrates the inadequacy of the current reporting regime. We have a lot of figures there, but they do not actually tell you a lot, in particular about the number of actual individuals who are being affected by the regime.

We make reference to the progressive weakening of controls over interception over the last 15 years or so. There is a whole range of examples of that—progressively broader criteria for warrants; progressively broader scope of warrants, including B-party warrants and named-person warrants; the introduction of prospective data requirement for preservation orders; the introduction of the new stored communications regime; and the provision for warrants to be issued by AAT members rather than judges. I think the Law Council made four very good recommendations for clawing back some of those. They were all of concern. And, again, the boiled frog analogy: when they were individually introduced they may have appeared relatively innocuous, but when you put them all together it paints a picture of less control, greater access, greater surveillance.

We make the point about the blurring of what we think is a vital distinction between national security and law enforcement, and also within law enforcement between serious crime and relatively minor transgressions. We spend a fair bit of time on what we call the metadata furphy. I know you have been canvassing that extensively, but one point that I think you do need to be aware of is that there is considerable confusion out there about what is covered by metadata. I know the official line from the government is that it does not include subject lines of emails, for instance. But it is quite clear that that is not universally understood. I think ASIO's evidence that you took recently clearly showed some confusion on their part about what was covered. And I know from raising it in another context with some telecommunications carriers that they also have different understandings about what is actually covered by metadata as opposed to content. So that is something that clearly needs to be addressed.

In terms of metadata, I think it is easy, when we say 'All metadata should be covered by warrants', for the law enforcement agencies to come back and say, 'That's completely ridiculous; it's administratively impossible for us to go for warrants for all of those 320,000 authorisations.' I think one of the questions that needs to be asked is: how many of those are just for customer name and address? I do not think any of us are suggesting that you should have to go for a warrant just to say to a telco, 'Do you have a customer Nigel Waters?' So, we could get rid of that sort of furphy and say that maybe 50 or 60 per cent of requests are in that category and that it is no different from any other business that the police might go to and ask for customer information. But when you get into the details of their billing records, their transactions and all the other associated metadata, then it is our position that that should be subject to the warrant regime.

You have also been canvassing the data retention requirements in great detail. Again, we have a very strong position on that—that a new data retention regime is not necessary. The preservation notice regime should be sufficient to provide agencies with what they need, and there are so many uncertainties, as we have just heard from iiNet, about what the government will actually be asking for and the logistical issues in providing that, the cost of providing that and the security issues that are raised by creating those huge honey pots of data that nobody can give an absolute guarantee of security about. To our mind, they all contribute to the case against those requirements.

I think it is very important that a proportionality principle gets explicitly built into the regime, not only in the objects clause but also at the various levels of authorisations and warrant provisions, where it becomes quite clear that they have to make a case for why they need this information, why they cannot address their concerns from other sources not only to the satisfaction of the authorising official, whether that be a judge or an AAT member,

but, we would argue, also to the satisfaction of a public interest monitor, and we strongly support the concept of a public interest monitor role in the process.

At the end of our submission we draw attention to a set of international principles on the application of human rights to communications surveillance, which is being developed by a broad coalition of international NGOs—more than 400 civil society organisations around the world—looking at what is happening in all the different countries and pooling their common knowledge to come up with a set of principles. We would refer you to those. Thank you for your indulgence, and I am happy to take any questions.

CHAIR: Thanks very much for your time and your expertise. Maybe we could start right at the beginning, and you could help us with a question that troubles many people and that Senator Marshall has asked on a number of occasions, which is, 'Who cares?'—what is the point of privacy? Does it matter? Does any of this really matter? As long as the material has been accessed lawfully, does any of this really matter?

Mr Waters: Obviously I think it does. There will be people who continue to trot out the 'I've got nothing to hide; I've got nothing to fear' line. The reality is that we all have areas of our life that we wish to remain private. There is an inherent human right in having some private space, and that extends to information space as well as territorial space. There are some very clear arguments about the consequences of a surveillance state and information being held about us in terms of the chilling effect on people's willingness to explore ideas, to communicate freely with each other and to have relationships that may or may not meet with society's approval—a whole raft of examples where it is clear that if people know or fear that information about them is going to be held and potentially accessed without necessarily any prior suspicion then that will have a chilling effect and will be deleterious in many cases to mental health and social development.

