COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

ENVIRONMENT AND COMMUNICATIONS REFERENCES COMMITTEE

Reference: Protection of the privacy of Australians online

FRIDAY, 29 OCTOBER 2010

CANBERRA

BY AUTHORITY OF THE SENATE

INTERNET

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

The internet address is:

http://www.aph.gov.au/hansard

To search the parliamentary database, go to:
http://parlinfo.aph.gov.au

SENATE ENVIRONMENT AND COMMUNICATIONS

REFERENCES COMMITTEE

Friday, 29 October 2010

Members: Senator Fisher (Chair), Senator Cameron (Deputy Chair) and Senators Boswell, Ludlam, Troeth and Wortley

Participating members: Senators Abetz, Adams, Back, Barnett, Bernardi, Bilyk, Birmingham, Mark Bishop, Boyce, Brandis, Bob Brown, Carol Brown, Bushby, Cash, Colbeck, Coonan, Cormann, Crossin, Eggleston, Faulkner, Ferguson, Fierravanti-Wells, Fielding, Fifield, Forshaw, Furner, Hanson-Young, Heffernan, Humphries, Hurley, Hutchins, Johnston, Joyce, Kroger, Ian Macdonald, McEwen, McGauran, Marshall, Mason, Milne, Minchin, Moore, Nash, O'Brien, Parry, Payne, Polley, Pratt, Ronaldson, Ryan, Scullion, Siewert, Stephens, Sterle, Trood, Williams and Xenophon

Senators in attendance: Senators Cameron, Fisher, Ludlam, Troeth and Wortley

Terms of reference for the inquiry:

To inquire into and report on:

The adequacy of protections for the privacy of Australians online, with regard to:

(a) privacy protections and data collection on social networking sites;

(b) data collection activities of private companies;

(c) data collection activities of government agencies; and

(d) other related issues.

WITNESSES

Committee met at 9.03 am

FLYNN, Mr Iarla, Head, Public Policy and Government Affairs, Google Australia Pty Ltd

VIJ, Ms Ishtar, Manager, Public and Policy and Government Affairs, Google Australia Pty Ltd

CHAIR (Senator Fisher)—I declare open the hearing of this committee into the protection of the privacy of Australians online. I welcome those present. Evidence given today will be on the public record. If at any stage you want to give your evidence in private, you are entitled to make a request and the committee will consider your request and the grounds for so doing. It is contempt of the Senate and potentially unlawful for a witness to give false or misleading evidence to the committee or for a third party to attempt to interfere with evidence that would otherwise be given before a committee. I welcome our first witnesses from Google Australia. Would you care to make a short opening statement?

Mr Flynn—Yes. Thank you very much for the opportunity to appear here today. I think it is very timely that the committee is looking at privacy online, and we certainly view the committee as an important contribution to debate and discussion in what is a very important area. By way of quick background, Google has been in Australia since 2002. Today we employ about 400 people at our centre in Sydney. We are best known as a provider of search services, but in fact Google in Australia has a bigger story than that. In particular Australia has a very strong engineering and R&D centre for Google worldwide. It is the place that originated Google Maps, for example, and Google Wave. So some very important innovations have originated here.

This morning we would like to try and talk about two things: firstly, privacy online generally and then Google's approach. Our approach is to put the user in control through transparency and choice and also to be a responsible steward of the information that we hold. We think these kinds of principles are actually important for everyone and that they are worth considering by the committee. We also want to talk about Google's collection of Wi-Fi data, because we think that is important. Following our comments we will be very happy to answer whatever questions you have, but we may look for your permission to take some issues away if we do not have the full information to offer here.

First of all, regarding online privacy generally, our view is that the online world offers tremendous opportunities for people—opportunities to get access to all the information in the world and opportunities to communicate and collaborate with people everywhere. Australians are enthusiastic users of the internet. We have research from Nielsen which shows that some 86 per cent of Australians have internet access. But of course the adoption of any popular technology can impact on society. This is certainly true with the rapid uptake of internet technologies, and particularly in relation to privacy it can raise some concerns. But it is our view as we move towards the digital economy here in Australia, enabled by the NBN, that Australia is well positioned to benefit from the opportunities that are out there and to protect privacy online. That is our assessment.

Our view is that the best policy approach to privacy combines education with carefully framed laws and with technology tools that put internet users in the driving seat. From a public policy viewpoint we think there are two things to focus on. The first is education of internet users to be

good digital citizens—and we would be happy to expand on that—and the second is carefully framed laws. We think that the draft privacy legislation currently before the finance and public administration committee is based on a strong principles based framework that has the flexibility to respond to further developments in technology. Another key element of the privacy framework is to have an independent and effective privacy regulator, which is what we believe we have.

Switching to Google, we are motivated to work towards a safe and secure environment for users because it is fundamental to gaining and maintaining users' trust, and that is a key to our continued success. Our view is that service providers generally, and certainly Google, want their services associated with comfort, safety and security, and ultimately that is imperative to the providers' bottom line. Otherwise, if we do not get that right, internet users will switch, and on the internet that is very easy. A different service is literally just a click away. That choice, that ability to switch, is a key protection for individuals. They can easily move to another service or two if they so choose.

For Google, in terms of principles and practice, we take the following approach. Number one, we use information to provide users with valuable products and services. Number two, we put our users in control through a combination of transparency and choice. We design products to give people choices. To give you some quick examples, there is the ability to pause or delete a users browsing history—users have the choice to go off the record when they use Google Talk, which is our instant messaging service. They also have the ability to take their data away from Google if they want to switch to a different service provider. That is something we prioritise. We let our users know what information we collect when they use our products and services, why we collect it and how we will use that data to improve our data.

Our Privacy Centre provides easy to understand information about our products and policies, and that is to help users make informed choices about the services that they will use and how they use them. Google Dashboard is a tool that tells an internet user what Google stores in their account. It lets the user view and control the data accessed or associated with their Google account in one central location. It summarises the data for each product, their use, and provides direct links to the privacy settings for each of those products. The other key element of good privacy practice obviously is security. We need to be a responsible steward for the information we hold. This is something we prioritise and I believe we have a strong security framework in place.

I mentioned Wi-Fi at the start, and I think it is important to address upfront Google's mistake in the collection of payload data from unsecured Wi-Fi networks. We do not always get everything right on privacy. Our collection of this data was a mistake, for which we are sincerely sorry. When we discovered our mistake, we took action—we grounded our Street View cars and we proactively notified regulators around the world, including here in Australia. As you may know, we cooperated with the Privacy Commissioner's investigation, which concluded in July. We have given undertakings to the Privacy Commissioner, which we are in the process of implementing.

As a result of our internal reviews, we have recently announced a series of changes to our internal processes around privacy. I just want to list those quickly. Firstly, we have appointed Alma Whitten, who is a very senior and experienced engineer, as our director of privacy across

both engineering and product development. Her focus will be to ensure that we build effective privacy controls into our products and internal practices. The second point is on training. We are enhancing our core training for engineers and other important groups within the company such as product management and legal, with a particular focus on the responsible collection, use and handling of data. Thirdly, with compliance, we are adding a new process to our existing review system under which every engineering project leader will be required to maintain a privacy design document. That document will record how user data is handled and that document will be reviewed regularly by managers as well as by an independent internal audit team.

As you can see, we take privacy very seriously. We want to reiterate that the collection of payload data was a mistake, for which we are sincerely sorry. We are determined to learn all the lessons we can from this situation. I think a good summary is that maintaining people's trust is crucial to everything we do, and we believe we have to earn that trust every single day.

In conclusion, overall our assessment is very positive. We think there is a huge amount to be gained from the online world. We think Australians are keen to participate and benefit. We think Australia is on track to take advantage of the benefits of the privacy world in a way that addresses the challenges of privacy, and we would focus on two things: education—we need to ensure that people know how to be good digital citizens; and, secondly, we need a carefully framed, principle based legal framework that has the flexibility to respond to future developments in technology. For our part, we are committed to being a participant and a partner in this process.

CHAIR—Thank you, Mr Flynn. Once you have got it this information, can you give it back? Whether that is information that for example organisations like yours might have got through individuals giving it to you or through some sort of let's call it misadventure, irrespective of how you have got information that people might regard as personal and private to them can it ever be given back in an online world?

Mr Flynn—One of the things I mentioned in the statement was that we actually prioritise giving people the ability to exit and take their data with them. We have a program internally which is called the Data Liberation Front, an interesting—

CHAIR—Yes, that is why we have these inquiries. We learn lots.

Mr Flynn—This group has a very serious role and that is to ensure that anyone who wants to leave Google, any service, can take their data with them easily. That team are systematically working their way through all the different products that Google has, to make it easy for people to leave.

CHAIR—But their personal data that you have had up until that time does not vaporise. What do you do with it? It does not vanish, does it?

Ms Vij—For example, if I have a Gmail account and there is data that I have chosen to store in my Gmail account, I can choose to delete that at any time and that will be done. We have backup systems so that, for example, if I want to access my data and for whatever reason I cannot get it from one location, we have a system to ensure the security of that data so that it is

backed up. Once I give the command to delete, it will take a short time to wipe from our backup services, but it is deleted.

CHAIR—Does it exist anywhere after that?

Ms Vij—Once it is deleted and gone from our backup servers it is gone.

CHAIR—From the entire techo-stratosphere—in my language. Senator Ludlam will be a whole lot more savvy in pursuing this line.

Senator LUDLAM—No, we will stick to that from here.

Ms Vij—It depends: if I have stored my data with my Gmail account and I delete it, it will be gone. If I have chosen to put the same material somewhere else, I would have to delete it from the same place. I cannot speak for other services.

CHAIR—So your answer is necessarily confined to how Google operates.

Mr Flynn—Yes.

Senator LUDLAM—Thank you for joining us today. I will continue in that same vein. I have just been looking through my Google account and the privacy dashboard that I think you mentioned before. There are certain kinds of material in here that you are holding: search history is one, web history is another and whatever else is attendant on Gmail, the chat stuff and so on. To confirm: if I am in the crime browser, for example—and presumably in other browsers—and I delete those things here, from my records, that would completely eliminate them from Google servers as well. How does that square with the sorts of requests you might get from law enforcement—for example, serving a warrant seeking you to turn those records over?

Ms Vij—If we take, for example, a law enforcement request that might relate to our logs data from search history, we can only do that during the time that we have retained those logs. We have an internal policy to retain our logs for nine months, and beyond that we obliterate the IP address and have no way of going back. So there are constraints on when and in which circumstances we can do that. To talk more about Google's approach to law enforcement requests, we have a team who examine requests that come in from law enforcement, and we comply with all valid legal requests. That team will look at the request, look at the law it is given under and make sure that the request complies with both the letter and the spirit of the law, and then proceed as appropriate with that request. As an example, in 2006 Google considered one particular law enforcement request to be excessively broad and applied to the court to have that reviewed. In that situation, the court decided that it was too broad, and that formed an important precedent for user privacy—to make sure that the balance between ensuring that law enforcement agencies can get access to the data they need for public safety purposes is balanced against user privacy.

Senator LUDLAM—After nine months you presumably have a pretty sound record of search data and statistics and so on. Is that material just de-identified and held or do you actually eliminate it after that period?

Mr Flynn—With search logs what we do after nine months is we 'anonymise' them and that involves actually altering the IP address such that it could not identify a particular machine any more. So we have anonymised records which may be of some use, but I would imagine for law enforcement—

Senator LUDLAM—Only statistical, I would have thought.

Mr Flynn—Yes.

Senator LUDLAM—Now presumably you have not been forced into that kind of position and that is just company policy. But given that you are not based in any particular country—in a physical sense you do have offices but your business model is very, very distributed—on whose privacy laws did you base Google's privacy policy? Or what is the closest match?

Ms Vij—You are right. Google does operate globally and in that way we believe it is important to maintain industry-leading standards of privacy protection that do meet the expectations of individuals in privacy aware countries like Australia. We provide our services at what we believe is a very high standard and in a lot of cases that will involve looking at the highest denominator in different areas.

Senator LUDLAM—Okay. I want to come to an issue that I think might be a bit of a theme of the day—the government's data retention policy. I am not sure we could call it a proposal yet, but it has been discussed and debated, although it is still rather opaque. The bar on this issue is set higher in some European countries as a result of the EU directive. My first question in this area is: has Google been consulted in the development of the Australian government's data retention policy?

Mr Flynn—We have not been involved in those discussions but obviously we have seen media reports and are aware that those discussions are going on. You mention Europe and we do have some experience there. As you mention, Europe does have a data retention directive which is in the process of being implemented into national law in the different countries, and certainly there is an apparent tension between the need to protect users' privacy on the one hand and seeking to protect public safety through giving law-enforcement the tools they need on the other hand. Our view is that any requirement to retain data to enable the investigation and detection and prosecution of serious crimes has to be proportionate to the resultant privacy impact and anonymity loss for internet users, as well as the costs to search providers of implementing something like that. I guess the key thing that we would take out of it is transparency. That is something that we emphasise in our efforts around privacy and we think it is very, very important. We think the same principle is actually very, very important for measures from government that impact on people's transparency.

On the transparency front, we have launched a tool which you may have seen. It is a website and it actually gives details of the requests we get from governments around the world for two things. One is for data on users and the second is requests to remove content from our different services—like YouTube, for example. We think it is important because it is a step on the road to having greater transparency around these kinds of efforts and we think that is important. We would be interested to see others in industry take the same kind of approach.

Senator LUDLAM—Would you give us the name of that while we are on the record. It is a very useful site.

Mr Flynn—I can give you the URL, which is www.google.com/transparencyreport/. I think if you search, preferably on Google, for 'Google transparency tool' I think you will find it pretty easily.

Senator LUDLAM—Thanks. I am still a bit perplexed though, because you have to deal with a very wide variety of jurisdictions. For example, you had a widely publicised falling out with the government of China. It is probably pushing the boundaries to suggest that they are privacy issues but I guess we could make that case. You have got new laws coming into place in Europe and a similar system under consideration in Australia. Short of pulling out some of your services and your people—as you have had to do in the case of China—I am not sure how you would manage it if the system in Australia or in the EU, for example, went further than your comfort zone as a company and required you to hold this data for longer than nine months.

Mr Flynn—There are a lot of complex legal questions to that. It is a very good question at its core: how does a provider that operates in many different countries, and that in our case seeks to provide a consistent global product with a consistent policy and a set of terms and conditions underpinning that product, meet differing legal requirements? I guess ultimately it is a matter for legal analysis as to which particular laws we have to comply with. We are bound by the laws in countries that we operate; as Ishtar said, if we get valid legal requests we have to meet them. But these kinds of issues are complex and there is not an easy answer to what we do. I think it is fair to say that in some respects European privacy law is amongst the most prominent legal models in the world and something that all providers need to take account of. Beyond that, I do not think I can add much.

Senator LUDLAM—I am not sure that we got much out of that. That sounds like you are possibly as perplexed by the question as we are. I will come back with some more questions later if we have time.

Senator CAMERON—Mr Flynn, I must say I was a bit perplexed by your response that you are bound by the laws in the countries that you operate. People like Nike have been using that for years to exploit workers overseas. It seems to me to be a standard corporate response. Why can't Google establish a best practice approach on this and apply it across all of its operations?

Mr Flynn—We believe we have, Senator. We take privacy very seriously and we are very conscious of the different legal frameworks around the world, but the primary thing for us is what users in privacy aware countries expect, as Ishtar mentioned. So when we are designing our privacy policies in general and our overall policy in terms of privacy, we try to set that as global best practice. I think we can point to initiatives we have taken in a number of areas which represent the cutting edge. We could refer to our efforts around transparency. For example, the dashboard that Senator Ludlam referred to I think was widely recognised as a very good initiative: a tool that gives the user very clear information about their Google account and what is in there. On the retention of search logs, which is another thing we have mentioned, we were the first leading search provider to initiate a policy around a defined period for the anonymisation of those logs. That was another first. And just broadly, in terms of transparency

and choice, we believe we are continually out there innovating and actually developing and following best practice in terms of privacy.

Senator CAMERON—What was Nike's worldwide profit?

Mr Flynn—I do not know.

Senator CAMERON—How much do you spend on research and development on issues such as what is described as privacy enhancing technology?

Mr Flynn—I do not have a figure for that.

Senator CAMERON—Can you take both those questions on notice? I think if you are going to say that you are actually at the cutting edge of this I would like to know how much you spend on research and development on privacy enhancing technology.

Mr Flynn—Okay. The question on Nike, I am not sure we are in a position to answer.

Senator CAMERON—No, I am not asking you a question on Nike. I was just advising you that I thought your statements were consistent with what Nike were saying a decade ago when their contractors were exploiting people all over the world.

CHAIR—For clarification, Senator: I think you indicated two questions on notice, so in fact there is only one. Is that right?

Senator CAMERON—No. Google's profits internationally and if they can indicate what their profits are in Australia and, secondly, how much they spend on research and development internationally and in Australia on these issues of privacy enhancing technology.

Mr Flynn—We would be happy to follow up; we do not have specific figures. Senator, I am not sure if you were implying that Google was exploiting workers in some way, but I would be very, very confident to say that—

Senator CAMERON—No, I did not say that, I said—

Mr Flynn—the treatment of workers by Google is world leading. I think anybody who has been to any of our offices will attest to that, and we value our people. They are genuinely our greatest asset. We have about 400 people here in Australia and are often voted amongst the best workplaces in the country.

Senator CAMERON—Don't be too defensive. I did not say that you were exploiting workers.

Mr Flynn—Okay.

Senator CAMERON—I just said your response was consistent with what big business have said for years about their operations internationally—that is, that they follow the laws. And that

has been used to go to the lowest common denominator. The point I was making, you have answered. You have said you go to the highest common denominator—

Mr Flynn—Yes.

Senator CAMERON—and you use it everywhere, right?

Mr Flynn—Yes.

Senator CAMERON—I understand that some of the best laws around are in the EU, so can you take this on notice: can you advise as to how you commit in Australia to the best-practice laws in the EU?

Mr Flynn—Okay. We will take that on notice.

Senator CAMERON—You say you treat your employees very well. Do you monitor your employees' private computers during working hours? Not their private—do you monitor what they do?