Senator MARSHALL: I am nearly being verballed, but not quite. I am actually a great supporter of privacy. What I want to try and tease out is that this is a relatively new technology. By its nature, it stores stuff; we know it does. We understand the internet—or, at least, I thought I did to a degree. My employer can have access to the stuff I do at work and family members can look at it. What happens at the other end? People can circulate it and forward it on. Electronic communications or putting staff on the electronic system—because it is not really a communication till someone communicates back the other way, I suppose—ought not come with the expectation of privacy. If I want privacy, I should write you a letter. You keep it private at your end and I will keep it private at my end. Unless someone opens it on the way through, that should be private. Or I should speak to you without other people listening. But I am just not sure. Are our expectations that the electronic system should be private, as we understand it as people over 50, realistic expectations? Personally, I am not sure that it is. If people do not have the expectation that it be private, a lot of these issues sort of disappear. It becomes a little bit like, 'So what? You knew what you were doing when you put all your information out there anyway.'

Mr Waters: There are a couple of points. One is that, realistically, people increasingly do not have the other options. We are increasingly being forced to communicate electronically by the businesses we deal with and by government. We are being pushed into that and it is actually quite difficult these days to operate with pen and paper and verbal communication only. The counterargument is that all we are doing now is using these new technologies to communicate things that we used to do on pen and paper and orally. We had a reasonable expectation then that, if we chose not to share that with a wider group of people other than the person we were communicating with, it would be respected, whether through the post office not opening your envelope or people not tapping your phone or snooping and overhearing you in public space. So why shouldn't we have that expectation simply because we have a new set of tools available for communication? Why shouldn't human beings, as social beings with economic lives and suchlike, be able to use those tools and those facilities without any change to that expectation? I concede that it is probably technically the case that we have to concede some loss of privacy if we want to use these tools, but part of what this exercise is about is saying, 'That should only be to the absolute minimum extent necessary.'

Senator IAN MACDONALD: I always tell my staff, 'Don't put anything on the email that you wouldn't want to see in a headline in *The Australian* tomorrow.' So even someone of my vintage understands that there is not a lot of privacy. But, as Senator Marshall says, you can have privacy—and we politicians know this—if you throw your phone away and get rid of your iPad. I suppose we do have that alternative, albeit inconvenient in this day and age. I suspect one of the things you say is that we should always ensure that government communications and forms can be filled in manually, although that may be—

Mr Waters: I think you will find that is becoming increasingly difficult. The government agencies are moving in a direction where it will be extremely difficult for a lot of people to not use electronic means.

Senator LEYONHJELM: I know you are from the Privacy Foundation, so you have been coming at this from a privacy aspect. What are your thoughts on the fact that this is not just privacy per se; this is privacy between citizens and the government?

What we are discussing is the claim that the government has a right to look at what you have been doing online, in the same way that you might say that, in 1984, they had cameras in each room of your house and Big Brother could look at you. Or at an earlier age you could argue that perhaps it would be the equivalent of having a federal policeman living in your house with you, checking on what you were doing. Do you come at it from that point of view or are you only looking at it purely from a privacy perspective?

Mr Waters: No, we certainly share those concerns. Privacy and civil liberties issues closely overlap and we work closely with colleagues in Electronic Frontiers—whom you are hearing from later—and with Civil Liberties. I do not think it is any exaggeration to make those sorts of analogies. It seems all very innocuous when it is just data and it is just taking place out of sight, out of mind. But by drawing those sorts of analogies you do actually make people stop and think, 'Gee, would I really like a policeman in my bedroom?' It may not be going that far, but we are moving in that direction. I think that is a major concern for a lot of us.

CHAIR: You raised section 313 of the telecommunications act in your opening statement. Could you tease out what your concerns are there, because my recollection is that that is the same section that is being used to censor particular web pages or particular kinds of content by ASIC, the Federal Police and one other agency—we do not know who. You have concerns about wider interpretations of that section. What are they?

Mr Waters: I am not our APF expert on this one, but my understanding is that there are two separate parts to section 313—that is, 313(3) and 313(2), which are related to crime prevention, which have been used for content blocking. But there is also a wider law enforcement wing, which is section 313(3). That potentially, as we see it, would allow a wider range of agencies than exist under the TIA Act to actually go to a telco and ask for information including, potentially, content information. We have no evidence that it is being used in that way, but one of the problems is that, in a sense, section 313 is a permissive provision. It is not a power. It seems to us that it has been used in the content-blocking sense almost as a power.

CHAIR: We only found out about it because sites were being knocked over, not because there were any reporting obligations.

Mr Waters: Absolutely. The whole idea that things could be happening under section 313 without the detailed safeguards that apply under the interception act is a worry.

CHAIR: Thank you. That is not something that I had come across; it is very useful. You mentioned, as did one of our previous witnesses, the utility of having a public interest monitor providing some kind of adversarial point of view, at least in the application of warrants at the moment. Do you think there is a role for a PIM at a federal level or are you talking about replicating the Queensland and Victorian experiences through their states?

Mr Waters: I think you need them at both levels, because clearly the state monitors can perform that role in relation to the state police and the state law enforcement agencies exercising their powers. But there also needs to be a federal one to play a role in AFP-ACC use of these powers.

CHAIR: Thank you. That is very useful. From the APF's point of view has the experience in Queensland and, more recently, in Victoria, by and large, been a positive one? Do they play a useful role?

Mr Waters: I do not have personal knowledge of that, but I understand from colleagues that they have had limited success. I think there are flaws in the models and they can always be improved. But they certainly have been valuable.

CHAIR: One of the difficulties we have had and I guess one of the tasks to be taken on is proposing reforms that bring privacy protections up to date with the way that some of these powers operating are being used. You put one proposal to us before—that perhaps metadata that was more invasive or more categorical than simply a billing record of 'Who does this handset belong to?' could be subject to a warrant process. I suspect the AAT would ask us for more staff if we did that. But, at the moment, those processes are conducted entirely internally through that administrative arrangement. What other formal, specific proposals, specifically governing the use of metadata that is currently warrantless, do you think would make sense?

Mr Waters: Two things spring to mind: one is better reporting, and more complete reporting—including of rejection rates, which I think is very important. We need to know—

Senator LEYONHJELM: Transparency, you mean?

Mr Waters: Transparency about the number of authorisations, but also the number of requests that were not authorised, so that we can get some sense of how disciplined the agencies are being—

CHAIR: And the number of individuals that are covered, perhaps? You raised that.

Mr Waters: Yes—so a whole range of better and more complete reporting, but also external oversight of any residual warrantless authorisations, because at the moment that is entirely left to agencies. We think either the ombudsman or the inspector general, depending on which agencies we are talking about, should be looking in detail proactively at the level of warrantless access as well.

CHAIR: Thank you. That is helpful. Unless there is anything else, Mr Waters, that you would like to raise with us, we will probably let you go and call our final witness.

Mr Waters: Perhaps I could just mention a couple of other suggestions for changes, apart from the ones I have already mentioned: clearer objects, the proportionality principle, better and more complete reporting, warrants for most but not necessarily all metadata, winding back the range of agencies allowed to access data—that is very important; that has blown out—

Senator IAN MACDONALD: Would you suggest who should not be there?

Mr Waters: We do not think it is appropriate that local authorities or NGOs such as the RSPCA or even some federal agencies that are looking at very minor misdemeanours should be able to have direct access. There may be some arrangements whereby they should go to the police and, if they think there are sufficient grounds, the police could exercise their powers—so some sort of tiered arrangement.

CHAIR: I think the PJCIS made a similar recommendation, though not as specifically as yours. But that was in there.

Mr Waters: Greater thresholds for access, such as the types of crimes for which warrants are given—that has been eroded over the years, and I think the thresholds need to be raised; greater safeguards on sharing and re-use of information after it has been obtained, including internationally; and no additional retention obligations.

CHAIR: We greatly appreciate it. Thank you very much for sharing your time.

LAWRENCE, Mr Jon, Executive Officer, Electronic Frontiers Australia

VULKANOVSKI, Mr Alexander, Member, Policy and Research Standing Committee

[12:23]

CHAIR: Welcome. Thank you very much for talking to us today. The committee has received your submission as submission No. 22. Do wish to make any amendments or alterations to that submission?

Mr Lawrence: We have prepared a statement as an overview of our position. We realise that we are coming towards the end of the process and you have probably heard most, if not all, of what we have to say already. We will try to keep it fairly high level and not labour your time in covering the same ground too extensively.

CHAIR: I think you are reasonably aware of the material that we have traversed so far. If you would like to make an opening statement, you can keep it as brief as you like and then will go to questions.