Mr Flynn—We are not actively monitoring our employees, but we do have a very extensive security framework internally, which is what you would expect for a company of our nature. Most employees in Google have no access to any data. Decisions on that are very much taken on a needs basis; we are very conscious of that, and we have a whole set of layers, if you like, to our security network. That starts with physical security, so we have extensive systems internally about restricting physical access to data. I mentioned our employees. We have some of the world's leading security experts, who are both internal facing and external facing, to try to address any security challenges that arise. We have extensive training around these things that we deploy extensively across the company, and I mentioned in our opening statements some of the updates we are doing to that. We also have a company code of conduct which every employee must sign up to, and that contains additional provisions around security and privacy. So, in summary, we have a very comprehensive security network internally, and that is about protecting the data that we hold. Ultimately, we need to be a responsible steward of that data. We are very committed to that.

Senator CAMERON—The point I want to make is that there has been some concern in some submissions we have had about monitoring employees' use of computers for private purposes during working hours. Do you do that?

Mr Flynn—I think we will take the question under advisement, if you do not mind. I am not aware of any policies we have in place for that, but obviously the work that a person does during company hours is something that is relevant to the company. Certain employees will have the ability to access data, and I think it is reasonable to expect that the company will be in a position to implement its code of conduct and to meet any legal requirements that might come across.

Senator CAMERON—If one of your employees has that level of access but they want to pay their electricity bill online, is that monitored?

Ms Vij—The kinds of things that we would look at in terms of that are that we would audit the access logs. As Iarla mentioned, there are a very finite number of people who would have access to any of the data, and it is on an as needs basis only. We do spend a lot of time auditing those logs to see what has happened. Coming back to your question about monitoring use during work hours, we will take that on notice, but, as we said, the types of concerns that typically an organisation like Google would have are security concerns—making sure there is no malicious software being downloaded and those types of things.

Senator CAMERON—That is fine; I understand that. I have a couple of other questions before I finish up. I do not have a Google account, but I use Google quite extensively. I have two Google configurations up here now that I can access—

Mr Flynn—Thank you very much!

Senator CAMERON—But I have a few of your opposition ones open here as well. I did not know about these things previously, and I use Google quite extensively. I was totally unaware of your Data Liberation Front. I was unaware that I had the option to wipe any print of what I had been doing. A user like me does not have a Google account, so you do not know these things; it is impossible to know. So how can we fix that?

Ms Vij—Let us step back and look at it. What you are talking about is where a user is not logged in and they are using services. We build services like Google Search and Maps without a requirement to log in because we respect that people might want to interact anonymously. In that case in terms of education and making sure there is a broad understanding of the types of tools for being able to control your browser history or whatever it is, we take that kind of education work really seriously through our privacy centres—and we have got really short videos that are very accessible. I think sometimes a privacy policy can become a long kind of legalese document that is very difficult to digest, so we do our best to make sure that the information that we provide is really easy to understand.

Senator CAMERON—I really do not have much time left and you are off on a little frolic here. That is not what I am asking. I am just a user who does not have a Google account and there are all these checks and balances in terms of privacy, but not for me because I do not know. As I said, I have got Google boxes open here. I cannot tell that there are any privacy checks and balances that I can access. Why not?

Ms Vij—First off, if you are not logged in Google does not collect any personal information. So the only thing that would be going into our server logs is the IP address of the machine that you are using at the time you make the search. We do not have any way to tie that back to who the individual is, so there is no personal information in that instance being collected.

Senator CAMERON—I have noticed when I have been on Google and I have been doing some searches that up comes an advert for something in the bottom right-hand corner. That is not me who has been doing that; that is somebody out in etherland saying, 'We're watching what you are doing. Here we are.'

Ms Vij—For the advertisements on the search page there is a computer algorithm that looks at the search query that you type in. For example, if I am searching for 'kitten' it might throw back an ad for kitten food, so it is matched to the particular search term that is used.

Mr Flynn—The other thing that I would say is that a person who has a Google account is getting into a greater level of engagement and we are in a position to have greater privacy tools for that person. As for the person who is using services without an account, that, I think, goes to our broader approach to privacy, which is you have a choice not to log in and you have the choice to just use these services if you want. We have a link to our privacy policies on our homepage, so that is there and you can click through and access that stuff very easily. The other thing that I think it goes down to is this: you are at liberty to switch to other search services if you want, and I think it goes down to an element of trust because some users will not want to look at privacy policies, even though we try to make that as easy and as accessible as possible. Fundamentally, there is the issue of trust. If you do not trust Google to be a responsible protector of your privacy and a responsible steward of the data, you can move elsewhere very easily. That is the key test that we face every day with every internet user.

CHAIR—Senator Troeth has a question for you about that.

Senator TROETH—Yes, that is right. I made sure that I knew what the term 'cookie' meant and I just wanted to ask this. Does Google use cookies to track the websites that the search engines that it uses visit for the purposes of targeted advertising?

Mr Flynn—First of all, cookies are very widely used on the internet.

Senator TROETH—Yes, I understand that.

Mr Flynn—Most websites and, indeed, all search engines will use cookies, so it is a well established practice. Google does engage in interest based advertising, and I would be happy to talk a bit about how that works. What it is about essentially is trying to give an internet user more relevant advertising.

Senator TROETH—How do you store that data?

Mr Flynn—The way it works for us is that we do interest based advertising on a network of websites that we refer to as the Google Display Network. That is a network of websites, including YouTube, where we have the opportunity to place these kinds of ads. The interest based advertising system effectively uses a cookie and, when the machine on which that cookie is present visits one of those websites, that is added to what we have as an anonymous database. Over time that may effectively add interest categories. For example, if a particular machine is visiting a lot of sports websites, then over time the interest based advertising system will conclude that that particular user is interested in ads for sports. Then, when that user goes to another website on that broad Google Display Network, they may get an ad for sporting material.

Ms Vij—There is a very high degree of transparency around what Google does with this as well. You can visit what is called the 'ads preferences manager.' You can edit the different

interest categories associated with the cookie on your computer. You can also choose to opt out entirely.

Senator TROETH—I do not mean this in a bad way, but are you selling that data to advertisers or are you simply holding it for your own purposes?

Mr Flynn—We hold it. We do not give data to advertisers in that manner.

Senator TROETH—And you can opt out?

Mr Flynn—You can opt out. As Ishtar says, you can select or deselect categories and you can opt out from that entire Google interest based advertising system. We have set up the two, which allows people to do that.

Senator TROETH—I know when I go on to the Amazon website, it says, 'If you're interested in this, you may also be interested in this' et cetera in terms of categories of books and music. If a jurisdiction were to legislate that you must get consent before cookies can be used to track an individual's web-browsing history, what implications would that have for Google?

Mr Flynn—It is difficult to say. I am a bit cautious about speculating. Maybe if I could talk more broadly about advertising. Certainly, Senator Cameron referred to the ads that appear with search results. That is Google's primary business, and it is the revenue from that advertising that allows us to do research and development and to develop new products. Indeed, it is true that, on the broader internet, advertising is one of the key ways that pays for all the services that people can access online. Internet users have become used to the ability to freely access a lot of very useful information. Interest based advertising is generally about trying to make advertising more useful and about trying to allow, in particular, publishers, news organisations and others to get a better revenue stream. One of the big challenges in the internet space that we face is making good content pay for itself. So a system that requires 'opt in' could have a negative impact, but I do not want to speculate beyond that because obviously there would be complex legal and operational questions.

Senator TROETH—You also referred in your opening statement to education. I would point out to you, as you probably know, that the Privacy Commissioner's submission makes the point that individuals often do not read or understand privacy policies. Is that a concern to you and, if so, what type of measures legislative or otherwise do you think would be effective in dealing with that issue?

Mr Flynn—We acknowledge that that is an issue. What we try to do with our privacy policies is make them as easy to access and as simple to understand as possible. One thing we do for a lot of services is actually use videos to explain the main features of a service, particularly the privacy features. Often, videos are just an easier way for people to access and understand the main elements. We then try to use really simple language to describe, again, what the service does, what information is collected and what we are doing with that. Obviously, we have very comprehensive privacy policies but, again, we make a really determined effort to make those as simple as possible. I think education has to be an ongoing effort. At the rate at which the internet is developing and new services are coming along, it is never something we are going to fully achieve. We are certainly very committed to that effort. It is ongoing.

The other point I would make is that we think there is a broader concept here of digital citizenship, which is maybe a broader educational effort to ensure that everybody, particularly kids at home—perhaps in schools—is given information about the services that are out there, the opportunities and also the risks and how they can essentially—

Senator CAMERON—(Inaudible)

Mr Flynn—They are the users of these services and probably understand them better than most. But there is the challenge there of ensuring that they understand the broader context, because there are privacy risks online. We need to ensure that kids are particularly aware of that. But I would not make a pessimistic assessment. We have seen some research that indicates young people are amongst the most active users of tools on social networking sites—for example, about tailoring what information is and is not out there. We should be more positive about that. But it is an ongoing challenge and it is really important. Maybe there is a case for making digital citizenship education broadly a part of the curriculum in schools.

Senator WORTLEY—In your submission you say that you started:

… collecting WiFi network information via our Street View cars to improve location-based services like search and maps.

Further on—it is almost in the present tense—you say:

… we have decided that it's best to stop our Street View cars collecting WiFi network data entirely.

Could you just explain that to us?

Mr Flynn—The cars that we had driving here and in other countries were primarily taking pictures for the street view service. They were also collecting Wi-Fi information. The information that we were looking to collect and intended to collect was essentially the publicly available network addresses for Wi-Fi services and that was to help with location based services. But when we discovered the mistake in the collection of payload data we stopped all street view driving and we have not currently resumed driving here.

Senator WORTLEY—Not only are you not using the Wi-Fi network data connection; there are no street view cars operating in Australia at the moment?

Mr Flynn—That is correct. For the future phases of street view driving we will not be collecting any Wi-Fi information at all.

Senator WORTLEY—What do you see is the future for street view driving?

Mr Flynn—We think street view is a very useful service. It is very popular. Street view allows somebody who is looking for information about a particular place to actually see an image. So if you are going to a hotel, you can see it on a map and that tells you one thing, but to actually see an image is more useful.

Senator WORTLEY—I understand that. Will the street view cars be active again in Australia?

Mr Flynn—We would like to do that, but we have no plans to resume at this time.

Senator WORTLEY—You do not have a plan for them at this stage?

Ms Vij—Ultimately, we would like to. There is no time line associated with that at this time.

Senator WORTLEY—How many street view cars did you have operating in Australia?

Ms Vij—I would probably have to check on that one. I can do that.

Senator WORTLEY—If you could take that on notice.

CHAIR—Ms Vij, you talked about deleting data so, once you have it, individuals can delete it. Mr Flynn, in response to Senator Ludlam, you talked about anonymising data. How do you delete it? 'Anonymise' means that you keep it, but you disconnect it from the person to whom the information belongs. They are not the same, are they? I come back to my original question: once you have it, you have it forever, haven't you?

Ms Vij—It depends on the service. So for something like Gmail it would be deleted. Search logs would be anonymised. There would be no way to go back and connect that to an IP address. In that case, that aggregate, anonymised data would be kept, but that is not people's personal information.

Senator WORTLEY—In other forums people have said that they receive advertising specific to their age. There are advertisements coming up that are relevant to people's ages. So if you are a teenager you will get advertising targeted at teenagers and if you are a middle-aged man you will get advertisements targeted at a middle-aged man. How does that process work?

Ms Vij—There are a number of ways that you could be targeting the ads. If it is based on contextual advertising it would be what kinds of keywords are on the page. In another circumstance, if it was based on interest category, perhaps popular music, then an ad related to popular music might come up. So whilst it might look like an age thing it could also be a particular interest category.

On Google's part—and I cannot talk more broadly than that—Google recently announced that it will begin inferring demographics for interest category advertising. This means that the cookie on the computer will have associated with it an inferred demographic. How that would work is that it would take into account the websites that a computer visits over the Google Display Network. Perhaps they visit websites which publicly available information says are popular with 30-year-olds. In that case Google might infer that a person is in that age bracket. Any of those age bracket are only 18 and above and they are entirely transparent to the user. They are included in the ads preferences manager and can be removed or edited by the individual.

Senator LUDLAM—Is Gmail reading the mail that we get and send in order to target ads—reading in the loose sense of the way in which software would stand for something?

Ms Vij—No person is reading—

Senator LUDLAM—No, not a person, but the software, the database itself, in order to target the ads.

Mr Flynn—There are algorithms which are scanning the mail in order to push ads rather than—

Ms Vij—It is contextual advertising based on keywords.

Senator LUDLAM—So it is; the database is actually reading our mail and deciding which ads to flick at us depending on our inward and outbound mail.

Ms Vij—It is the same kind of technology that also scans to identify viruses or spam. In a similar way it looks for particular word—or patterns, I guess, in the case of viruses or spam—to identify that, in the case of advertising, this keyword appears, so this might be a relevant ad. If a person does not want to see advertising on Gmail they can use the HTML version of Gmail.

Senator LUDLAM—Yes. I find that whole concept a little bit creepy, particularly as these algorithms get better and better and better. It is not that a person is reading the email; it is that the database itself is reading is and then targeting material to you.

CHAIR—And could not a person later access that information?

Senator LUDLAM—Or a law enforcement agency.

CHAIR—Spot on!

Senator LUDLAM—For example, if you are served with a fairly broadly based warrant that was essentially a phishing expedition, how deeply into people's communications could that sort of thing read?

Mr Flynn—For any requests from law enforcement we have a specialised legal team who will review that in detail. Anything that is in the nature of a phishing expedition will not be accepted. Requests for customer data we take very seriously, and the request will need to meet the spirit and the letter of the law. Those are the tests that any requests will have to go through and, as I mentioned earlier, we have created the transparency tool to give a level of transparency to all users as to what is going on. Certainly things like phishing expeditions are not things we would cooperate with. Ishtar mentioned a request in 2006 from the US Department of Justice for a large body of search records. In fact we challenged that in court and won that particular action. So we do take these things seriously. We think it is a very important role that we protect our users' privacy and are a strong steward of that information.

Senator LUDLAM—But we are very much relying on Google's goodwill. The technology is sophisticated. Presumably you are spending a lot of money better developing and targeting it, but we are effectively relying on their goodwill and a corporate culture which has come from a certain place—I think most people are quite appreciative of that, but it could change.

Ms Vij—I think we mentioned in the opening comments that everything that Google does is only as successful as the trust that our users place in us. We are incredibly conscious of that, so

we have to constantly be earning that trust and making sure we are protecting the privacy of our users.

Senator LUDLAM—Did the Street View Wi-Fi data all get deleted?

Ms Vij—There are ongoing investigations in various parts of the world.

Mr Flynn—We certainly want to delete the data.

Senator LUDLAM—I will leave it there. Thanks.

Senator CAMERON—It seems to me that you are not allowed to phish for law-enforcement purposes—if it is a phishing expedition you are not allowed to do that—but you can phish for profit and you can phish for people who are paying you in terms of your company's profits. I think there is a bit of an issue there, and I would like you to think about that and tell me if that is a position that is acceptable. I also would like to know whether your profit model would allow an opt in on monitoring of the browsing history or on Gmail. Could you say, 'I opt in to allow this monitoring'? Would that destroy your profit model?

CHAIR—Those are two questions for you to take on notice rather than answer today, I am afraid. Thank you very much.

[9.56 am]

FALK, Ms Angelene, Director, Policy, Office of the Privacy Commissioner

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

CHAIR—Welcome. I believe you were both in the room and heard the formal palaver at the opening, so I shall not repeat it. Would you like to make a brief opening statement?

Mr Pilgrim—Yes, I would like to do that. Prior to making a brief opening statement, I will make a personal claim for both of us that we are in the process of losing our voices, so if we need to stop—

CHAIR—We will try to help you do that.

Mr Pilgrim—Secondly—for the committee's benefit as well, because it may have some importance for the ongoing interaction with us after today's hearing—this will be the last hearing that the Office of the Privacy Commissioner will appear at in its existence as the Office of the Privacy Commissioner. From next Monday, 1 November, we are integrated into the new Office of the Australian Information Commissioner, which has been established through various enactments. That office will be set up with three statutory office holders: the Australian Information Commissioner, who will be Professor John McMillan; me, as Privacy Commissioner; and a yet to be announced Freedom of Information Commissioner. The new office will have responsibility for freedom of information under the Freedom of Information Act, continuing responsibility for privacy under the Privacy Act and a broader role to provide advice to government and other entities on government information policy. So, for the purposes of the committee, from next week interactions with us will be to the Office of the Australian Information Commissioner.

CHAIR—Can you recap those three roles that the new office will have, very quickly—just the names?

Mr Pilgrim—Certainly. There is the Australian Information Commissioner, the Freedom of Information Commissioner and my position, the Australian Privacy Commissioner.

CHAIR—Do you have an opening statement?

Mr Pilgrim—Yes. Thank you for the opportunity to address the committee today. I appreciate this opportunity to provide input into the Senate Environment and Communications References Committee inquiry into the adequacy of privacy protection for Australians online. Privacy issues continue to be in the news a lot these days and privacy remains a key issue in the information age. It has come to the fore much because the information disseminated online is information about people, whether via blogs, social networks, online news sources, instant messaging, email, internet shopping or banking. In the internet age personal information is easy to access and publish. It is searchable, downloadable, reusable and can remain in circulation sometimes indefinitely.

These changed conditions for information handling can have a significant impact on the protection of individual privacy. Once released online, it can be difficult to recoup, delete or control what happens to personal information. A major focus of the work of my office is ensuring that individuals have as much control as possible over their personal information and how it is used. In the information age it is critical that we find ways to provide protections for privacy online and to allow the control of personal information to remain as much as possible in the hands of the individual.

In Australia, the Privacy Act provides a mechanism to support good personal information handling by government agencies and private sector organisations and offers an avenue of redress for individuals who believe their personal information may have been misused. Since its enactment over 20 years ago, the Privacy Act has operated against a backdrop of significant change associated with the information age and the rise of the internet. To ensure the ongoing effectiveness of the Privacy Act in a rapidly evolving technological environment, considerable work has been done in recent years to review and reform the act. Most significantly, the Australian Law Reform Commission undertook a review of privacy—the largest review to date—and the government has provided a first stage response to that review.

I am of the view that proposed reforms in line with the government's response will enhance the operation of the Privacy Act, ensuring it remains effective in the face of continuing technological change. However, legislation alone is not sufficient to ensure the protection of personal information for Australians online. One reason for this is that domestic laws will not always have jurisdiction in the transnational space of the internet. For this reason, I support a multifaceted approach to the protection of privacy online. This approach should comprise principles based legislation with specific technology issues dealt with under binding codes where desirable and necessary, user empowerment through education, privacy enhancing technology design and international cooperation between jurisdictions.