Mr Lawrence: As a bit of background, EFA are celebrating our 20th anniversary this year. We have been fighting for civil liberties within the digital space all that time. We are a national membership-based non-profit organisation. Essentially, our objectives are to promote the civil liberties of users in the digital context. We certainly do understand the challenges that intelligence and law enforcement face in a context of very rapid technological change and increasingly ubiquitous digital communications, and we obviously support appropriate and reasonable reform of relevant legislation, including the Telecommunications (Interception and Access) Act, to ensure that those agencies can have the tools they need to investigate, detect and prosecute serious criminal activity and other threats to the peace and security that Australians have long enjoyed, but we are very concerned, and have been for some time, that the T(IA) Act in its current form—as I am sure you are well aware—does not adequately balance the needs of security with protecting the rights and interests of citizens.

We are particularly concerned around the right to privacy and also the subversion of the presumption of innocence which mass surveillance brings with it. So we are keen to ensure that these rights, particularly, are given meaningful protection in any reform to the act. We are very concerned about the growth in the scale of access to data under the act. We believe that is far in excess of what any reasonable person could assert is necessary to tackle serious crime and terrorist activities and other threats to security. We are also strongly opposed to the introduction of any mandatory data retention regime, for a whole range of reasons, much of which Mr Waters covered in his testimony, so I will not cover that as well.

We also share concerns around the use of section 313 of the Telecommunications Act, as discussed. In particular, I would like to raise one other issue there, which is recent reports in the Fairfax media about police gaining access to mobile phone tower data in bulk. It is not clear to us whether this access is being achieved under the terms of the T(IA) Act or under section 313 of the Telecommunications Act or potentially under some other power, but we think that is something that requires some investigation, because it is clearly, by definition, bulk access to data of anyone with a mobile phone within the range of that mobile phone tower.

From a principle perspective, Mr Waters also mentioned the international principles on the application of human rights to communications surveillance. EFA was an original signatory of that document, which, as has been mentioned, was developed by a very wide range of actors from around the world and has now been signed by over 400 organisations, across not-for-profits, civil society generally and the commercial sector, from around the world. I will not labour the point there, but we would refer the committee to those principles, which are available at Necessaryandproportionate.org. We encourage you to go through them.

In terms of looking at the current context of where we are compared to when this act was written in 1979, obviously there have been a few changes in the way people communicate. I think it is important to stress that digital communications now, particularly for those in the younger generations, are an all-encompassing aspect of their personal and non-personal lives, in ways that obviously could not have been anticipated when this act was written. The idea that, for a lot of young people, the internet is real life is something that people need to absorb. With that comes the point that, while in many ways the only way to be truly private these days is not to use the internet, there are actually quite serious social costs involved in that in today's society, which I think need to be appreciated.

In line with that, we reject pretty strongly the assertion that taking the powers of this act from 1979, a context where mobile phones did not exist and the internet was still a pipedream, and extending those powers into a context of ubiquitous mobile devices and internet usage is not in any way a logical extension of the law to, as it were, keep up with technology on a like-for-like basis. We strongly believe that in fact this represents a very dramatic escalation of surveillance deep into all aspects of people's lives and goes far beyond anything originally envisaged when this act was drafted.

Mr Waters touched on some of the issues around the definition of metadata. It is clearly a pretty critical starting point that we get a clear definition of metadata. In the telephonic context it is fairly straightforward, but if we go beyond that into non-telephonic communications we have some very serious concerns that it is even technically feasible to effectively separate metadata from content, particularly in the case of email communications. We also strongly disagree with the assertion that metadata is less invasive than providing access to content. As the Attorney-General's Department itself admitted in its submission:

… telecommunications data can contain particularly sensitive personal information justifying special legal protection.

We completely and wholeheartedly agree with that. Clearly, it can be used to build a picture of a target, their network of associates, where they shop, where they eat, where they sleep. As Professor Edward Felten said in his submission to a US case involving the ACLU and James Clapper, who I believe is a former head of the NSA:

… metadata is often a proxy for content.

In many ways it should be, particularly in any substantive form, taken as much the same. David Seidler, you may be aware, recently did some work for ACCAN looking at data retention. His point was:

Although on its face, metadata might appear anonymised and trivial, the development of big data analysis techniques (for which metadata is "perfect fodder") means that the insights it provides after manipulation might well meet this definition—

of being content, that is.

We echo Mr Waters calls for tighter access restrictions to this data. I think it is very clear that, given the potentially highly invasive nature of this content, of this information, there should be much tighter restrictions and, ideally, a clearly defined list of agencies that are able to request access to data. As mentioned, there may be cases where agencies outside that list can apply via an approved agency, as it were, to do that, but we think that there do need to be some very tight restrictions around that. We also agree that there should be very tight, very stringent and very clearly defined thresholds for access to data. We support the implementation of a warrant process for access to metadata in any substantive form, as Mr Waters said, outside of simple customer information. We do not think there is a need for wider access to that, but for anything involving any substantive amount of metadata we would certainly support that.

In principle, we think the thresholds for access should be set taking into account the principle of proportionality and we should ensure that access is only available in relation to a reasonably serious offence—for example, a criminal offence attracting a certain maximum term of imprisonment or a civil offence attracting a predetermined minimum penalty, and where there is a reasonable suspicion of the people involved in such an offence. We also support calls for more detailed reporting of access to data, including all the points mentioned. We also see no reason why access to communications data by intelligence agencies should not be reported on, at least on a statistical basis. We cannot see any harm in doing that. We agree that there needs to be more effective external and independent oversight of this process. We would also suggest that there need to be very clear rules about what happens to data that has been accessed through this process, how long it is retained by the agencies and how it is disposed of and so forth.

Senator LEYONHJELM: This is similar to the question that I had for Mr Waters previously: are you approaching this from a civil liberties point of view or a privacy perspective? I heard you mention the presumption of innocence, so I am assuming that that is a factor. So are you, like Mr Waters, saying there is a private space and it should also exist in the electronic area, or are you saying this is a civil liberties issue of the relationship between the individual and the state?

Mr Lawrence: I would say both. As was mentioned, EFA works closely together with the APF on many issues. We share their views on most privacy factors—not all. We do believe—and I think it is important to touch on this—that it is important that there be a private space for people. As I mentioned earlier, I think that, if you are a young person these days, the social cost of opting out of things like Facebook and other social media is quite significant, and I do not think we can just dismiss that and say, 'If you really want privacy then don't use the internet.' I just do not think that is an effective response to the reality.

We are predominantly a civil liberties organisation. Privacy obviously is a large part of that for us, but we believe that this—and when I say 'this' I mean the entire scope of mass surveillance that we have become aware of, particularly over the last 12 to 13 months—really undermines the appropriate levels of government access to people's lives. As I say, if everyone is being surveilled then everyone is a potential suspect and is not really being treated as a citizen, which I guess is at the core of our concern.

Senator LEYONHJELM: I tend to agree with you on that. So at what point do we say it is acceptable if it means preventing a London bus bombing, a Bali bombing or those sorts of things? At what point do we say that

we trade off a degree of either our privacy or our civil liberties in exchange for heading those sorts of things off? What is your view?

Mr Vulkanovski: Firstly, I would like to raise the point that civil liberties and national security do not necessarily have to be mutually exclusive. It is not a zero-sum game, so we should not treat it as such in terms of having to concede one to gain another. But, in terms of what kinds of restrictions or standards should be in place, basically at the moment the T(IA) Act allows for three things to justify it: a criminal offence, a civil penalty of any kind and any issue relating to revenue. Basically, the authorised bodies and persons are drafted as such. What Jon proposed, or what EFA proposed, was setting some kind of standard or test for that—even simply the employment of a 'reasonableness' test. That is a fairly wide, reasonably well understood term, but it is sufficient to allow some kind of threshold. Going back to your question, it is that threshold that can justify it.

You mentioned the London bombings. I would put up the example of littering, for instance—simple littering or a fine of arguably trivial value. These things are currently justifiable, and I use the word 'justifiable' as it is used in the T(IA) Act. So you are right to question what kind of threshold there should be. I do not think we can answer, right here and right now, what kind of threshold should be in place, but I think reasonableness is a good place to start.

Mr Lawrence: If I can just add to that, in some ways what I would do, without question, is turn it around and suggest that there actually is no real evidence—certainly not anything that we are aware of—that has shown that access to this sort of information does prevent activities like that. I was actually on a tube train in London at a quarter to nine on 7 July 2005, so I do not take this lightly, but there is no question that the British intelligence agencies did not have access to this sort of information prior to that act occurring.