I know there are a number of issues that the committee is particularly interested in, and I might touch on a couple of those. In terms of transborder data flows, we note in our submission that regulating privacy online can be difficult due to the greater ease with which personal information can flow between jurisdictions. Like other regulatory schemes, domestic privacy laws may struggle to cope with the ubiquitous nature of the internet. In Australia, organisations that send personal information overseas for processing continue to have obligations under the Privacy Act with regard to that information. The Privacy Act also contains provisions to allow extraterritorial operation where an overseas organisation carries on a business in Australia and collects or holds that information in Australia, and the current reform process is working to enhance those provisions.

To further enhance the ability of the privacy regulators to protect personal information, there has been considerable work done to strengthen international cooperation on privacy regulation. This has included development by APEC of cross-border privacy enforcement arrangements to facilitate the handling of privacy complaints between jurisdictions. As well, there is continuing activity through the OECD's working party on privacy and internet security issues.

Another area of interest is data retention, particularly for law enforcement purposes. A central principle in the Privacy Act is that agencies and organisations should only collect the personal information that is necessary for their functions or activities. Generally, my office would not

support the collection of personal information on the chance that it may be just useful at some later date. As noted in our submission:

> … broad scale collection and retention of web browsing information could significantly impact on the privacy of individuals.

I would suggest that any changes to the retention and use of web browsing information are closely analysed for privacy impacts. A privacy impact assessment would provide an avenue for ensuring that privacy is appropriately protected.

A final issue I will touch on that I know the committee has interest in is online behavioural advertising. In my view individuals should be able to move about the web without their movements being tracked or monitored by others, including the providers of targeted advertising. Where the identity of an individual can be reasonably ascertained from information collected online, the Privacy Act may apply; however, in many cases the information handled by providers of online behavioural advertising may not meet the definition of personal information under the Privacy Act, and in such circumstances other approaches to regulation may need to be considered.

Finally, I would add that the information age promises great benefits to enhance the lives of the individuals within the community. I believe that these benefits can be achieved while still recognising and respecting the privacy of individuals and therefore their dignity.

Senator TROETH—In its submission, the Internet Safety Institute pointed out that the threshold tests for law enforcement agencies to gain access to online data versus offline data are currently inconsistent, with the former being substantially easier. In your view is it appropriate for different standards to apply depending on whether information was sent online or offline?

Mr Pilgrim—I would say that my position is that I would favour a consistent approach to data protection. I have not seen demonstrated necessarily why there should be any difference between whether the information is being handled online or offline. I have not seen a strong case put forward to explain that to me.

Senator TROETH—A number of submitters also expressed concern about the Commonwealth Attorney-General's proposed data retention framework. Some of these submitters were the Law Institute of Victoria, Electronic Frontiers Australia and Rule of Law Institute of Australia. Does your office have a view on whether internet service providers should be required to retain information in the event that a law enforcement agency requests it at a later date? And do you have a view on the privacy implications of such a practice?

Mr Pilgrim—One of the issues that we face when we are looking at the retention and collection of personal information are the risks that are going to be associated with holding information for a long time when there may not be necessarily a clear or defined purpose for it. If you hold information—whether it be in databases or even if we look at it in the old style of a filing cabinet—and have it sitting around for a long time there is often a great risk that something could happen to it. It could be mishandled or used for inappropriate purposes.

Our office takes the approach that when we are considering any proposal for data usage, particularly data retention, we need to first of all understand what the exact problem is that is trying to be responded to by proposing something such as data retention. Is the response—be it setting a timeframe of six months, one year, two years or however many years—proportionate to the risk that is being proposed? You need to clearly understand what the risk is that we are trying to address by maintaining and keeping this information.

We then say that a further test should be that if there is a decision to go ahead and keep this information, and if that is going to be based in legislation, then we would like to see a privacy impact assessment done to assess and to further identify where there may be particular risks in holding onto information for that length of time. One of the other key issues that we would need to see addressed in any proposal for data retention is what the accountability mechanisms are going to be. Are there sufficient accountability mechanisms to ensure that if that information is being held it is being held securely and that it is not being misused or used for any other purpose that would be beyond the expectation of the individual? Finally, there should be review mechanisms to ensure that those processes are in place and to make sure that, for example, the risk that led to the establishment of those sorts of proposals is still there and still warrants that sort of retention.

Senator TROETH—What sort of length would that review mechanism entail?

Mr Pilgrim—Again, if we are talking about a review of legislation, it would depend on, in my view, what the legislation is seeking to achieve. I would suggest that—I do not want to pick a period out of the air—it is not uncommon to have either a two-year or a five-year review of legislation such as that.

Senator TROETH—I would like to move on to the small business exemption. If an Australian company which falls within the small business exemption stores its data with an overseas company, is there anything in the Privacy Act 1988 which prevents that overseas organisation from using that data other than in accordance with the NPPs? If not, what options are there for regulating that practice?

Mr Pilgrim—If an organisation within Australia is a small business, as defined by the Privacy Act—that generally means it falls underneath the $3 million threshold—then the Privacy Act does not apply to any of its activities: how it collects the information, what it needs to do with the information, and who it passes it on to. Flowing from that scenario, if that small business that is exempt from the act then passes that information to an organisation overseas, and assuming that that organisation overseas has no links to Australia, then with that scenario the Privacy Act would not come into play for either the small business or the overseas entity, and therefore that personal information would not be subject to the protections of the Privacy Act.

Senator TROETH—On that same subject, the Australian Law Reform Commission recommended that the small business exemption in that Privacy Act 1988 be removed because of the increased use of technology by small businesses. Do you have a view on that recommendation?

Mr Pilgrim—We think that the application of any exemptions to the Privacy Act should be carefully worked through. There should be very strong policy justifications for why you exempt

any organisations from the coverage of legislation such as the act, which is intended to protect the personal information of all Australian citizens. I balance that by saying though that, when we are looking at an area such as small business, we also need to take into account the regulatory burden that legislation inevitably will impose onto organisations. At the moment, with small business exemptions, an organisation can be identified—possibly, say, due to its large holdings of personal information. An example might be ISPs. An ISP could be in the small business category. Its turnover could fall under $3 million, but when you think about the amount of information that is flowing through an ISP you can assume there is quite a large amount of personal information.

There is already provision within the Privacy Act that, in that situation, a group of organisations such as ISPs can be inscribed into the coverage of the Privacy Act—so there is a mechanism to do that. So I suppose, without giving a very black or white answer on it, I am for making sure that the exemptions are minimised. Where there is a need to protect personal information where there are large data flows, I think there are mechanisms there to do that.

We would need to look carefully at any recommendation to remove the small business exemption, because I too would acknowledge that there is potentially an impost through the regulatory process on small businesses that may not need to have that sort of impost. If I could use not a glib term but a colloquial example: the local fish and chip shop or the corner milk bar may have very little personal information. But if you remove a blanket exemption like the Privacy Act from small business then there may be issues that they would have to consider that may not necessarily warrant that level of regulatory burden on them.

Senator LUDLAM—Thanks very much for coming in this morning. I will start with comments you made on online behavioural advertising. There has been a little bit of material in the press but I do not know that many people understand how pervasive that is becoming. You are probably better informed than nearly anybody else in the country, so what would you describe at the moment as the cutting edge of online behavioural advertising? What is the innovation at the moment that you are tracking?

Mr Pilgrim—I would not necessarily flatter myself by saying that I might have more information than other people on what is going on. We pick up a lot of our information, like everyone else, from what we are reading in journals and through the press as well, and we try to keep abreast of what is happening. In terms of online behavioural marketing, I would just like to digress for a moment and say that some of the challenges we do have from a regulatory perspective with online behavioural marketing are when in fact the information that is being used is personal information. The Privacy Act has a definition of personal information which at its very basis says that the person needs to be identifiable or that the identity of the person is reasonably ascertainable by that information. So we start to get into quite a complex issue when we are looking at organisations' data holdings about whether or not what they hold is in fact personal information—when does an IP address, for example, become a piece of personal information?

We then look at the information that is collected from search profiles, for example, or search logs where a person may be going through Google searching for particular information. One of the challenges we face too when we are looking at what is personal information in that context is where an organisation could hold the IP address—that, by itself, may not be personal

information—and it could start pulling together search profiles of where that IP address has been going to. One of the challenges that comes out of that is: when does that compilation of information give a particular organisation enough information to say that that is a particular person and therefore they are identifiable? That is one of the challenges we are finding as we start to look into the issue of behavioural marketing and those areas. It is not something that we can give a very easy black-and-white answer to simply because it does rely on a lot of different organisations pulling together disparate bits of information to end up with a piece of marketing turning up on your computer and then whether that particular organisation had enough to say, for example, that is Timothy Pilgrim who is doing that particular bit of search.

CHAIR—Mr Pilgrim, would you care to reflect on Google's input in terms of the ability for individuals to delete data versus Google's anonymisation of data in terms of disconnecting user from information to which you just referred? Have you got any reflections on Google's evidence—and I presume you heard it?

Mr Pilgrim—Yes, I did hear Google's evidence. I would also say that I would like to be cautious and just make some general comments. I would not like anything I was going to say in this response to reflect a particular view on Google's activities.

CHAIR—It can be generic.

Mr Pilgrim—Any large organisation that does collect information like that will have access to various different aspects of a person's search history—their browsing, their preferences online and the like. When an organisation deletes information—which we encourage and is actually in the National Privacy Principles that when it is no longer needed or necessary it should be deleted—that is an excellent approach and we would support any organisation following those principles obviously.

In terms of a anonymising the information, again we would say that if it is truly anonymised and you cannot link it back to any source or to any other identifying characteristic of the person—so it cannot go back to their IP address and it cannot be linked back to, say, their email account—then without putting a blanket black and white response, that would probably not constitute personal information for the purposes of the act. We would then say that there is not a regulatory role on that bit of data—and I use the word 'data' deliberately as opposed to personal information—because if it is completely anonymised we would say that it is data and no longer personal information and therefore not subject to the protections of the act.

Senator LUDLAM—I still feel as though we are walking into a little bit of a grey area. We spoke a bit about cookies. I have recently been reading about the system that Flash software uses to track what kids are up to online on some the games sites and so on. Just recently we heard from Google that people are not reading your Gmail account but that software is. Maybe 'reading' is not quite the right term. Software agents, with targeted commercial messages, are learning more and more about us, in which case it starts to be a little less relevant as to whether they know who we are or what our name is. The fact is that these agents are gathering more and more accurate ideas of who people are and what kind of material to fire at them. It feels like we have moved into a bit of a grey area. It is not about how much somebody else might know about us but that very large and quite powerful commercial entities have databases that know quite a bit about us, whether their management care to or not. That information is quite valuable. Given

that it is not necessarily transnational—perhaps postnational is the right word to use—how on earth as domestic legislators are we meant to cope when that kind of material is so completely postnational? I do not know that that is the right word to use. We have privacy principles that we are in the process of redrafting and reconsidering, which is helpful, but do you have any advice for us as a committee as to where you think we should go, given that we are not just dealing with people anymore?

Mr Pilgrim—I entirely agree with you in that it is extraordinarily grey and complex. First of all, I go back to one of the areas I just covered, which is: what is the information that is being used by the organisations? I do not want to apologise for coming back to that, but our responsibility in our office is to look at the regulatory role under the Privacy Act and that regulatory role is based around what is personal information. What we are dealing with here in terms of marketing is that, when you or I go on the internet—whatever we are doing—we will get advertisements coming up to us. As you say, those advertisements are getting more and more targeted because of the ability of the systems to be able to check our browsing history, look at our IP address and make assumptions that the person at the other end is interested in something. I leave aside this issue: what if you have one computer in a household with a number of people? Different people could be accessing it and getting totally irrelevant marketing.

What we would like to see as much as possible in that context is choice—choice for the individual to know what is happening and choice to be able to at least opt out if not opt in to that sort of marketing, where it is effective and will work. In terms of how we can deal with that for individuals, as I said at the beginning of my statement, one of the key things we have to do in recognition that legislation, in my view, can only go so far when we are dealing with transnational flows of data is find ways to better educate the community. Our office does its bit in trying to do that and puts out publications and advice. Many other government agencies do that, such as the Australian Communications Media Authority and the department of broadband and communications. Everyone is trying to help educate the community a lot more. I would add that quite a number of the private sector organisations we deal with regularly in this field also take a very positive approach to trying to educate their customer base and allowing them to know. It is a difficult and ongoing issue for us.

We heard from the previous witnesses about issues surrounding privacy policies. The Privacy Act requires all private sector organisations covered by the act to have privacy policies, but, again, we hear constantly that privacy policies get extraordinarily complex and can become virtually worthless if people are not prepared to read them. So we have to find new mechanisms to allow people to understand what is going to happen to their personal information and be able to make educated choices before they enter into various transactions, or even when they are just browsing on the web—how do we educate the community? That is going to be one of the key areas. We have suggestions on how that can happen, as do a number of different government agencies—through increasing awareness—but, at the end of the day, it comes down to individuals taking the time to read those bits of information and taking on responsibility to be aware of what is going to happen to their information once they are online.

Senator LUDLAM—I suspect that everyone in this room at some stage would have scrolled past 15 pages of finely printed legal waivers of various rights and just ticked ‘I accept’ so that you can get on with it. I suspect that is part of the problem. You make a point in here about

privacy impact assessment. How mature is that as an instrument or a tool? How widely applied are PIAs in Australia?

Mr Pilgrim—Our office has put out a privacy impact assessment guide on its website. We developed that initially for government agencies to be able to undertake those when developing new policy proposals or new legislation, and we strongly encourage all organisations to do it. We have recently amended those guidelines for application in the private sector. Obviously, we think that it is a great tool and it is one that we think can have a benefit for any organisation planning to use personal information in some way, because it can help them identify where the key risk points and the key issues in terms of how they are going to use that personal information are going to be and then put in processes which can make the policy or process itself more privacy enhancive or more privacy friendly. So we strongly encourage all organisations to adopt the use of PIAs as part of their development processes.

Senator LUDLAM—I think that is a very useful body of work. Has your office been consulted on the Attorney-General's proposed data retention policy? Have they come to you for some advice?

Mr Pilgrim—The office has had some discussions over the last 12 months or so with the Attorney-General's Department on those issues, yes.

Senator LUDLAM—In the interests of respecting the Attorney-General's privacy, what can you tell us about what they are up to, because we are finding this whole proposal somewhat opaque?

Mr Pilgrim—At this point in time I do not believe that I am in a position to be able to give any detail on that. The conversations we have had with the Attorney-General's Department, as you would probably appreciate, have been in preliminary policy type discussions, so it would not be appropriate for us to discuss those issues at this time. My understanding from the last interactions that I have been aware of is that they have been fairly preliminary.

Senator LUDLAM—Thanks for your time. I will come back again if there is time.

Senator WORTLEY—Mr Pilgrim, in your submission you talk about social networking sites and about the privacy policy, and you rightly point out that many of those sites will put on their privacy policy that they have the right to change it at any time. Given that, how confident can users feel that the privacy policy that they have signed up to is actually going to continue to exist? Even if you do go through however many pages worth of privacy policy and then agree, and the social networking site have explained how they would protect your privacy, there are no guarantees in that because at any time they are able to change it.

Mr Pilgrim—I think that is of concern, and it does concern my office. We have had discussions with some organisations about those sorts of clauses within privacy policies. We think that, if an organisation is going to change its privacy settings or how it handles privacy, it does need to be upfront with the individuals who have signed up to it. So, before any changes happen, it should be advising those individuals that there is going to be a change to the privacy settings and what they are going to be, prior to those changes coming into place, so that the individual can then make a choice to either continue using that site and continue being a

customer or choose to leave and take their business elsewhere. I do not think it is necessarily good practice on the part of organisations to say, 'We will change our privacy policies at any time and not give warning.' It may be useful to say that there may be changes—to acknowledge within a privacy policy that you may need in the future to revisit your privacy settings or your privacy policy—but I would say that that is when the person should be aware of that before it happens so that they do have the ability to make a choice to remain or not remain.

Senator WORTLEY—So the user has no ability to have an input into whether they agree with that or do not agree with it. The other thing you said is that you think that, so there is actually no requirement for the social networking site to inform the user that that is the case?

Mr Pilgrim—Under the Privacy Act, if they are an Australian company, they have to set out specific issues and specific uses of personal information within a privacy policy and they need to comply with that. If they did not comply with what they have said about how they were going to use the personal information then they could be in breach of the Privacy Act, assuming that they are an Australian based company. If the organisation arbitrarily changed how they used that personal information and started using it in a different way that the individual was not aware of, they could then be in breach of the act as well. So there are some protections there, and I would stress again, coming back your point, that this is where the companies are Australian based.

Senator WORTLEY—So if they are a social networking site from overseas then that will not be the case.

Mr Pilgrim—This is why, leaving aside whether the privacy policies are 17 pages long or two pages long, there is a real importance for all of us involved in this area to try and stress to the community why it is so important to carefully read these policies. Even though they may be long and sometimes boring, it is important so they have at least the best understanding possible about what is going to happen with their personal information.

Senator WORTLEY—Even though you read the policy and then that could change?

Mr Pilgrim—I would suggest—and this is a personal view—that if I was reading a policy that suggested that at some time it was going to change and I was not going to be made aware of that, I would be very carefully thinking about whether I wanted to provide any information to an organisation such as that.

Senator WORTLEY—Thank you.

CHAIR—I have a couple of questions before we bid you well. In our quest to ensure privacy online, are we applying offline thinking to online issues?

Mr Pilgrim—That is a very good question. I would like to think that none of us are in this debate, but there are so many things going on in the online world in the new technological environment it is very difficult for all of us to keep up with what is happening. That is why in terms of the reforms of the Privacy Act my office would stress that it needs to remain technologically neutral. We need to have principles based laws that can remain flexible, given the rapid changes that do happen within the information technology sphere. That is why we need to maintain flexible laws.

CHAIR—Using your office as an example, and a good one for the job you do, are you capable of staying abreast of the technological game? That is No. 1. No. 2 is that I presume when you develop your policies and your approaches to things you are basing that on the lessons you have learnt from before. Even though by Monday you will be housed in a different organisation, you are basing it on stuff that has gone before, which largely, surely, has been offline thinking to deal with offline problems. So are organisations like yours capable of technologically staying ahead of, or even abreast of the game? How do you online your precedent, I suppose, so that you can deal with the online?

Mr Pilgrim—I would like to think that our organisation is doing as best it can, for a small organisation, to keep abreast of what is happening online.

CHAIR—Of course, but let us be realistic—can you or anyone else cut the mustard? I do not mean that in a threatening way. If at the end of the day we are on a useless quest in attempting to ensure privacy, it is organisations are like yours that will start to recognise those signals before the policymakers perhaps.

Mr Pilgrim—First of all, I would certainly say I do not think it is a useless quest. I think it is extraordinarily important that we need to ensure that, to the greatest extent possible, people are given choice around how their personal information is used, handled and protected. That goes to the very core of us all as individuals and our dignity as an individual. I think it is incumbent upon us, governments, parliaments to ensure that those rights for the community are maintained, but also are maintained in a way that is relevant and maintained in a way that the regulatory model that is trying to do that job is kept relevant. The current reforms that are going on in terms of reviewing the Privacy Act are a case in point.

The review was undertaken following a recommendation of our office that there needed to be a wholesale review—I am sorry, I might be getting off your point a bit—to make sure it was maintaining its relevance in the 21st century so that these protections can do the job they were meant to do, hence my comment about having technological neutrality and also keeping principles based legislation, but with mechanisms to allow us to recognise things like technologies where you may need to have more specificity in terms of regulation. I think we should all admit that this is challenge and it is hard to keep abreast, but I think it is incumbent upon us and everyone involved in it to do the best we can to keep abreast of that so that we can help the community maintain its control around its personal information. We have policy sections within our office who continually do research to try and keep abreast of that to the best we can.

CHAIR—A final question on culture: have we shifted so much that we have sacrificed our right as individuals to expect privacy? We want access to everything, we want everything to be open to us, yet we want some of our information to remain private. We have to balance the tensions—for example, public safety, et cetera. In terms of culture, have we sacrificed or should we be accepting that we have sacrificed, more than in the past, our right to expect personal stuff to be private?

Mr Pilgrim—It is an interesting exercise to look at what has been happening over recent years in terms of that issue. Some commentators have said, 'Privacy is dead now the internet is here—get over it,' yet we see the issue coming up time and time again. We saw what happened

recently when Facebook tried to change some of its privacy settings. We saw the repercussions and the statements made by the founder about his views on privacy. I think that shows recognition that there is an issue out there for the broader community and there is a threat to organisations which are seen not to be trusting people's personal information. I also accept that I do see on a daily basis the issue that people are wanting to maintain their privacy, yet they may get frustrated when they go to get a government service and say, 'Why don't you know that about me? Why do I have to constantly keep giving you that information?' When those two messages come at the same time, it seems to be a very odd scenario.

I would suggest that the fundamental one we see constantly coming back is people's discomfort, when they find out that their information has been used in ways they are not used to or they were not expecting. They start to get nervous. It is an interesting psychological exercise to start to work out why, on the one hand, we are naturally nervous and worried about this, yet, on the other hand, we may be seen to do something like put a lot of our personal life out on Facebook.

It seems to be a very interesting issue. I would also say that from our perspective we need to recognise in the democracy we live in that privacy cannot be an absolute. We live in a community and there needs to be a balance. You touched on law enforcement. We all expect to have safety and we need to recognise that there needs to be a free flow of information in certain circumstances to allow that to happen.

CHAIR—Thank you very much Mr Pilgrim and Ms Falk.

[10.38 am]

McCLELLAN, Mr Scott, Chief Executive Officer, Australian Association of National Advertisers

CHAIR—Welcome. Were you in the room earlier when I went through the formal palaver?

Mr McClellan—I was, yes.

CHAIR—We have your submission. Do you need to amend it in any way?

Mr McClellan—No.

CHAIR—How about a short opening statement then?

Mr McClellan—I would be pleased to give a short opening statement. Thank you for the opportunity. AANA appreciates the opportunity to appear before the committee on the important issue of online privacy. We represent common interests and obligations of companies across all business sectors involved in the advertising, marketing and media industry. This industry contributes approximately $30 billion to the Australian economy each year.

AANA also serves to protect the rights of consumers in ensuring that advertising and marketing communications are conducted responsibly. We develop and administer industry codes of practice and the self-regulatory system generally, including the complaints handling system delivered through the Advertising Standards Bureau and board. This system acknowledges advertisers' responsibility, while allowing industry to respond to consumers quickly and effectively through this complaints handling service.

A key benefit of this system is its ability to respond and adapt to evolving technology and changes in the way consumers access the media, both online and in the traditional sense. The AANA Code of Ethics, for example, is the overarching code for all Australian advertisers. It has the objective of ensuring that all advertising is ethical, and prepared with a proper sense of obligation to consumers and fairness to competitors. Underneath that code sit several others; in particular, I would mention the code for marketing communications to children, where privacy is referenced more directly. The World Federation of Advertisers has published global standards for online advertising; AANA contributed to this document and has urged its member advertisers and the advertising community generally to follow these standards. I have brought a copy of them with me and am happy to refer to them as we go along this morning.

AANA emphasises the important role of consumer education in this space—particularly of young people, who may be less aware of the risks associated with publishing information about themselves online or just surfing the web. AANA is working on a public education program based on a successful initiative of the World Federation of Advertisers.

CHAIR—Mr McClellan, if you have only got one copy of those standards, would you mind allowing us to take a copy whilst you are continuing with your statement? It might assist the committee.

Mr McClellan—Sure. As I said, we are working on a public education program based on a successful initiative of the WFA. The program will include development of tools to help educators, particularly teachers of younger children, to better understand advertising generally, including in the online environment. We began to discuss this program with various stakeholders recently and the interest level that we have experienced already has been quite high, so I am quite enthusiastic about pushing on with that.

I will conclude my opening remarks there and invite you to ask me some questions if you want. I would just emphasise that I am not an advertiser by training or background, so technical questions on issues like interest based advertising I might take on notice and get back to you on, but I will do my best to answer.

CHAIR—We will see how we go. We will kick off questions with Senator Ludlam.

Senator LUDLAM—Thanks very much for coming in this morning. You mentioned, I think, in your opening statement—and it is pretty clear from your submission as well—that you prefer a model of self-regulation rather than having legislators intruding on what is going on at the moment. Do you want to maybe just offer a bit more detail on why you think that is appropriate?

Mr McClellan—Our default setting as national advertisers with national brands to protect and promote is to take responsibility for those brands and the promotion of them in all respects. Our codes deal with the kinds of issues that consumers tend to complain about—issues like vilification on the basis of race, ethnicity and that sort of thing; the way sex and sexuality is treated in the media; the use of coarse language and so on. In fact, when complaints come they are very often framed in the context of a privacy concern—people feel offended; people feel that their personal privacy somehow has been offended by the matter, especially if the communication vehicle that has been used is a direct communication vehicle such as an online one.

So our concern is to ensure that we accept, as national advertisers, our responsibilities in this regard, but we also take some comfort, I think, in the fact that there is, in the privacy space at least, a legal framework underpinning what we do. I note, in particular, that there is provision in the national privacy framework for industry codes. A couple of industries have implemented privacy codes—perhaps not as many as might have been expected 10 years ago or so when this legislation was working its way through. I think it would be an interesting thing to look at whether—in the context of reviewing privacy legislation and its provision for sectoral codes, as Timothy Pilgrim alluded to just a moment ago—there may be scope for more work in this area, to address the nuances of particular industry sectors and how they go to market.

Senator LUDLAM—My question was not so much about the content of the advertising and whether it is vilification or whatever it might be, because we do have in the offline world a reasonably consistent set of standards and complaint mechanisms. It was more about the technologies that are changing very quickly for tracking people's movements online and increasingly, through the use of locative technologies, offline as well—for example, our phones

know where we are at any given time. We are seeing interesting and potentially quite invasive technologies that will target messages to us depending on what the software aggregation of our various emails and activities online think we are interested in. My question goes more specifically not so much to the messages that are delivered but to the ways in which people are now being tracked and how commercially valuable that information is. Do you think there is a role in some instances for either enforceable codes or direct legislative intervention if people's privacy is being abused?

Mr McClellan—I think there is greater clarity needed in these areas. There is experience of this already, for example, in the biometrics sector. That is a sector I have direct knowledge of because I authored the biometrics privacy code which actually introduced new principles around the protection of personal information, the control over that personal information and handing some measure of control back to the data subject, as we tend to describe them, and introducing an accountability principle. The reason I mention this is that there is precedent here for an industry sector actually taking existing privacy standards and building upon them and having those proved standards authorised by the Privacy Commissioner and given the effect of law. Although biometric technology is only just gradually being introduced, it has privacy advantages built into it but also privacy risks built into it. You have in that sector the example of an industry that has looked quite carefully at the implications of what it is doing and is trying to rebuild trust with end users, the consumers who have to interact with the technology. I think that is exemplary. It is a good example of how the private sector can respond to genuine community concern.

Senator LUDLAM—Your point of view would still be that self-regulation is the most appropriate way to regulate online privacy because the technologies are moving so quickly, but there are still fairly regular reports of websites and services breaching their own privacy policies either through deliberately pushing the boundaries or through the stuff that has been in the press recently about Telstra, who inadvertently sprayed the entire contents of their database to the wrong addresses. What is your view of the approach taken in other jurisdictions—and one that we are aware of is in New York—of holding advertisers accountable for purchasing information from websites which they know are breaching their privacy obligations—that is, importing data sets from others whose standards may be lax?

Mr McClellan—The key word in your question is 'know', that the advertiser purportedly knew that a supplier was behaving in a way that was in conflict with accepted law. I would venture that national brands and national advertisers would be very concerned about what their customers feel about their behaviour, not just in privacy but across everything that they do.

One of the issues that we are observing in the advertising industry is how quickly bad news about your brand can now spread. Bad news can go viral almost instantaneously and can rapidly get out of the control of those who in the past felt they were in a position to protect and promote the brand. I think a lot of national advertisers and national and international brands feel very vulnerable. That is actually an important governing factor as to their conduct and the conduct of the people working for them. There will always be human error. That is a fact of life. It puts a strong emphasis on the need to properly train staff and make them aware of the company's values and also the laws that the company and the brands are bound by.

That set of principles I alluded to a moment ago puts education right at the very top of the list. It is not just education of consumers but education of businesses and the people working for businesses. There is a lot of learning to be done by a lot of people at the moment. It would be fair to say that my members have been traditionally focused on using the many broadcast forms of the media to get their brand messages across to consumers and they are still predominantly doing that. But it is significant that internet based advertising has just crested the $2 billion mark in terms of advertising spend. It is now challenging free-to-air television in terms of the actual media spend here in Australia. That is getting a lot of people's attention in the industry. There is a growing awareness that advertisers need to be fully conversant with the tools that are being used on their behalf to get their brand messages to consumers.

Senator LUDLAM—I appreciate your point about the public backlash being the key feedback mechanism. I think that is quite perceptive and helpful. But to succeed in the online advertising space it seems as though the cutting edge tools and techniques are mostly based on hoovering up as much information as you can, but you are not broadcasting; you are quite tightly narrow-casting to an audience of one if necessary. I presume you are not suggesting that the only boundaries on behaviour as to this are a kind of testing of the public's willingness to have these technologies invisibly surrounding us and that a public backlash is what guides the industry as to what is acceptable behaviour in the absence of enforceable codes or due to the lag as to how parliament can respond given how fast-moving some of these technologies are.

Mr McClellan—There does not need to be a widespread public backlash. It can be a single event that has a very high profile. International brands, being inherently recognisable, when they are attacked make a lot of noise across all media and incur damage as a result of that. The point I am making is that, in terms of mitigating any behaviour that they may be tempted to engage in, that may not be consistent with good information-handling practices. It is a strong factor in mitigating that behaviour. My point is a single event can trigger a lot of brand damage, so that is, I think, keeping advertisers on the right side of an invisible line in this area.

Senator LUDLAM—Interesting, thank you.

CHAIR—Mr McClellan, in terms of your answer to Senator Ludlam and talking about self-regulation, given that is by definition limited in enforcement capability, what is the shelf life of your attempts to self-regulate? That is presuming they do not have a happy end. Perhaps your self-regulation may well go on a happy journey, but if it were not to how long should your organisation members ought to have to demonstrate that self-regulation can work before policymakers might think about jumping in, loath as we are—on the Liberal side anyway.

Mr McClellan—We like to think of codes and self-regulation as living documents and an ongoing process. In fact, the AANA code of ethics, which as I said a moment ago is the overarching set of principles that guide behaviour in the industry, is currently under review. We have had more than 50 written submissions to the review. We have undertaken about 25 face-to-face contacts with key stakeholders as part of an exercise in bringing a 12-year-old document back up to date. We did not have clear evidence that it was dated or broken in any substantive way. On the contrary, it seems, by the level of complaint activity that the Advertising Standards Bureau is dealing with, to be quite an active and involving code. Consumers are interacting with it. They are getting about 3,000 to 5,000 complaints a year under the code.

However, it is important to recognise that when the code was developed, the internet was not a factor as a medium to reach consumers 12 years ago—it was in its infancy—and now it is. We want the code to be relevant for the next five to 10 years. One of the key elements of it, and I refer again back to Timothy Pilgrim's comments about technological neutralities—it is difficult to roll off the tongue—one of the strengths of this code is that it does not try to address particular technologies or particular media, but addresses the use of the media generally. There was an interesting question earlier about whether you could think about traditional media and online media in similar ways.

CHAIR—So are you capable, are your members capable? And on what basis would you claim so?

Mr McClellan—I think they are. I would come down on the side that experience in dealing through traditional media is relevant, but at the same time there is a lot being learnt about how to apply good marketing principles in the online space. We mentioned in our submission that there is a revolution going on in our industry. In the good old days it was a one-to-many broadcasting paradigm, and now it is really many-to-one. It is many brands trying to reach the individual consumer and competing through a narrow pipeline of the internet, in this case, to reach them. That is causing a lot of rethinking about how that is done.

Advertisers are experimenting with this, sometimes at their peril, when they try to introduce themselves into a social media forum where people inside the forum are exchanging views on that advertiser's brands. Of course it is very tempting to get involved in that discussion, but how do you get invited in? That is the question they are trying to deal with, and industry does not really have an answer to that yet. If you try to force your way in—

CHAIR—You might want to try to get there before the policymakers feel they have to.

Mr McClellan—Exactly, yes. If you try to force your way into that conversation, it can be a very unwelcome intrusion, and we get that. It is interesting that we are having this discussion at this moment because a lot of the questions that are being explored through this debate are also being considered actively by advertisers, and we do not have the answers.

CHAIR—Yes, well we always like to be up with it in the Senate, don't we, colleagues?

Senator CAMERON—How many breaches of these global principles for self-regulation in online behavioural advertising have taken place, both internationally and within Australia?

Mr McClellan—I should clarify that this set of principles is not a code in Australia administered by the AANA as our others codes are. So breaches of these principles would not be recorded, monitored and acted upon in the same way that alleged breaches of our code might be, so there are no statistics that I am aware of.

Senator CAMERON—What is the point of this then?

Mr McClellan—The point of it, in the absence of either a self-regulatory or legislated framework, is to adopt a best practice approach. I think the value of this initiative is that it is an international effort to think about how these questions of transparency, surrendering control and

providing data security can be dealt with by international brands in an online context. To the extent that companies actually adopt and apply these principles you are getting some uniformity in behaviour. I think a question was raised earlier about the lowest common denominator in some countries. These principles, I think, represent very high standards. I think it is possible for us, in applying these principles, to develop more media-specific and sector-specific guidelines that will inform them further and flesh them out in ways that give consumers more comfort and give business more guidance about how they should conduct themselves. That is actually occurring at the moment.

Senator CAMERON—If I was being cynical—

CHAIR—Never!

Senator CAMERON—wouldn't I just say that this was a spin on behalf of advertisers to say that you are doing something when you are not doing anything?

Mr McClellan—You could make that suggestion and advertisers often are in the business of putting a positive spin on a product or service, so that is a logical conclusion for you to draw. I think, however, the reality is that advertisers do see the issues that are coming through in these principles as business or commercial issues—that if they do not get them right it will be commercially damaging for them and their brands in the future. So I would not underestimate the commitment that the private sector has made to apply this kind of thinking not only at the individual business level but also at the industry-sectoral level.

Senator CAMERON—Again, I am not being cynical about this, but as an advertiser you could put this up on your website and say, 'That's it, I have done this.' You could do nothing else about it and the consumer would not know, and it would be business as usual. That is my concern about this.

Mr McClellan—These principles are meaningless if they are not given expression through the corporate values of the organisation or across industry sectors and if they are not backed up by meaningful and more detailed best practice approaches. Ultimately, these initiatives are meaningless unless there is a real spirit of willingness to adhere to them. I come back to the importance of not getting this wrong for the protection of the brand and the ability for consumers to trust brands. Everything, for these companies, relies on that. If we did not have brands, in some ways we would have a bigger problem because you would not have that important limitation on conduct. But because brands are so important to businesses you have that kind of important self-regulation element.

CHAIR—Trust is becoming a familiar thing. We heard it from Google earlier on and now from Mr McClellan.

Senator CAMERON—You say in this that the global principles do not apply to a website's collection of viewing behaviour solely for its own uses. Can you tell me why they should not apply? Please take that on notice, because I do not have time to get the answer now. Then you say the consumer principle calls for mechanisms that will enable users of websites at which data is collected for online behavioural advertising purposes to choose whether data is collected and used or transferred. I am not sure if you were here when I was asking Google, but could you, in

the context of this consumer control principle, give me a view on whether an opt-in approach could be used as opposed to an opt-out approach, and what your view is on the relative merits of opt-in versus opt-out? Could you also give the committee your views on the legislation in New York that holds advertisers accountable for purchasing information from websites when they know they are breaching privacy obligations? Those are the three areas I would like you to give some consideration to and come back to us on.

CHAIR—Thank you, Mr McClellan. Nina will help you if you need some information on how to deal with the questions on notice.

Proceedings suspended from 11.06 am to 11.15 am

LEESONG, Mr Daniel, Chief Executive Officer, The Communications Council

McDONALD, Mr Iain, Board Member, The Communications Council

WOLTERS, Ms Linde, Media and Public Affairs, The Communications Council

CHAIR—Welcome. You all heard the formal stuff earlier on. Is there anything you wish to add about the capacity in which you appear today?

Mr McDonald—I am also the founder of a digital agency in Sydney.

CHAIR—Thank you. We have your submission. Do you need to change it in any way?

Mr Leesong—No, it is as read.

CHAIR—Then how about a quick opening statement please?