Probably a more pertinent and recent example is the Boston Marathon bombings, where not only did the USA, through its various agencies, have essentially what appears to be unfettered access to telecommunications but also they knew these guys were dodgy, because the Russians had told them. They had even interviewed them. Having all this information did not stop the blowing up of the marathon. So there are genuine questions here, and there has been a fair bit of research done in various jurisdictions looking at just how effective this information is. Mr Waters touched on this as well. Having more information does not make things easier. In many ways, it potentially makes things harder. It also raises the likelihood of false flags and false positives—

Mr Vulkanovski: and Australian resources.

Mr Lawrence: and Australian resources and so forth. There is a real issue here. We have seen this come out of the revelations about the National Security Agency in the US. There has been to this point very much—we know their mantra was 'collect it all'—an approach of 'We can do this, therefore we should.' I think we need to have some pretty serious conversations—as this is a very important part of that conversation—about the limits to do that. There is a burden of proof on the intelligence agencies here, which they can very easily circumvent by saying, 'We cannot comment on intelligence agencies.'

Mr Vulkanovski: It's hard to make comment without any data.

Senator LEYONHJELM: One of the chief champions of data retention, in particular, is ASIO. What is your opinion of their enthusiasm for it?

Mr Lawrence: Being very absorbed in these issues for some time, it is certainly clear to me that this sort of mass-scale data mining and signals intelligence will never go anywhere near replacing good old-fashioned human intelligence. That is the point. If we learned anything from Edward Snowden it is that having all this information does not necessarily make anyone any safer. In many ways, it undermines—this is one of my real concerns. We cannot protect our civil liberties. In a sense, ASIO was set up to protect the civil liberties of Australians but we cannot protect those by dismantling it.

CHAIR: Nicely put. Quoting briefly from your submission, and following along a similar line, you said:

> Those acting against national security will not be affected by data retention. The ease with which data retention regimes can be evaded is grossly disproportionate to the cost and security concerns of the data retention regime.

Effectively, what you said is that it will be rolled over the general population, but those seeking to avoid it will have the expertise or tools to do so. Since you have a technical background, let us use that. How would people avoid these collection techniques? How easy is that to do?

Mr Vulkanovski: Anonymous browsers, like Tor, can be used to circumvent this data. I have some examples not with me at the moment—

Mr Lawrence: The use of encryption generally does raise the cost of surveillance quite dramatically. We are already seeing, in response to revelations about the NSA, people starting to become much more cognisant of the

value of encryption. The reality is that if you have strong technical knowledge—and it is fairly clear that the more sophisticated terrorist networks and organised crime gangs do have some pretty serious technical knowledge—you can take various steps to bounce around the internet and hide your location and identity, which does not mean you could not necessarily be found in the final instance but it does make it very difficult and very time-consuming and very costly for the intelligence agencies. I think the takeaway from that is that these sorts of mass surveillance project are likely to not really address the issue of major crime, in a sense. You will catch a few people, but they are probably the people you were going to catch anyway, I would suggest.

Mr Vulkanovski: I think David Seidler, working for ACAN, who we quoted earlier, summarised it quite well when he said the people that we are trying to catch will likely be the ones that will know how to evade them. I think that brings it home.

Senator IAN MACDONALD: But surely the security agencies would know what you have just said—that those that we are trying to catch would know how to evade them. So why do they still persist? What I am suggesting is that they obviously do think it is a useful tool.

Mr Vulkanovski: I imagine they would be aware that these devices of circumvention are out there. I would hope that they would be aware of that. But I think a data retention scheme or the loosening of access to any stored data would simply make their job easier. In doing so, we assert it is disproportionate to what we give up in terms of civil liberties. Making something too easy to access or allowing a wide variety of bodies to access it tends to shift the proportionality against our cause.

Mr Lawrence: I would add that I do not personally feel that the intelligence agencies or the Attorney-General's Department or the Federal Police have made a reasonable case as to why this information is required. The primary argument I have heard essentially is: 'Well, we've always had access to this information through the phone system. We're just extending that. It is a logical extension into these new communications technologies.' As I said in our opening statement, we strongly reject that. If you think about when this act was originally drafted, the information that you would get would be the fact that a phone call was made from No. A to No. B at a certain time and lasted a certain duration. That is four pieces of information. As soon as you widen that into a mobile phone context, all of a sudden you have got a location at each point, which is an entirely new thing, where literally people's locations can be tracked. Then, if you go beyond that into non-telephonic communications, all of a sudden the amount of information that has been collected starts to explode. You start to have potentially dozens, if not hundreds, of different points of data that can tell all sorts of things about what is going on. It is really quite a different scale, a different scope, a different context, and it needs to have very different rules.

Senator IAN MACDONALD: We might ask the ACC when we are down there later whether people can circumvent it.

Mr Lawrence: The argument that is often made—this may have been explained to earlier—is that because the business models and so on are changing, particularly within the ISP space, their requirement to store a lot of this data, which was usually just billing data, is starting to go away. This is understandable. There is a concern on the part of the agencies that it will get to the point where they will go and request data and it just will not be there, because the company had no reason to store it. That is the point at which I think you start running straight into some of the fundamental privacy principles, which is that information should not be stored unless there is a legitimate reason for it. Storing it just in case we might want to do some surveillance on you is, we would argue, beyond that line.

Mr Vulkanovski: Just in case there is a needle in the haystack.

Senator IAN MACDONALD: I do not want to suffer the fate of one of my colleagues, who used television drama shows as a substitute for actual facts, but I might say that the American television cops would never solve a crime without surveillance access to phones. Even some of the British cops would seem to be at a disadvantage if it were not there. Perhaps that is not real life though. Senator Marshall, I assume you are going to ask your question?

Senator MARSHALL: I was just going to ask, as a general question, whether you have issues with warrants that might have been issued for a purpose that then identify other issues of criminal activity—whether you then have a problem with that incidental information being used and passed to other agencies that it might affect, from a civil libertarian point of view.

Mr Lawrence: That is kind of a difficult question to answer in the abstract, I think. Warrants are there and are given specific restrictions for a purpose. In that sort of circumstance—and I am not a criminal lawyer by any means—if other evidence is uncovered and there is a reason for that to require police investigation then

presumably there would be a process where they could then go and get a secondary warrant and so forth. But I do not pretend to be an expert on that.

Senator MARSHALL: You are right in terms of the development of the legislation pre internet and pre mobile phone—not necessarily all mobile phones, but the electronic world anyway. You make a point which is right: there is so much more information out there, and inevitably, if you are targeting someone and you are right about that and you get the information, you may get much more information. But my understanding at the moment is that it is then very problematic to pass that information on if it was not specifically on the purpose of the warrant.

The other point is that a lot of people have used examples. You say, 'Why should everyone be treated as a criminal?' and I agree with that, but what about the example that we all walked through the security screening into this building? Do we also take the attitude that we were all being treated as potential criminals because we did that and conceded to that?

Mr Lawrence: No, I think there is a really simple answer to that: it was my choice to walk into this building today. What we are talking about here—and another example that is often used is that we all use loyalty—

Senator MARSHALL: Can I just pick up on that. You said earlier that it is too easy and not acceptable in today's world to say, 'If you want privacy, don't use the internet.' Okay, maybe it is your choice to walk into this building. It might be your choice to go through an airport. There are lots of buildings in town where there is security required, and sometimes it may not be your choice. Is it the same argument?

Mr Lawrence: Partly. I think part of that is that we have spaces now in the digital context which, whether we like it or not, are becoming public spaces. To a large extent, Facebook is kind of a privately owned public space.

Senator MARSHALL: I am told it was so yesterday, but I do not know; I was not there yesterday either.

Mr Lawrence: Tumblr, Instagram or whatever—Snapchat. But I think there are some really serious questions there about how we treat these new public spaces, potentially. But, even having said that, if I am using a private email to communicate with somebody else, I think there is an expectation of privacy there, which is not the same as walking into a building and going through a metal detector.

Senator MARSHALL: Does a lot of it come back to what people understand? Again, in the example of someone using their private email address on their employer's computer, the employer still ultimately has access to that if they want to. Is that really the mistake of the user saying, 'I should have known that this wasn't private because I don't own that', or should they have had the expectation of privacy?

Mr Lawrence: I would agree with Senator Macdonald's point earlier. If you are at work, it is not private; it is work. It is important that people do have a distinction between—

Senator MARSHALL: Not in your lunch break?

Mr Lawrence: People do have some expectation of privacy, but I always counsel people, as the good senator has said: do not write anything in your work email that you would not be prepared to defend in court or see on the front page of the *Herald Sun*, but—

Senator MARSHALL: What about if you use the phone during your lunchbreak? Should the employer be able to listen to that?