Mr Leesong—Thank you for the opportunity to appear before you. We took the approach of taking the chance to inform you of what the industry is doing at a practitioner level. One of the reasons we have Mr McDonald with us today is that he runs one of the most successful digital agencies in Australia and internationally, so as a practitioner he is involved right at the forefront of the latest developments in technology and how, in particular, privacy principles are being implemented on a practical basis.

The Communications Council is a relatively new body. It brings together the old Advertising Federation of Australia, the Account Planning Group, the Australasian Writers and Art Directors Association and, more recently, the Australasian Promotional Marketing Association.

CHAIR—How new is relatively new?

Mr Leesong—It was formed on 1 January this year.

CHAIR—Pretty new.

Mr Leesong—New enough. It represents businesses in the creative industries which together, as a sector, contribute a large portion of dollars to the Australian economy—around $30 billion at last count. There are about 15,000 businesses and about 60,000 employees working within the sector so, in its own right, it is a substantial contributor to the economy.

The council's members hail from different creative disciplines, including traditional advertising agencies, healthcare advertising agencies, design agencies, production companies—really, the full production cycle from brief concept to delivery of the advertising communication.

Our organisation is about helping our members grow their businesses and develop their individual careers, and we provide various educational services, whether digital or ethics related services. We also provide advocacy advice and support. The council has a very important role in

generating social interaction in what is a very traditional industry that is undergoing substantial changes at present.

From the outset, council recognises the importance of its members acting in a legally responsible manner. In fact, the businesses' reputations are derived solely from operating in an ethical manner. To do that our organisation conducts training, through major agencies around Australia on an ongoing basis, in ethics and other relevant socially responsible initiatives that the agencies should be implementing as a matter of course. We also run the industry accreditation program and, as part of the industry's sign-up for accreditation, they sign up to abide by the code of ethics as it stands.

Our industry strongly supports the ongoing use of self-regulatory frameworks as the mechanism for effectively dealing with this area. The theory behind that is more related to the fact that it is changing so rapidly. We can explain later how rapidly it is changing, but literally on a daily basis the techniques and delivery mechanisms are evolving. We believe a regulatory environment capable of keeping up with that is best structured through self-regulatory mechanisms.

In our submission, we highlight the importance of and the focus that we have on the right of agencies and their clients to contact the customers. There needs to be a very strong correlation between what customers and potential customers want and the message that is being delivered by the agencies. In this day and age it is clear, from our perspective, that consumers are demanding a form of tailored communications. It is not acceptable anymore to have a scattergun approach, and this is part of what we believe is the evolution of modern communication methodology. That is a very general outline of what we do and where we stand.

CHAIR—Thank you. To what extent does your membership overlap with that of the Australian Association of National Advertisers?

Mr Leesong—There is quite clear delineation in that we represent the advertising agencies and the AANA represents the advertisers. There is a very small overlap of a couple of members, but broadly we are the people that put the creative concepts together and deliver them.

CHAIR—I presume the national advertisers would not differ with that assessment of your capacity?

Mr Leesong—We would hope not.

CHAIR—Thanks.

Senator LUDLAM—Thanks for joining us this morning. If I had stayed in my previous occupation you would be my rep body, so it is nice to see you here. Can I pick you up on one of the last things that you said—that consumers are demanding tailored advertising and you are responding to that demand. Is that actually true and can that be backed up? I have never specifically asked advertising companies to learn more about me so that they can better target ads, so where is this perception of demand coming from?

Mr Leesong—I can speak broadly. The marketing messages that are put out to the consumers are massaged and developed in a sophisticated way through focus groups and a heap of different research methodologies. It would be fair to say—Iain, correct me if I am wrong—that consumers do have a level of comfort in knowing that the communication is targeted towards their specific interests. If I have an interest in computers, I would much rather be reading about the latest software rather than reading about the latest widget manufacturers.

Senator LUDLAM—It is a general expectation in the industry that it is in the public interest that advertisers know more about us to target their messages better, but it is very strongly in the interests of the industry, obviously. I am much less clear about our understanding of what people actually think.

Mr McDonald—I think we as an agency tend to put consumers first in understanding what they want and how they behave in order to give them the best experience. We will hopefully make them love a brand more. If you look at any website, for instance, no matter whether you are an advertiser or somebody who has a blog, you want to make people like you by serving the best content possible. So we know from all the studies that we have done that more effective advertising leads to greater consumer love or trust for a site, and certainly contextual advertising, from point to view of being relevant, deeply affects the experience around the site. If you go to a technology site, as Daniel said, you tend to want to see advertising around that. We also look at that from the perspective of response. Whenever we run a campaign, we might see that a banner ad is or is not being clicked on et cetera. There is a lot of analysis that goes into looking at not just effectiveness but also how much a consumer has actually enjoyed an experience. It is a very important part of the journey.

Senator LUDLAM—I recognise that the industry is feeling its way a bit, and we heard a little bit this morning about behavioural marketing, which I will ask about in a sec. The offline equivalent would be having an exec from an agency following you around making a note of who you were talking to, what you stopped and looked at and what books you were reading. I do not want somebody following me around in the real world, so what makes you think I am happy to have that occurring online?

Mr McDonald—That would be correct if we could identify who you are, but to a large extent when we are firing behavioural advertising it is just the same as going to a football match and knowing that there are many people there who like sport. We do not target individuals. It is very, very difficult. Even if we wanted to, the data is not there for us to do that. Certainly Google et cetera do a pretty good job of disallowing that type of activity. If I were talking about personal data specifically, I think Facebook would be the biggest concern because we are able to advertise things that you like based on what is in your profile. Then again, you have the freedom of information to turn on what you like and what you do not like. But certainly there is a lot of development in that area and we are very careful around how we use that.

I should point out that there are a lot of benefits to the way that the whole system works. We could look at being able to target ads for specific products that should not be reaching people like minors, for instance. If we want to protect the younger audience, then we are able to use the same systems to make sure that advertising reaches the right audience—the right products that do not offend different people. So you could even look at it from the perspective that the same technology could be used to target people who were in areas prone to bushfires so that they

receive the messaging, as opposed to people who were not in those affected areas. So there is a lot of good that comes out of this technology, and I think as an industry we try to find the best way to utilise those technologies for good—although I am absolutely in agreement that there is the ability for that data to be misused on occasion. But in that instance I would probably argue that it fell into an area where it was more criminal.

Senator LUDLAM—I think you have given us a couple of useful public interest arguments, so I appreciate that, but primarily the research, whether it be on a level of psychology or in data matching or trying to line up personality records or whatever the behavioural marketing technologies might be, is about selling stuff. Despite any collateral public interest benefits like the example you raised around miners—I think that is a really useful one—primarily these technologies are about tracking us so that we can be sold stuff better. So I am not sure that I would agree with your example about the football match. I think we are using techniques that are way, way more sophisticated than that.

Mr McDonald—Yes, certainly they are more sophisticated. I would probably bring in an example of how we have used that within a business and how the business and the economy are changing. This year, we presented for the summit on the future of broadband a case study for Aussie Home Loans, who are a very traditional company, when you think about it, in terms of bricks and mortar and somebody actually sitting down to book an appointment. In that particular instance—I am able to use this instance because it is public knowledge—in the last few years, 78 per cent of all their business has come through digital. So it is not just the fact that they use digital to advertise and try to find people who are interested in their product; it is actually the way that their business has started to work now. The economy relies very heavily on using this technology right to sustain businesses, and that is just one example of many that I could probably use if you want me to go into more detail.

Senator LUDLAM—I might, but I will cede the floor for the time being and come back later if there is time. Thanks.

Senator CAMERON—Thanks, Mr Leesong and Mr McDonald. I would be much more confident in what you are saying if some of your members were not engaged in things like the sexualisation of children. There has been a lot of critique on that, and you say in your submission:

> In considering any reforms the Council therefore would state that the right of agencies and their clients to contact consumers is paramount and should be preserved.

It is a pretty strong statement. Why should your rights as a business be paramount over the rights of individuals to privacy?

Mr Leesong—I do not believe we were referring to denigrating the rights of individuals, but what we were pointing out by that statement is that the commercial world, business, in its fundamental nature is reliant upon being able to communicate to an audience. All through history, whether it is more traditional forms of media or now, that has been the fundamental way that the economy ticks over and those sales are made. It is not saying that is no need for protection mechanisms and doing the right thing. We are not shying away from that. In fact, when you look at the sexualisation of children, there have been things that come up, but the

industry has been very proactive in addressing those concerns. We would put our hand on our heart and say that our members are very conscious of that and do everything they can in a broad sense to make sure that we are not sexualising children. It is something we believe very strongly in.

Mr McDonald—I think on that, as well, it is very important to the industry that those opt-in examples that you spoke about earlier in terms of communication one to one are very important. Probably the main peer-to-peer communications that take place are under email. They are under very strict guidelines, which we all follow pretty rigorously. On the broader platform of social networking: brands tend to use social networking for one-to-one communications to address things like dissatisfaction around a product or dealing with misinformation. P&O Cruises last year very effectively handled the swine flu crisis on board its ship by engaging very personally with consumers on a one-to-one basis inside channels like YouTube. I think for the most part, where those interactions happen, it is in a very positive light. What we are trying to work towards is more of that and understanding the pitfalls.

There is no doubt that a lot of brands are making mistakes. The one thing that I personally would bring to your attention—I think it has been raised here—is the lack of education, not just within the industry but within the wider public. It is certainly something the council has really very high on its agenda—better education to people within the industry.

Senator CAMERON—In your correspondence you use the word 'paramount' when you talk about your rights but when you talk about the rights of those who might have a problem you use the words 'reasonable steps', to put that in place. You talk about 'reasonable steps to destroy a penalty, de-identify personal information'. Why is it paramount for your rights but only reasonable for the rights of others, or am I misinterpreting?

Mr McDonald—I would agree with you that it is paramount that data is handled responsibly. For the most part, agencies do not really operate under our own provisions. We are very much bound by legal provisions but more than that by the provisions clients put around us. Again, to use a personal example, one I have been through with Microsoft, being one of the bigger entities out there: when we collect personal information for that particular organisation, for the most part it is supposed to exist on Microsoft servers. Where that is not practical, we undergo very strict security audits and at the end of any given campaign we are asked to hand over a CD of any personal information, to be shown that information has been physically deleted. We know that there are clients who behave very responsibly on that level. I do not think that is consistent across the industry as clients' rules and regulations change. We try to put the best of our experience together with what the client is doing. It is not consistent though.

Senator CAMERON—I put that last question to a previous witness. What is your view of the approach taken in other jurisdictions—an example is New York—of holding advertisers accountable for purchasing information from websites which they know are breaching their privacy obligations? Are there any other methods you think would be effective in curbing this practice?

Mr McDonald—That is a good question. Obviously anything that breaches privacy is an issue. Policing that from here and overseas is clearly an issue. The industry as a whole has a lot of talks with the various bodies. Consumers are very important to us, so working with Facebook

and Google, et cetera, is easy, but when it steps down a level there are a lot of things going on which are invisible to us. Again, I have absolutely no doubt that trading information on a lower level goes on. I do not think that we are in a position to police that as the Communications Council, just to follow best practice to help our members understand how best to avoid that.

CHAIR—Your submission talks about the joint industry initiative you developed last year in establishing standards. How did you do that if you came into existence in January this year?

Mr Leesong—The four component bodies existed in their own right.

CHAIR—Of course they did.

Mr Leesong—So it is part of the amalgamation.

CHAIR—In your submission you talk about a 10 August meeting and the sorts of initiatives including educating the public and convening further meetings to deal with online behaviour or advertising. How have you been progressing and what has happened since? You say you are continuing to discuss and to engage but how are you going with some results?

Mr Leesong—It is fair to say, because the industry has grappled with the exact issues that you are dealing with, it is highly complicated. But that being said, the discussions are continuing. There are a number of complicating factors about ownership of information and different bodies and ISPs interplayed with agencies. It is fair to say at this time that conversations are ongoing and that they are productive conversations.

CHAIR—Yes, of course there are complex and sensitive issues, but the collective industries that you represent are asking the policymakers to leave the regulation in your self-regulatory laps. So that we do not lapse, we would be looking for some reassurance that progress is being made or is going to be made yesterday.

Mr Leesong—Yes. Speaking from the Communications Council's perspective, we are committed to ensuring that progress is made. We can certainly take it on notice and perhaps write to you more formally about progress. It would be under the auspices of that group, not necessarily ourselves.

CHAIR—I see. That would be helpful. You might not want to say who your actual members are, but are providers like Google and Yahoo members of your organisation?

Mr Leesong—No, they are not members. They are certainly companies that we have a lot to do with on a day-to-day basis, but our members consist of companies like M&C Saatchi, Clemenger, Leo Burnett, George Patts. So a number of the larger multinational advertising agencies, and then the smaller and midsize agencies fall under that category as well. On the other side of it, the production side, we have a lot of production members too, who are charged with the writing and direction of producing commercials in all the different mediums.

Senator TROETH—On page 3 of your submission you have discussed various initiatives that attempt to self-regulate the behaviour of advertisers—please let me know if this question has

been asked already—for instance your privacy guidelines and AANA code of ethics. If somebody breaches those, what mechanisms are available to enforce those codes and guidelines?

Mr Leesong—The AANA are probably the best organisation to talk about the specifics. There are unofficial agreements. There are agreements in place where the agencies pull advertisements if they are found to be in breach of the codes. The ASB—the Advertising Standards Bureau—monitors and regulates that. But from an online privacy perspective, we have our guidelines which we teach on a regular basis throughout the nation to the agency practitioners when they are implementing their campaigns. So it is a more practical mechanism rather than a big stick approach.

Senator TROETH—So the industry response to that, if anything was perpetrated by any of your members, would be fairly instant in that they would be asked to explain themselves?

Mr Leesong—Absolutely. A couple of other submitters have mentioned this issue of brand damage, and that is a huge issue. It cannot be understated how important the preservation of the brand is. In fact, if an agency does deliver a poorly executed campaign which is in breach of privacy principles or is pulled up, it can be fatal to that agency's business.

Senator TROETH—Yes, I think we have had a few glaring examples of that in the past few years.

Mr Leesong—Yes.

Senator TROETH—Okay, that is good. I am pleased to hear there is such a responsible attitude.

CHAIR—This is the same question I asked a previous witness: what should be the shelf life on the industry's attempts to self-regulate?

Mr Leesong—It is a bit 'how long is a piece of string'. Self-regulation has been around for a long time. From a regulator's perspective, it is reasonable to expect to see the industry being proactive and keeping its codes up-to-date. It is reasonable to expect the industry to be communicating its activities to people like yourself, to interested parties. I would not want to put a time frame on it, but it would be more 'actions speak louder than words'. If there was a real absence of communications and activities, then I think, quite rightly, the industry would be leaving itself open to being regulated.

CHAIR—Indeed, you would.

Mr McDonald—On that, again, because technology is changing so quickly, as a group we probably do live on the cutting edge of what is going on and what technologies are coming out. We work with technology clients to see some of these things on the road map. We work closely with companies like Gartner and Forrester to be aware of those. I think the landscape for the next five or 10 years is a very scary one for companies to adapt to and the role of the Communications Council in being able to adapt and guide its members and clients and the consumer through those is a very important one. I believe we are in a position to effect change a lot faster than other people, by what we do.

CHAIR—In these circumstances what do you mean by 'scary'?

Mr McDonald—We have not even got to IPTV yet. If you go into JB Hi-Fi or Harvey Norman, you will increasingly see TV that is Wi-Fi enabled, or you can plug an ethernet cord into the back. I am a consumer as well. I would have the same concerns about what that connection is doing. TVs are coming equipped with Skype built in. You can have conferences; you can buy those TVs now. Google TV has just gone live. As an industry we have not got to grips with how in the future we will measure, monitor or ensure the same things that previously, I believe, we have dealt with very well in terms of where we are with the internet now compared to what existed 10 years ago. We have come a long way but we are certainly not at the end of the journey; we are just at the start of it. Location based services are all very new. If I walk into a department store and say on Facebook, 'I am here,' what does that mean? I believe we are discovering as many things as we are actually sorting out. So the ability of the Communications Council to play a proactive role with everybody is an important one.

CHAIR—So you mean 'scary' in the sense of the rapidity with which things are changing and the need for your industry to keep up. To be a step ahead would be good.

Mr McDonald—A step ahead would be good. Again, we have already seen the victims of the digital age, with the entertainment industry losing massive profits through things like piracy. We can be involved in those things, such as what happens to map companies that are superseded by GPS devices. There is a lot going on and all of those things have a lot of consumer involvement. Naturally, advertisers are going to want to be in that space and consumers want better services, and we are developing those with clients. We are not just advertising our products any more; we are starting to work on how businesses actually evolve in a digital space.

CHAIR—Thank you. My final question is: are you seeing examples of any application of what I call offline thinking to online problems in this area?

Mr McDonald—That is a fantastic question—

CHAIR—Oh, thank you. That must be why I have asked you about it. Seriously, then what?

Mr McDonald—It is probably not just an industry problem but a nationwide problem. As consumers change their habits change. But we continually like to put things in boxes and the boxes do not always frame the question well and are not always able to answer the problem correctly. There is a need for more dynamic, out-of-the-box thinking about some of these problems, and not just online but thinking about privacy. Clearly, it does not work when you apply it to Facebook.

CHAIR—If other examples come to mind after your appearance today, please feel free to provide them on notice.

Senator LUDLAM—Maybe this is on notice, or maybe you are going to have to point me to somebody's PhD thesis. One instance that has been raised with us of the online and offline worlds bleeding into each other is with new techniques of locative marketing, where you start to become a very important ingredient of what can be targeted at you in a communications sense. Can you tell us what is on the horizon from your industry's point of view. Some of the stuff is

quite fascinating—it is not all necessarily bad news—but what should we be looking for over the horizon? From the communications industry's point of view, what can you see coming down the pipeline?

Mr McDonald—Obviously location based devices will be emerging—phones being able to state our locations to us. Again, it is important to split out that the location based services are both push and pull. If you have subscribed to a service like Foursquare, it allows you to broadcast to your social network where you are—Facebook does the same now. The advertising model on Foursquare is to give local deals. Interestingly, the take-up around Foursquare has been very much around small businesses and coffee shops. One of the things that we are increasingly seeing is that advertisers and especially small businesses are able to advertise without the need for an agency, which is obviously a good thing for the economy and for small businesses to survive. They can put their ads on Facebook. Obviously with location based services for the consumer it is incredibly important to be relevant. If I am in a shopping centre—I think it is great to use shopping centres as an example—and I am shopping for the best deal, advertisers are in a situation where those types of services can enable their products to be found and the consumers at that point are given more choice. There are a lot of positive things.