Mr Lawrence: It probably depends whether the employer is paying the bill or not, to some extent, but I have always counselled people to maintain a very strict distinction between their personal and private emails, for a whole range of reasons, but particularly because it is important to have that distinction. I think that is part of the point. When you are at work, your expectations of privacy are slightly different from when you are in a private context. I think that is largely as it should be.

Senator MARSHALL: Should there need to be a warrant system for non-privately owned systems? I understand there should be a warrant to go and get your personal stuff, but, if it is not your personal stuff and you have been using it, should there be a warrant at all?

Mr Vulkanovski: I think ultimately each individual needs to take some responsibility when they are online. That is a given. That has to be done. We need to exercise prudence and we need to be aware of where our information can land, who is seeing it in its immediate capacity and who can probably see it in its immediate or future capacity. In saying that, laws such as the T(IA), or any laws in particular, provide that level of—you mentioned, 'Should this person be allowed to view this?' or 'If someone is standing next to me, they inherently can hear me, so would that be an invasion of privacy?' All these things can be mimicked online, except you probably do not know that someone is over your shoulder or that the boss is there. Why we are here today and why you are here today is basically to ascertain the standards that should be put in place. That is what we are trying to

determine, to put some kind of standard on and create the bridge between my personal data—possibly rather personal data—and the legal capacity to obtain this data. We all know they have the capacity to retain this data. A lot of people do. But why we are here today is to determine what that legal threshold is. Basically this is something that should be sorted out and determined, hopefully, ideally, here today.

Senator MARSHALL: That is why—

Mr Vulkanovski: That is how the process works and that is how it should be.

Senator IAN MACDONALD: This is not really germane to our terms of reference, but you did mention earlier the difficulty with the social implications. There are lots of stories about young children suffering badly from bullying and other things and thinking that Facebook and Twitter are real life. Do you think that there should be some compulsory warnings flash up on the screen every time you turn on your computer, saying: 'Please be aware, whether you are young, old or indifferent, this is not private; this could be seen by anyone'?

Mr Lawrence: I think it is important. There is a lot of really excellent work being done at the moment, particularly in the school context, educating and empowering people about what the issues are so that they understand what they are doing. There is this emerging concept of digital citizenship, which has been promoted by a lot of the agencies that are focused on protecting children in that space. In my role, I see some of the adults who slip through that net, in a sense. There is a lot of really excellent work being done in the youth space and probably not quite enough attention being paid to educate people that did not grow up with the internet. We are all aware of that. I was somewhat overjoyed the other day to see my 86-year-old father reading the newspaper on his iPad for the first time. Does he understand the privacy implications of what he is doing? Not really, but I think there is a role for us all, and, to many extents, that is at the core of EFA's mission: to educate people as to exactly what they are doing. As Alex said earlier, I think there is a great deal of personal responsibility that people need to exercise.

There are great dangers out there on the internet, as there are on Macquarie Street. But it has been our experience over two decades that the internet is an overwhelmingly positive revolution in communications. There are bad things happening there, and we need to be educated about what they are and we need to understand them so that we can tackle them effectively, both on a personal level and on a society-wide level. One of the other things that has really become clear to me over about 15 years of working in this space is that while there is a great deal of hope and the internet is an enormously enabling technology and has fantastic opportunities for education, particularly in less developed countries—if we can fix the copyright regimes, that is—it is also potentially the most powerful surveillance device ever imagined. And we need to get that balance right. I guess that is at the core of our concerns.

Senator IAN MACDONALD: It amazes me that people give their credit details over electronic media so regularly. I am surprised that there are not more fraud cases than we hear about—well, I know there are more than we hear about.

Mr Lawrence: Perhaps I could put one quick question back to you on that: do you give your credit card information over the phone?

Senator IAN MACDONALD: I try not to, but I have on occasion, yes.

Mr Lawrence: I would assert that it is much more secure to give it through an encrypted connection to a computer than to a person.

Senator IAN MACDONALD: Probably, yes.

CHAIR: A cheerful thought. Thanks very much again to both of you. We will wrap there, but your time today has been very much appreciated. Perhaps I could get a motion to accept any tabled documents from today's proceedings, principally this stuff from iiNet. It is so moved. That concludes today's proceedings. The committee has agreed that answers to questions taken on notice at today's hearing, I think mainly from the first witness, will be returned by 12 August—two weeks from today. I thank all witnesses who have given evidence to the committee today.

Committee adjourned at 13:02.