In terms of tracking and tracing, it is really not something where the agencies themselves have that data. That data is held by the social networks or maybe by the manufacturers themselves. To my knowledge, we have not seen the opportunity to use specific data other than targeted to a location, not a person.

Senator LUDLAM—To be continued, I think.

Mr McDonald—Yes, probably.

Senator LUDLAM—If I become the mayor of Aussies we will see who comes targeting me with advertising.

CHAIR—Thank you very much for your evidence.

[11.57 am]

CORBIN, Ms Teresa, Chief Executive Officer, Australian Communications Consumer Action Network

CHAIR—Welcome. I believe you have appeared before committees of this ilk before, so you are familiar with the ground rules and I will spare from everyone having to hear them again. Do you wish to amend your submission in any way?

Ms Corbin—No.

CHAIR—I invite you to make a brief opening statement.

Ms Corbin—Our submission is based around some research that we recently published. It was actually published after we made our submission, but we highlighted that it was going to be published, so I have brought hard copies with me. Some of you may already have hard copies, but I thought it was worthwhile to bring them along.

CHAIR—We will distribute those now.

Ms Corbin—In addition to that, I want to point out that we have put out a tip sheet for consumers. This research report was prepared as part of our grants program. The University of New South Wales Cyberspace Law and Policy Centre put a grant application in to consider the question of privacy complaints and the paths that consumers took to resolve those complaints. This report was coming out at the same time as this inquiry was convened and we felt that this information was relevant to your consideration, even though it does not go directly and specifically just to online privacy complaints.

I also want to note that previously we made a submission to and an appearance at the inquiry into cybersafety. There were some elements of that submission that may also be relevant, specifically in relation to young consumers and what might assist there as far as protection goes. But, of course, that related to cybersafety overall, not just the privacy element.

CHAIR—To the extent that that is applicable, you might apply your mind to that and then direct those specific elements to this committee. That way you will not have to recreate the wheel. You know what you have said. That would be appropriate, I think, and helpful.

Ms Corbin—Thank you for that. We will. Our opening statements are about what the main elements of this review are. There are three different agencies that handle privacy complaints for consumers. Depending on which agency you go with, you could actually get quite different outcomes. Also, what we have realised is that there is a quite significant quantitative difference in the number of complaints that go to the different agencies. Some of those are the result of legislation but some of them are perhaps a result of consumer awareness and possibly even delays that are evident. We have also wanted to make sure that we make a submission to this inquiry because we are very concerned about privacy. Our membership, and consumers in Australia generally, highlight that they are very concerned about privacy issues overall,

especially given the greater reliance upon communications technology and also so by companies who collect our personal data on technology that includes access to cloud applications and databases that are perhaps increasingly collecting more and more information with a potential for harm and for mistakes to happen increasing in magnitude as a result. Obviously, our members are also concerned about social networking and the future use of location based information—and of course spam never goes away as a concern, and I do not think I will be the only one that mentions that in this inquiry.

CHAIR—It never goes away; full stop!

Ms Corbin—That is right. All of these things obviously reinforce the need to have robust systems in place when we are handing over our personal data. There is this week's example of Telstra's privacy breach of a magnitude of 220,000 customers' details being given to the wrong customer—and 23,500 of those numbers were silent numbers—and the fact that Telstra really had to rush behind the eight ball to catch up and make sure that they actually had the right strategies in place to deal with that breach. We assisted them with that because we were very concerned about any potential damage to those silent-number holders but, to be perfectly frank, I think that this has highlighted some inadequacies in the risk-management plan that Telstra had in place and potentially in the risk management plans that other companies also have in place.

So what did the analysis of the data for complaints handling in this privacy space reveal? The ACMA deals with general privacy complaints, spam privacy complaints and 'do not call' register privacy complaints. In all that amounts to 16,000 complaints in the previous year when they collated the data. Twelve thousand of those 16,000 are actually 'do not call' register complaints. The Office of the Privacy Commissioner deals with a thousand complaints, and 110 of those are specifically related to privacy and communications complaints. The Telecommunications Industry Ombudsman deals with nearly 5,000 complaints. But what we also found was that the ACMA deals with these complaints in 30 days, in the Office of the Privacy Commissioner the information commissioner takes six months on average and the Telecommunications Industry Ombudsman takes only 10 days. Also, we found that each agency has a very different approach, and this relates to their powers. In that time the ACMA made eight enforceable undertakings for telemarketers, two about spam, gave 22 formal warnings—and some of those were paid infringement notices—and also they publicly named all companies subject to enforcement. The Telecommunications Industry Ombudsman awarded financial compensation, ordered corrections and made sure that service providers took restorative action where it was required. Also they published a list. On the other hand, the Privacy Commissioner elicited apologies and corrections, and during that time they did not make any determinations. Whilst they have the ability to, as we believe, they did not do any naming or shaming.

To us this reveals quite an inconsistency in the length of time it takes to get a complaint done and the amount of complaints that are going to the different agencies. I think there is probably a much greater in-depth analysis that could be had to establish the reasons as why that is occurring. Some of it possibly relates to the resources put into consumer awareness, and I think that would be separate information that possibly might be able to be acquired. Also it possibly relates to how much resources are put into processing those complaints once they are received.

I think it is also important to acknowledge that all these agencies have very different ways of approaching these complaints. For example, one of the reasons the Privacy Commissioner takes

longer to deal with these complaints is that they conduct an investigation and conciliation. That is a very different process to an investigation and then making a decision awarding an outcome, which is what the ACMA and the TIO both do, because their powers allow it.

The other thing that is very difficult for us to assess are the types of consumers that are actually going to these different agencies. There is not a lot of information captured about the profile of the complainants. There is a big debate about whether to do that in the privacy space, in fact, as you could understand. We would like to see all the different privacy agencies have the same kinds of powers. They should all be able to give compensation to individuals, ensure an apology occurs, ensure that there is prompt action or removal of personal data or a prompt correction if there are any changes to business practices at individual company levels or a broader industry practice for a systemic issue, and occasional naming of individual companies and occasional enforcement action to ensure that we promote a culture of compliance.

The other thing that is important that we have highlighted through this research is that there needs to be better coordination between the agencies. We have contacted all of them, and the Ombudsman, the chair of ACMA and the new Privacy Commissioner have agreed to sit down with us and work towards better coordination, more consistent information and clear information for consumers. Without having to wait for that date to happen, given that we had a massive privacy breach just this week, two of those agencies worked very effectively together by putting out a joint statement. We were very pleased about that because that just showed that they were actually listening to our concerns. I think that is about all I have to say for an opening statement.

CHAIR—Thanks, Ms Corbin. I will kick off. You have talked about the resolution of complaints. Speaking generally, do online complaints take longer to resolve than traditional offline complaints?

Ms Corbin—Based on the granularity of the information I have, the only ones—

CHAIR—Sorry, what did you say? Granularity?

Ms Corbin—The specificity of which kinds of complaints are being dealt with. I only have general complaints—'do not call' and spam. A couple of the spam complaints go to the TIO but pretty much all of them go to the ACMA, and they are resolved within 30 days. That is a very short time frame. The reality is that, if you actually did look into privacy breaches that are online, it is probably highly likely that a lot of consumers are not fully aware that there has been a privacy breach or in fact that they have not set all the right settings to ensure that they have protected their privacy. I am sure I am not the only witness who has said that this is a very difficult area for consumers to get their head around, because every social networking site is slightly different and the information is changing all the time to try to keep up with the new technologies. I guess my answer is that I do not have that information, but it would be useful to explore that with those three agencies to find out a bit more.

CHAIR—Just from what you have said it is pretty clear that we are in a novel area of enforcement, at the very least. There is no use having rules if at the end of the day you have not got a way to enforce them when necessary. The sort of resources that taxpayers would have to contemplate if we want to deliver on that as policy makers are sounding, from what you have said, as though they have would be far more significant with online than offline.

Ms Corbin—There is no doubt that the place we have to start from is better consumer awareness, but I think we also have to make sure—and this is going to be an ongoing battle—that the actual service providers, both those that develop software and new equipment and those that provide network services and all the different elements of service provision in an online environment, have privacy at the forefront of their minds.

It is very interesting to consider the submission by the Australian Privacy Foundation, who talk about how you make sure that consent is actually the most important thing when you are developing anything new. They talk about how you change the culture to focus on consent being paramount, so that you are not forced into accepting an agreement that waives your privacy before you can use a service which may in some instances be an essential service for you. So I think that ultimately we do need to have strict regulation about consent and we do need to make sure that we have the occasional enforcement action that actually demonstrates that this is of high importance to Australians and to the government. I do agree that rule-making is not an easy thing when we are talking about the future of technology and where it is going to go, and I guess that is why we should focus more on the principles and make sure that we have built in some protection around the principles.

CHAIR—Indeed. I have a final area I want to ask about before I swing to others. There was recently an article in the *Age* talking about an industry springing up to protect the identity of the proprietors of dubious websites online. So whilst this inquiry primarily looks at protecting the privacy of private citizens who utilise the net, it would seem that there is a service industry built up to protect the privacy of bodies that are intent on doing less than good. Do you have a view on that?

Ms Corbin—I have not read that article but I am not surprised about that line being considered because the truth is that we have talked quite a lot of times about privacy protection having those unintended consequences. I think ultimately we do have to consider law enforcement, which comes into this equation, how much harm is involved and whether there are any laws being broken. In the construction of any regulation we would have to make sure there are some caveats to ensure that law enforcement agencies still have the powers they need in any circumstances where harm might be done to an individual, regardless of privacy.

CHAIR—Yes, so that, in attempting to protect the well-meaning majority, we do not unintentionally give some protection to the would-be rogues.

Ms Corbin—True. It is not an easy path to travel, but by far and away we have to talk about protecting the privacy of a very large number of Australians, first and foremost, before we talk about those other unintended consequences, which I believe can be dealt with through mechanisms that law enforcement agencies would no doubt advise you better on.

CHAIR—Thank you. Senator Ludlam.

Senator LUDLAM—Thank you for coming in, Ms Corbin and for providing us with another copy of the privacy report. It is good to have some data at hand. Congratulations on your appointment.

Ms Corbin—Thank you.

Senator LUDLAM—There have been quite a few media reports about sites and online service providers collecting personal data without the knowledge or consent of individual users, and particularly this idea of the tick-a-box: 'I accept' whatever it was that might have been written in the 20 pages of privacy waivers. Should we just get better at reading that material, or is there some need for reform at least in that area and also to stop lawyers writing that stuff and maybe get some of it written in plain English for people?

Ms Corbin—That is a very good point. We did raise that in our previous submission on cybersafety as well. There are a number of elements to answering that question. First and foremost, we believe that you should not have to opt out. It should be an opt-in scenario when it comes to waiving any right to privacy or anything in relation to your privacy protection. So in that respect you do not need the long agreement. That immediately makes the long agreement null and void—you do not need it.

Information that we have collected previously shows that even those consumers who actually do read through the long agreements do not understand them. In fact, I spent a bit of time reading through the iTunes one, and 70 pages later I think I had lost where I was up to, so that what mattered to me five minutes earlier did not matter to me at the end. In the end people really want to use the services, so they are faced with the decision of whether to use the service or to waive a right, and in most instances they do not understand the legalese that they are waiving their right to. So it is ultimately a waste of time to have these agreements.

Senator LUDLAM—They are not designed to be read; they are designed to anaesthetise you to the point where you just find the bottom of them and tick it.

Ms Corbin—That is exactly right. Most consumers tell us that they do not read them and that they just tick a box because they want to get on and use the service.

Senator LUDLAM—How much control do we have in Australia over what goes into those kinds of agreements? A good example is iTunes. How much leverage do we have over how those forms are crafted in the first place?

Ms Corbin—There is a lot of discussion about jurisdiction in the privacy space, but I think it is very interesting that some countries seem to be able to quite effectively have higher bars than we do. For example, I was astounded that in Germany everybody had a period of time within which they could opt out of street view with Google before the cameras came rolling down their street. That would have been great in Australia. I think there are a number of people who are still concerned about the rollout of street view even though we also value the service that Google Maps now provides us. It depends on the approach you use to implement new services.

This also relates to location-based services that are going to come into place. Ultimately there will be some great applications that we can use to help us with our accessibility and make things more usable and more user-friendly, but we need to be properly informed before we are coerced into or not given a choice about signing up. This can be done, and it can be done well. The introduction of caller number display in Australia was a good example—there had to be a demonstration by the industry that there was an understanding in the Australian marketplace about what caller number display was. It seems like nothing to us now, but at the time it was a very new technology and it was going to have unintended consequences.

Senator LUDLAM—What about the series of red flag issues that could be identified, probably voluntarily. For example, if I expressly consent to giving up my IP or my ownership of the photos that I upload to whatever site it might be, do we have the ability in Australia, even if these services are hosted overseas, to across-the-board implement that kind of more fine-grained opting in—'OK, I understand that'—those kinds of key issues?

Ms Corbin—I do not have the expertise to answer that question, but I think that we have a couple of examples that might be able to help as far as introducing regulation in the space is concerned. The way that spam was regulated would be one example. When the Spam Act went through, it was well and truly accepted that, because Australia produced something like 0.06 per cent of the world's spam, the Spam Act was not going to have a massive effect on spam generated in Australia. Yet, because the Spam Act had an impact on the internet service providers by drawing them into its regulations and empowering our government to go overseas and work on memorandums of understanding internationally, there has been a reduction in spam and also the ability to regulate spam in Australia. So whilst I do not have the expertise to answer that specific question, I believe that there are mechanisms that could be explored that could innovate in the space and set Australia aside as a world leader.

Senator LUDLAM—I recognise that there are a couple of processes under way which are relevant to this. One is the Joint Select Committee on Cyber-Safety. There is an overarching review going on at the moment and we have exposure drafts of the first batch of amendments to the Privacy Act. One issue that has been raised there and here is the exemption of small businesses. As our previous witness identified, you would not necessarily want to subject a fish and chip shop to the kind of regulatory rigour that you would an ISP. What is the view of ACCAN on the exemptions of small businesses and, indeed, individuals from provisions of the act?

Ms Corbin—Once again, we do not have a position on that at this stage, and that is probably more than anything else because we are a very new organisation. I would be happy to take that one on board and get back to you about a position in relation to it. I know that previously consumer organisations have expressed that the definition of a small business may have been too broad still, and that in fact there do still need to be some requirements on small businesses. Understandably, the harm that a small business may potentially cause to a group of consumers may not be as large as perhaps that caused by an organisation that has a million customers, but I think that they definitely should not be excluded without some good public debate and discussion.

As to individuals, once again I think that is a very different discussion. I do understand that, given that we are talking about social networking and a lot more user generated content, there is clearly a need to make sure that consumers are generally aware of the information they publish, and what they disclose about others as well. I do not know that that should be regulated, but I do think that people should be made more aware.

Senator LUDLAM—I think this issue is going to come up again and again. The Privacy Commissioner drew our attention to the fact that it is not all or nothing for small business, and that you certainly should not just depend on the number of employees as some of the marketing companies are tiny but still hold enormous clout in the information space.

Ms Corbin—That is right.

Senator LUDLAM—The Privacy Commissioner can rule a particular business or class of business in or out—can rule whether they are caught by the act or not. So I guess what we need to focus on is that threshold question of who matters, for the purposes of this discussion. But any light that you could shed on that question I think would be really helpful.

Ms Corbin—How much impact it has obviously does not necessarily just relate to how many customers it has but also how much impact any particular initiative may have on any one customer.

Senator LUDLAM—All right. Thanks very much for coming in and providing us with, finally, some hard numbers on the complaints.

Senator CAMERON—Ms Corbin, I am interested in your recommendation 3 which is to do with demographic profiles. I have just done a quick assessment and there are something like 400,000 complaints to the Telecommunications Industry Ombudsman, in round figures; on the internet it is about 100,000. You talk about the demographics of that. Has any analysis been done? Have you any idea of whether this is a problem for working-class people, who are just really battling in terms of paying?

Ms Corbin—There is a bit of a move from the consumer movement at the moment to get complaint-handling agencies to collect more demographic profile information—not necessarily from every consumer who goes to them but from a sample, for example—so that we actually do know whether there are specific groups that are more vulnerable or more disadvantaged.

So, no, there is not data but only anecdotal evidence. Obviously, those who are most disadvantaged and vulnerable in our community are also going to be most disadvantaged and vulnerable when it comes to privacy, because a lot of the privacy protection—not waiving rights—revolves around people having high levels of literacy. Clearly, in some of those vulnerable and disadvantaged groups they may well still be using plenty of online services but not necessarily reading everything that goes across the screen. It could well be that they are just using lots of other cues—for example, icons, pictures and video. So, yes, it is a concern and something that we need to do some more work on.

Senator CAMERON—Many of your recommendations go to dealing with the issues of how to handle complaints—not all of them, but a lot of them. The evidence that we have had is that self-regulation is the way to go. What is your comment on that?

Ms Corbin—This fits in with our general approach in relation to self-regulation and that is that, whilst we are happy for the industry to take initiatives and develop codes of practice that lift the bar and provide a model of best practice, we really do think that self-regulation has to be underpinned by a good regulatory framework in the first place, with the regulator having the ability to take strong enforcement action—not constantly, but when needed—and the power to do so when needed.

We do not necessarily think that that regulation has to be very prescriptive or long, but we do think it has to be outcomes focused and needs to make sure that the actual principle that we are

trying to achieve, of consumer protection, is at the core of it. Anything that is an add-on to that we are well and truly happy to hear about and to assist industry to implement. There are some examples of those sorts of things, but we do not think that the safety net should be handed over to a self-regulatory mechanism.

Senator TROETH—Going on with the question of the complaints I, like you, was horrified at the very lengthy nature of the resolution of the OPI. Without asking you to speculate in any way, they advised us at the start of their proceedings that, as from next Monday, they are combining with a new statutory agency, the Office of the Australian information Commissioner. Obviously, this has the capacity to make things a lot better, but it may have the capacity to make things a lot worse. How do you view this development?

Ms Corbin—We are hoping it as an opportunity to improve the situation. That is how we have approached the Privacy Commission, although they obviously were not too pleased about our report. We have suggested that, in our dialogue from now on, we actually focus on: why is this the case, how can it be improved? Also, perhaps it cannot be taken to be exactly the same as the TIO or the ACMA, but how can we actually reduce that time? Or do we need to get more resources to that body? Maybe the new resources that are available because of the information commission will assist there. We also think that if they were perhaps a little bit more informative towards those who are keenly watching and interested—like the consumer, and I am sure the government in different capacities as well—in the investigations that they are undertaking on a proactive level and how they are handling it, say, perhaps publishing their decisions, not necessarily identifying who the complainants are but providing examples, then there would be a better awareness of why it takes longer to get an apology than to trigger that enforcement notice. I think there is room for some further explanation from the Privacy Commissioner, but I think there is also some room for improvement, even within the existing powers and structure that they have. I cannot comment specifically on the information commission, because I think the proof of the pudding will be in the eating. One thing we have been concerned about is that we do not want the Privacy Commission to be buried inside the information commission. We still want it to be very high profile and for people to know that the Privacy Commission still exists, even though it is a commissioner underneath the new office.

Senator TROETH—You would also hope that, when people do go to them, they would make it very clear that this could be a lengthy process for the reasons that you have mentioned but, at the end of it, while they would never guarantee that there may well be the prospect of an apology et cetera, I do think, like you, that as people go into the process they should be well aware of the length of the process, as compared to some others. You would hope that, as you say, in the new structure that that will happen. A number of submissions discuss the issue of Australian organisations sending data to overseas companies which are not covered by the Privacy Act. Is that a concern to your organisation and, if so, do you have any suggestions as to how that may be dealt with?

Ms Corbin—Absolutely it is a concern. I am amazed that they would not be covered by the Privacy Act, because the company that is doing it is an Australian company or an entity covered by Australian law. So it would seem that, like the telemarketing laws, which capture much of the telemarketing that now happens in Australia, even though it may be sourced from offshore it is still commissioned by an Australian company. So in that way it can be regulated. We do need to think more seriously about how we can address the global context of privacy. Once again, I

would go back to the example of the Spam Act and the fact that, as far as spam regulation is concerned, Australia is considered to be a world leader and that that set off a whole list of agreements and international developments that have definitely assisted. Obviously, they have not made spam go away.

But I think that I would encourage the Australian government to work with other governments around the world to make sure that we do not have any holes, any gaps, in the levels of protection that we need, because everyone in the world deserves the right to privacy. I think that is a basic premise from which to start. I am totally agreeing that it is a massive task. I also think that, as a result of that, it puts the emphasis back on what we can do in Australia to show that we are a world leader or that we can be a world leader but also that we can do it insofar as making sure that our consumers are fully aware and educated. There is a lot of new and innovative work being done, particularly with young consumers, to try and help with that.

Senator TROETH—My second question was about small business. You may have covered this in your discussion with Senator Ludlam, but is it your view that small businesses should be subject to the requirements of the Privacy Act?

Ms Corbin—I did not give a commitment to that because I felt that it was too early in our organisation's history to have a position on that, but I gave an undertaking to take that back on notice. I also said that I think that at the time there were a number of consumer organisations that spoke out and said they felt it was too broad a distinction—I think it is $3 million, or $3 million and less—

Senator TROETH—Yes, that is right.

Ms Corbin—that is considered to be small business—and that that still created too big a gap to go through. I think that warrants a bit more consideration and thought.

Senator TROETH—Thank you very much. Your survey as printed in the submission and in there as well was most helpful, I thought.

CHAIR—Indeed, as has been your evidence today, Ms Corbin. Thank you very much.

[12.32 pm]

ROHAN, Mrs Melina, Director, Corporate and Regulatory Affairs, Australian Direct Marketing Association

CHAIR—Welcome. We have your submission. Do you need to make any changes to it?

Mrs Rohan—No, I do not.

CHAIR—Would you like to make a short opening statement?

Mrs Rohan—Yes, thanks. Thank you very much for inviting ADMA to appear you before you today to discuss our submission and our views on the adequacy of protections for the privacy of Australians online. I will not go through the work that ADMA have done and our central preoccupations except to say that we are the principal industry association representing industry for information based marketing. We have appeared before the committee before, so I will not go through too much more than that.

In terms of this specific inquiry, significant changes in technology and the increase in growth in the digital economy mean that it is not only right that our society should continually assess whether Australia's privacy framework is sufficient for the recent advancements in technology. I am sure you have already heard today that the work to ensure that the Australian privacy legislation is fit for purpose is well underway. This work includes important reforms put forward by Senator Faulkner and, once implemented, should bring Australia's privacy legislation in step with the technological landscape. The inquiry here today underlines the importance of this work, and industry supports the progress of the review.

The Faulkner reforms will continue the principles based technology-neutral privacy legislation. In addition, it is going to recast the tranborder data flow provisions of the existing Privacy Act specifically to focus on transborder data disclosure of personal information. It is also going to increase the importance of binding schemes such as the APEC cross-border data privacy framework, and it is also going to require the federal Office of the Privacy Commissioner to issue some significant amount of guidance and consumer education in relation to developing technology. We note the excellent work that has been done through the APEC Data Privacy Pathfinder project. We have been involved in that project during its maturation. ADMA notes that it is not only consumer support and education that governments should be focusing on; there is also a real need to ensure that business is supported.

Our opening remarks were written before this morning's proceedings, when we have concentrated on small businesses. We want to turn our attention away from the larger companies and look at the smaller companies and see what more can be done to assist small businesses in understanding the need for online privacy protection and the risks associated with holding personal information. It was only last week at one of our council meetings that I met a woman who was just about to lose her business. She has a small nonmember company. The data that she had obtained online and which was held on a server had been hacked into and all the personal information of her customers had been posted on a website in India. It is a personal tragedy for

her to lose her business. There is a lesson to be drawn from that, and that is that more should be done to look at the ways in which government departments, such as CERT Australia, can work with industry associations in their work in promoting privacy within industry, providing resources to industry, raising awareness about the need to protect personal data and putting appropriate mechanisms and privacy protections in place. I look forward to your questions.

CHAIR—We have heard a lot this morning—you just happen to be the very capable rabbit in the spotlight at the moment—about trust: 'Trust us. We're from direct marketing. We're here to help you.' Why should we?

Mrs Rohan—Maybe our industry association is a good example of this. We have been in operation for 44 years. Membership to our organisation is a voluntary thing. I think it demonstrates that industry understands not only the need to be trusted but also, more importantly, that consumers need to trust a company before they can trust them with their personal information and deal with them. ADMA has for a number of years operated a direct marketing code of practice, which includes obligations that go well above the privacy legislation. We do that because we see it is important to protect the marketplace. Savvy companies will always know that—and the Privacy Commissioner talks about this frequently—privacy is good business. That means that, if consumers do not trust you or they are concerned about privacy, they will not deal with you. They will not give you the information and they will move to competitors.

Senator LUDLAM—We have heard quite a bit along those lines from industry folk who have been here today, but I do not understand how that applies to the companies that are doing the data matching, compiling databases and then selling them on to others, none of whom consumers have ever heard of. Google is a household word right around the world and they have a robust privacy policy and can come to a Senate inquiry and tell us about it, but there are companies, who have been in the press recently, who make a living out of collecting, aggregating and then on-selling datasets about people's commercial preferences and so on. That is not a question of trust because we do not know who they are. I can understand how that would apply to a familiar brand, such as if Nike is found abusing our personal information or something like that, but what about when it does not? What about aspects of the industry that do not have a branded face that we can have a consumer backlash against?

Mrs Rohan—There are a few things that need to be taken into consideration in that regard. The first is that, if those companies are dealing with Australians' data in Australia, they are subject to the Privacy Act.

Senator LUDLAM—This data is kind of everywhere and nowhere, though. If I enter my data into a social networking site based in Canada, where is that data located in the cloud? Stuff is not necessarily tied to geography anymore.

Mrs Rohan—Most of our members are Australian companies dealing in Australia with Australian data. We do not represent unnamed social media companies in other jurisdictions in that context. I think that the advice which the Privacy Commissioner gives in those instances, which is that you must read the terms and conditions and you need to make a determination about whether you will trust your data to those social media companies, it is important in that sense.

Senator LUDLAM—And nobody does. Is that just up to us?

Mrs Rohan—I do not know about that. I gave a lecture to some advertising students on Tuesday and I asked for a show of hands: 'Please show me how many of you have a Facebook account.' These were young people in their early 20s, and the teacher's hand did not go up but all of the students put their hands up. Then I asked, 'How many of you are playing games?' and all the hands went down. I was shocked by that result, actually. I thought it was quite interesting. I asked why and they said, 'We read the terms and conditions and we didn't like what we saw, so we don't deal with it and we didn't give our personal information out.' So yes, there are issues. The issues that ACCAN raised of some people not understanding the privacy policies and the readability and the understandability of them are true, but I do not think that should denigrate the fact that a vast amount of the population are alert to potential privacy issues, do read consent notices or privacy notices and do make a choice not to deal in some instances where they have concerns.

Senator LUDLAM—I think some do. I do not want to labour the point, but I would put to you that 99 out of 100 people who sign up to iTunes, or Facebook for that matter, skip right past that legal text. Maybe that serves us right if things are done with our data after that, but I suspect it would be around the one per cent mark who would read through that text and understand it and perhaps have a lawyer sitting next to them to help interpret it.

Mrs Rohan—The first thing I have to say is that Facebook are not ADMA members and we do not represent their interests, nor do we necessarily condone some of their practices. Part of the work that we do is making sure that industry members who self-select to become our members who are interested in privacy and sign up to our guidelines are aware of the Australian Privacy Act. But we cannot speak for every company in all the world in terms of what they do and do not do with privacy. I think it is really important, though—and I made this comment in the opening statement—that the extraterritoriality provisions which have been proposed under the new Australian privacy principles really will extend the power and the reach of the Privacy Act. I think when you look at that in combination with the APEC Data Privacy Pathfinder project, there are some very significant additional protections that go beyond what is in place at the moment.

Senator LUDLAM—This is where, if you disclose information to a third party offshore and they abuse it, you are liable here in Australia. Is that what you mean?

Mrs Rohan—The proposal for the extraterritoriality provisions, as I understand it, is that personal information of Australian citizens and permanent residents will be covered so long as the company has a presence in Australia. So it is a much lower threshold than is currently in place. In addition to that, you can look at the work which is being done by APEC—people who are naturally on the Pacific Rim. If this goes ahead, they will sign up to a base level of privacy principles. It also delivers, as I understand it, an accountability mechanism where there are accountability agents in each country and companies can sign up to this. That therefore allows complaint handling. I think that is quite a revolution in terms of what is around the corner and definitely in terms of the new technological regime.

Senator LUDLAM—Have you got a view on the question that has been raised this morning a fair bit about whether a small business should be in or out of the Privacy Act, or how we distinguish between which individuals and/or businesses should be caught?

Mrs Rohan—Any small business that signs up to being an ADMA member is subject to the ADMA direct marketing code of practice, which includes the national privacy principles as they are currently included in the Privacy Act. That allows an additional level of protection in that context to the extent that people sign up there. But in the broader context it is a broader issue than we would comment on except to say that an on-balance view should be taken. I think the fish and chip shop is a good example. Why should they have that additional burden? But in other examples, yes, they should be brought into—government should at least be giving additional education. This goes back to my point about the woman who was losing her business because of this information security privacy hacking: more can be done to educate small businesses who are holding personal information without necessarily reaching for the black letter law response and that resources should be put in place. Industry associations like ourselves, we do our best and we speak to small businesses that are in the marketing area and we try to reach beyond our membership, but we are an industry association. I think additional resources and focus in that area from government would be extremely helpful.

Senator LUDLAM—That is useful advice. Given the strong focus on self-regulation that you have expressed in your submission, as have other industry players today, what, if any, disciplinary processes exist within ADMA and how often do you breach people or kick people out of the association?

Mrs Rohan—Our code of practice was created in the 1990s. It is overseen by an independent code authority, which is chaired by John TD Wood, who has had a role in SOCAP. We have a number of mechanisms in place, including naming and shaming, issuing apologies, eventual expulsion from our industry association—

Senator LUDLAM—I was not asking about the mechanisms so much as how often have they been used?

Mrs Rohan—People who have complaints made against them are automatically listed in our annual reports as having complaints being listed against them. I have been at ADMA for only 18 months, so I would have to go back and check to see whether we have thrown anybody out. But I understand that naming and shaming through the annual report—we will take a company for a year and include them in the annual report and say, 'There was a problem and a difficulty.'

Senator LUDLAM—I might leave it there, but if you want to provide us with anything on notice about the implementation in practice of the code—we are aware of how easy it is to write things down and get companies to sign on to them, so what I am interested in is how often these things are brought to life and used and brought to bear on particular people who might be in breach of the principles.

Mrs Rohan—Just as an additional aside—I know this is a question on notice—we handled 52 complaints last year and we are well on track to handle more than 100 complaints this year.

Senator LUDLAM—Are things twice as bad this year as they were last year?

Mrs Rohan—No, I just think that we are doing better at raising awareness of the code.

Senator LUDLAM—It is a classic answer!

CHAIR—On the way through to Senator Troeth, Senator Ludlam suggested it is very easy to write things down. I suppose in the confines of this debate, Caroline Overington has apparently written about writing something online, it does not even exist. So when you write online, there are questions about whether it exists at all.

Senator LUDLAM—Tell that to Grog's Gamut.

CHAIR—Exactly!

Senator TROETH—There have been a number of recent media reports suggesting that advertisers are manipulating internet users into providing personal information or allowing cookies through vague and unclear privacy policies, and that was reported in the *Sydney Morning Herald* on 5 October. The Privacy Commissioner made a similar point. Do you have a view on that issue?

Mrs Rohan—I think that articles such as those that appeared in the *Sydney Morning Herald* are very useful in ensuring that consumers have a growing awareness of cookies and what they mean and what they do not mean. I think that industry would support more being done to educate consumers about cookies by providing additional notice and doing those things. I think that kind of covers off your question. I do not know whether I would want to comment on whether people are inappropriately enticing people in—

Senator TROETH—No, I did not want you to comment on that. I think any publicity on that is probably a good idea in that it raises the issue. If you think part of the response to that is educating people, do you think it is necessary to take any legislative measures to ensure that if their data is being used for marketing purposes people can give genuine, informed consent or nonconsent?

Mrs Rohan—In terms of legislation and black letter law, I would generally tend to suggest that maybe there are other approaches that should be considered first. The marketing industry has a very strong track record of arguably successful self-regulation. Some people would argue otherwise. But arguably it has quite a good track record of self-regulation. I think that industry overall would support, particularly from a privacy perspective, more being done in relation to educating consumers around cookies. Certainly that would not be outside the realms of possibility. I do not want to gazump any future questions but, on the question of whether self-regulation has a shelf life, I think the answer is, 'Not necessarily, so long as it is effective.' Self-regulation can be very effective, and I would suggest it should be given a run first. There are a lot of good things that can be done in relation to that.

Senator TROETH—The Privacy Commissioner also made the separate point that it can be possible to identify particular individuals through data about their web-browsing history. What steps do advertisers take to protect individual privacy with respect to collecting, storing and using web-browsing history data?

Mrs Rohan—I think you would have seen from the evidence given by the Communications Council that it is very rare that that would occur. My only observation on it is that as soon as you do start identifying someone through web browsing you would automatically in Australia fall under the Privacy Principles. As a result, you would be subject to those requirements and the 10—soon to be 14—privacy principles that apply. I do not want to gazump any questions, but I am not sure that those types of protections exist in New York and we would not make a comment on what people do in other countries.

CHAIR—In answer to Senator Troeth, you did not refer to organisations that might manipulate the situation so that they extract the data or information on individuals. You used another term and indicated, if I understood correctly, that you did not want to comment on that. Can you comment on the prospect of organisations manipulating or using manipulative behaviour in order to extract information that they want so then they can proceed with their marketing?

Mrs Rohan—The majority of websites have pretty clear privacy statements. In addition to that, they have very clear cookie statements. It is difficult to see how they would be manipulating people in those instances.

CHAIR—Part of the evidence is that the policies are not so clear. Also, what is clear to one person is not clear to another. Previous witnesses have talked about the ability of consumers to understand to varying degrees that which might be clear to others.

Mrs Rohan—I spend a lot of my time helping people when they are setting up websites. I also spend a lot of my time signing up to websites and looking at websites, predominantly with people who are members of our industry, if you think about our membership. I do not see too much evidence of that practice occurring and I see a lot of evidence within industry—in fact, we try to help thousands of marketers a year as they go about trying to create those websites, getting their privacy policy settings right and making sure that those things are in place. So I cannot really comment on deliberate manipulation. The evidence that I see is that they are trying their best to make sure very plain English statements are put in place and that consent—particularly in relation to being able to send emails—is abundantly clear. In those instances we are always encouraging them to comply with or meet best practice.

CHAIR—All right. I am thinking about being convinced, but here is the same question in another way. Settle, Senator Cameron. Let's use the workplace relations vernacular. Is there equality of bargaining power?

Senator CAMERON—You have not asked that question for a long time.

CHAIR—I thought it might surprise you! That is why I gave you the pre-emptive strike in 'Settle.' People would argue that it is your members that have the power—more power than those about whom and from whom they are seeking information. People would argue that that would, therefore, affect your members' argument that consent, once obtained, is genuine.

Mrs Rohan—I would argue that technology, as is always the case, is a great enabler. Technology provides quite significant—

CHAIR—I am sure that will be the union in a workplace relations environment, Senator Cameron!

Mrs Rohan—I make no comment on workplace relations, it not exactly being my field.

CHAIR—Be thankful.

Mrs Rohan—Yes. There are quite a number of privacy tools now available to consumers who are educated and informed. You can set your internet web browser to delete cookies every time you close it down. You can choose not to deal with a website. You can put your internet browser onto private viewing. You can exercise choices through search engines through ad preferences. So I think that, not only are those tools available, there is also the ability to go off to another competitor's website and not deal with someone if you have a query or a question about it. You can use a different search engine. You can use a different internet browser. You can choose not to use some software and use others. Perhaps there is actually more choice in some regards if consumers are properly informed and are so minded to exercise it.

Senator CAMERON—How much does your organisation spend on educating consumers?

Mrs Rohan—In terms of education of consumers we probably would not have a figure. We certainly keep our consumer help frequently asked questions website as up to date as possible, notwithstanding the fact that we are changing websites this weekend.

Senator CAMERON—That is handy.

Mrs Rohan—It is the digital economy in motion. Industry associations are not the size of an industry, but we have a hunt group which fields calls all the time in relation to privacy issues. That service as an education function—

Senator CAMERON—I am talking about proactive not reactive.

Mrs Rohan—We will deal with consumer inquiries as they come in. Our main focus is educating industry. We provide a free member service which is very heavily used. We provide compliance tools and websites. I teach a one-day compliance course 10 times a year. We have on call a 1-hour webinar which our marketers can access at any time. It highlights all of the requirements under the Privacy Act, the Do Not Call Register Act, the Spam Act, the Copyright Act and the Trade Practices Act. We do as much as we can to ensure that those resources are available. That is why I can say with confidence that we help thousands of marketers a year understand what the legislative requirements are.

Senator CAMERON—You indicated that, with the ADMA code, you like self-regulation.

Mrs Rohan—Well, yes.

Senator CAMERON—And I am a cynic on self-regulation. I have just got your annual report for 2009-10 and had a look at the code of practice. You outline eight different steps that you can take against a member in relation to breaches of the code. If you go further down, not one of these was used in 2009-10. It is either of two things, or somewhere in the middle: either they do

not work and they are irrelevant, or you have a membership that is so good that you do not need to take any action against them. I am not sure about either of those.

Mrs Rohan—But there is another alternative.

Senator CAMERON—Is there another alternative? You can take this on notice. You tell me this has been up since 1998. Can you tell me how many formal apologies you have issued since 1998? How much corrective advertising or withdrawal of offending advertisements or statements have you required since 1998? Can you tell me how much correction or deletion of relevant records and personal information you have required since 1998? Can you tell me how many times you have recommended refund or replacement of goods or services where appropriate since 1998? Can you tell me where you have required the member to take specified remedial action to correct the breach and avoid a re-occurrence? Can you tell me how many times since 1998 you have sought a written undertaking from the member that the breach will not be repeated? Can you tell me where there has been a recommendation to the CEO that the membership be revoked? I do not think this will be onerous, given this year's report. Can you just take that on notice and let me know.

Mrs Rohan—Indeed.

Senator CAMERON—I am always interested in these codes of practice and how they are actually applied.

Mrs Rohan—I will take those questions on notice, but I can tell you that, in relation to our annual report, of the 52 complaints that we received I believe 21 were in relation to members. All the ones that related to members were resolved to the satisfaction of the consumer by the member before it was referred to the code authority.

Senator CAMERON—That does not set my mind at rest, because I have had a look at your website. I must say that, if you were trying to make a complaint, you would be battling on your home page to find out where to make a complaint.

Mrs Rohan—I have done a benchmark against the BBC complaint-handling process, which has been held up to—

Senator CAMERON—I am not talking about the BBC.

Mrs Rohan—I am sorry. I would just like to finish.

Senator CAMERON—I am talking about your home page. If you were a consumer who had a problem, you would find it extremely difficult. I am not surprised you only have 50-odd complaints, because it is not easy to make the complaint. Would you agree with that?

Mrs Rohan—No, I do not. The reason why I do not is that we have done a benchmark against the BBC complaint-handling process, which is set up to be international best practice, and in terms of the number of clicks—and we are getting a new website on the weekend—

Senator CAMERON—I will give you a recommendation for your home page.

Mrs Rohan—But, if I could just finish, on our home page you have 'consumer help', and then you can go to frequently asked questions. Appearing in frequently asked questions at least 10 times is the way that consumers can email us with a complaint.

Senator CAMERON—Why wouldn't you just put that up front? Why would you have to go two steps into your website to find that? Is that best practice?

Mrs Rohan—From the BBC, and the way that we have consulted with the code authority, who have some expertise in the matter, it is best practice as I understand it.

Senator CAMERON—How can it be best practice if someone has to take these steps to find information? Why can you not have on the home page, as some companies have, a section where you can click on 'complaints' and find out how to do it?

Mrs Rohan—It is certainly something that we can take on notice.

Senator CAMERON—Can I recommend that you do that and next time you appear we will see how it works?

Mrs Rohan—Senator Cameron, if it improves your belief in self-regulation then we would be pleased to consider it.

Senator CAMERON—It may not, but let us try it anyway. Thanks.

CHAIR—Thank you, Mrs Rohan.

Proceedings suspended from 1.05 pm to 2.06 pm

JACOBS, Mr Colin, Chair, Electronic Frontiers Australia

CHAIR—Welcome. You have been before us before, haven't you?

Mr Jacobs—I have not; my predecessors may have been.

CHAIR—Then I will make you aware that the proceedings public, but if at any stage you want to give evidence in private then make your request and the committee will consider it. It is an offence and potentially in contempt of the Senate for a witness to give false or misleading evidence, as indeed it potentially is for a third party to attempt to interfere with evidence that a good witness like you might otherwise give to the committee. If at any stage you want to object to answering a question you may attempt to do so. We have your submission. Do you need to change it at all?

Mr Jacobs—No, although I will make a few remarks about it.

CHAIR—Proceed.

Mr Jacobs—First of all, I would like to thank the committee for listening to us today. We think it is very encouraging that the parliament is taking this issue is so seriously. It is one that is very complicated, but it is something that is going to be more and more important as the digital future continues unrolling. I will say a few words about the data retention plan, which was the basis of our submission, and then I will make a few remarks about online privacy more generally. Then I am happy to answer questions about either of those topics. I might present a couple of scenarios that I think show a few hurdles and a few wrinkles in attempts to regulate, particularly on transborder issues but online privacy in general.

I understand the committee is well aware of the reported plans by the Attorney-General's Department to institute a mandatory data retention scheme in Australia. From our point of view, this is probably one of the biggest threats to privacy that we can see on the horizon and it is a bit of a step backwards as far as the government approach to privacy goes because, like this inquiry and in the past as well, there have been many positive signs about government attitudes to privacy.

From the Attorney-General's point of view or from the police's point of view we can understand why they would want such a scheme. Cybercrime is growing, it is very important, it could have huge impacts on our economy and our citizens, and there is generally no physical evidence to speak of—all the evidence that you have in a cybercrime case is going to be digital records, logs from ISPs and things like that. However, the scheme as proposed has huge drawbacks as well for a society, and we have yet to hear a very good case for why such power should be necessary. We do not think it is hyperbolic to describe such a system as 'mass surveillance' because it does involve the most private communications of pretty much everybody in the country who uses the internet for communication—and if it is not everybody yet, it is going to be.

As we pointed out in our submission, we think that the experiences from Europe are very, very instructive. The data retention directive has been very controversial in Europe. Indeed right now, as we speak, there is a meeting of privacy and data protection commissioners happening in Israel and data retention is one of the topics that they have discussed. As I understand it, it has been quite controversial.

We mentioned, for instance, that in Germany the Constitutional Court found that data retention law that was enacted there to comply with the directive was unconstitutional. The judge pointed out that even though it was just the data about communications there would be sufficient data gathered to enable the compilation of a profile on somebody's interests, which political party they might be leaning towards, et cetera, and that it was out of proportion to the needs of law enforcement.

Sweden has declined to implement the directive and so they are subject of a suit by the European Commission. In Romania a court found that the data retention provisions violated the European Convention on Human Rights. Also the ACLU and others have come out and claimed that data retention schemes such as this one are in violation of the Universal Declaration of Human Rights, and I believe that others have pointed out in their submissions to the committee that you would violate the National Privacy Principles in Australia including fairness, being unobtrusive, and collecting data only for its stated purpose.

We went over some of the issues in our submission. I will just add that the cybercrime treaty, which we understand is being considered by the Australian government for ratification, and that is one of the impulses behind the data retention scheme, has other privacy implications as well. For instance, it contains clauses that give law enforcement almost unrestricted access to their networks of ISPs if they have a warrant from an organisation or a court in Australia or, indeed, overseas. It would then be incumbent on law enforcement to look only at the data that was pertinent to their particular investigation. There is very little oversight mandated in the treaty so there are a few privacy implications as well with giving law enforcement greater access to our communications networks.

We would hope that when push comes to shove the Attorney-General's Department would get some hard questions put to it, questions such as: which crimes could be solved with this extra information that could not be solved without a data retention regime and what evidence do you have to support that? Is there empirical evidence that shows that the crimes are serious and have big implications but that there is just not enough data available at present? Indeed, how do they intend to use that data? For instance, if law enforcement go to an ISP and say, 'We want the data on such and such an individual, or such and such an IP address,' will the ISP give them the entire data file that contains information about everybody else? Will the ISP have to sort the data in a way that filters out all the other information? That is a huge burden of work and expense to go into ISPs, for instance, and so we would expect that the cheaper option would be the one that might occur, and that has implications for privacy.

So in speaking about privacy more generally, Electronic Frontiers Australia is in agreement that a principles based approach is the way to look at regulation. We definitely support a well-resourced information commissioner or privacy commissioner. We think that the emphasis on education is the right one, although that is a particularly complicated area and it is going to be very difficult to figure out just how we educate people so that they make the right choices. This

sort of approach is great when it comes to the public sphere and, clearly, the government takes it seriously. In the past we have been involved in some privacy impact assessments and so on and, in general, apart from the data retention issue, it has at least been demonstrated to us that it is taken seriously.

But in the private sphere the pressures against privacy are very, very strong indeed. As the committee probably knows, if you are an advertiser and you go to Facebook, you can place an ad that only goes to university students between the ages of 18 and 23 who are interested in horses but are not yet members of the Equestrian Federation of Australia, for instance. From an advertiser's point of view that is a goldmine and you would be willing to pay a very high premium to target an advertisement that way, as opposed to something that is just seen by everybody. The more niche your market is, then the more you are willing to pay.

Against those sorts of forces it is always going to be in the interests of companies that collect data from individuals to make more and more of that public. And of course there is always fraud to worry about. It is very profitable to have access to people's private information as well. We think this is only going to get worse in the future. Something that has been on our radar recently is augmented reality. We have had questions from the media, for example, on the privacy impact of augmented reality.

You can do it today. You could use a mobile phone, for instance, hold it up and look through the phone's camera and it will overlay information about the environment around you with data that it has fetched from one database or another. When you combine that with things like geolocations—your device has a GPS and knows your location—facial recognition software and social networking, it is very easy to foresee an occasion when you write a message about where you are and what you were doing and other people in the area are able to hold up their devices and immediately identify you and associate that with your other profiles online. People may not be aware that what they are doing means that their actual location in physical space could immediately be detected.

So what is the answer to that? It is not obvious but it is one way in which things are getting more and more complicated. I noticed in other submissions to the inquiry that transborder issues are of concern. We know Facebook is very popular today, but we do not know what is going to be popular in two years from now—and it could very well be headquartered in Bermuda or Venezuela—how we approach that from a regulatory point of view; it is difficult.

We have seen some discussion of regulating Australian entities when they send data overseas but I can think of several examples—which I have prepared and which I can talk about later if need be—where simply transferring data overseas is, I think, a poor way to deal with regulation. It would be better to think about access and the purpose of moving data around. As things like the services offering data storage become more and more commoditised the physical location of where data is stored is going to become harder and harder to define. Sometimes we hear discussions about cloud computing, software as a service—people are outsourcing their data processing and data storage functions. These could end up anywhere in the world and that makes this sort of privacy regulation a bit more difficult.

Finally I would just say a couple of things about anonymity. Around the world we are seeing that there are greater and greater pressures towards removing the ability for anonymous

speech—for instance, on the internet—and for anonymous communication. Of course this is happening in countries like China et cetera where they are making it more and more difficult to even use an internet cafe and so on without proving who you are and all websites are registered et cetera, but we face similar challenges here in Australia. Come election time, for instance, there is commentary on elections online which has not been regulated in the same way as placing an ad in the newspaper or a TV advertisement where there has to be an attribution and anonymity is not allowed. But I do not think we have come up with a great way to handle that when it comes to the online world and borders start to get blurry and things like defamation and so on also put pressures against the ability of people to remain anonymous online.

One area we foresee where online privacy is going to heat up is in copyright. Around the world there is a lot of pressure from the copyright industry for schemes that are called graduated response, or three strikes, where the copyright industry are able to identify people based on an IP address, for instance, who they feel are violating their intellectual property. They can then go to internet service providers and say, 'Tell us who this person is,' or 'Can you please pass on a warning to this person,' or 'Can you shut off their internet access' without having to go through courts or any sort of law enforcement.

Countries such as the United Kingdom, France and Ireland have systems like this in place already and, in some of those, copyright holders are able to go, without proving anything in a court of law, to an ISP and say, 'Tell us the identity of this person because we want to sue them.' This is a trend which will lead to more monitoring of what people do online by ISPs if they are forced to do so by the industry, and it could ultimately involve the disclosure of people's identities and web surfing habits to a third party without judicial oversight. There are concerns about that as well when it comes to internet filtering—about whether ISPs might have to keep a log of people's attempts to access sites. In fact, from the operational point of view it is almost inevitable that the ISPs would have such logs.

CHAIR—Mr Jacobs, it is all very interesting but we want to fire some questions at you. Are you almost done?

Mr Jacobs—Yes. On that note I am happy to answer questions.

CHAIR—All right, I will kick off. What is the reason for the 'frontiers' in the name Electronic Frontiers?

Mr Jacobs—We were founded in 1994 so at that time the intersection of the online world and public policy was a new frontier.

CHAIR—Let us go straight to that. It is now not a new frontier but—and you may have heard my question earlier—are we still, nonetheless, trying to apply offline policing and thinking online?

Mr Jacobs—I would say, generally, yes.

CHAIR—Examples?

Mr Jacobs—Censorship, for instance. Our censorship system is based upon classification. Work is submitted to the Classification Board, which decides which classification it fits into.

CHAIR—'Our'—do you mean your industry?

Mr Jacobs—I mean Australia's.

CHAIR—Right.

Mr Jacobs—Now the government proposal to implement mandatory ISP filtering in Australia means they want to filter web pages based upon their classification—to wit, whether it would be refused classification or not. When a finite number of DVDs are being imported into the country every year—there are some thousands—it is possible to review them all in timely fashion and make a determination that is public. But when it comes to the web, which is international and dynamic and contains content upwards of a trillion pages, that is never going to work. However, that is the approach that the government is taking. We think we need to really go back to the drawing board and have a rethink about how that could be done.

CHAIR—Does your organisation think there is a way to get the policymakers to get with the program?

Mr Jacobs—Yes and no. Clearly, as policymakers tackle these issues and become more and more comfortable with how the internet works, the obviously silly proposals at least will become fewer. But that does not mean there are any easy answers. I am sometimes asked: 'Well, if you can't block these web pages this way, what can you do? What do you do when somebody goes onto Facebook and defaces a tribute page to a slain child with offensive material?' I believe it was Senator Xenophon who suggested an internet ombudsman who could look into these sorts of things. That is not going to work, just because of the way the internet is. So what is the answer? How do you deal with that? Unfortunately, I have to say that maybe that is just the price we pay for the benefits that we reap from the internet.

CHAIR—So profanity happens occasionally.

Mr Jacobs—Profanity happens. Offensive behaviour and offensive material happen.

CHAIR—All right. That takes me to the next part of the same question. Is it part of your observation, then, that since the birth, I guess, of your organisation and the move to embrace technology we have in some way compromised what we might otherwise regard as our right, as individuals, to privacy?

Mr Jacobs—Not all of the encroachments on privacy have been the result of a failure of government policy, by any means.

CHAIR—No, it may well be as a result of an individual like me—

Mr Jacobs—That is right. I think it will be a part of the future landscape that privacy will be different from what it has been in the past, and there will be less of it. It is almost inevitable. We get huge benefits from giving up our privacy sometimes: the ability to use social networking or

to use tools that take information about you and then give you a service in return based upon where you are, what you like or who your friends are. These are great. They have huge impacts on productivity. The number of people using Facebook attests to the fact that people really love that sort of thing. So it is going to be voluntary, in a large measure.

CHAIR—In saying that, to what extent does your organisation represent individuals—the layperson user or the working class that Senator Cameron likes to ask about?

Mr Jacobs—Our direct members are people who are more aware of these issues and have more of a focus on things like privacy, censorship and so on than the layperson would—that is for sure.

CHAIR—So the laypeople are not members of your organisation themselves.

Mr Jacobs—The internet-using population of Australia comprises almost the entire population of Australia. Our membership is much less.

CHAIR—How many of them are your members?

Mr Jacobs—I do not have the exact figure handy, but we have several hundred dues-paying members, several hundred life members and various other supporters, who do not pay dues, through various lists in Facebook and so on.

CHAIR—I am just trying to attest the extent to which you represent a certain part of the population that might be saying, 'Look, we're so eager to use this technology that, if we sacrifice some of our rights to personal information along that journey, so be it.'

Mr Jacobs—Even our members and I are willing to sacrifice some privacy, as long as we have some control over what happens to that information and as long as we are aware.

CHAIR—But, to the extent that your organisation represents stakeholders in the industry as well, they would have that view, because they have a vested interest in it.

Mr Jacobs—We do not represent industry. We are a membership based organisation that represents the users, so if you are talking about the industry—

CHAIR—Perhaps the best way to get my head around this is to explain how you define 'user'.

Mr Jacobs—That is a good question. The proprietors of Facebook use the internet as well, but—

CHAIR—That is what I am getting at.

Mr Jacobs—we are looking from the point of view of the average person who is consuming services as a consumer.

CHAIR—So user equals consumer.

Mr Jacobs—Right—in this case.

CHAIR—Do you have a constitution or membership screed?

Mr Jacobs—We do, yes.

CHAIR—Can you provide that to the committee?

Mr Jacobs—Yes, I shall.

CHAIR—Thank you. Did you hear Google's evidence on their Wi-Fi connection earlier today?

Mr Jacobs—I did, and I am familiar with the issue.

CHAIR—In the past you have said they deserve to be held to account. Mr Flynn's words today, to me, were that Google is saying, 'Oops; mea culpa, although there was no malice or forethought.' Is that good enough? Do you have any observations?

Mr Jacobs—In my view Google should have known better and should have done better; therefore, the mea culpa is justified and they deserve to cop a bit of flack for what they did, because it was a serious invasion of privacy. However, looking at things from a technical point of view, I do accept their explanation that it was accidental. From an engineering point of view I can see why this data may have been collected. It was sort of a case where engineers were told to solve a problem and they solved it in the most efficient and effective way but the privacy and legal people were not as involved as they should have been. Sometimes the engineers need to be reined in a bit. So I think that, given what the trends are—there are trends for deliberately collecting and making more public individuals' information—hopefully, what will come of this is that Google will have learned a lesson. I do not think it is part of a broader or more sinister trend to spy on people, for instance.

CHAIR—Point taken. That is good. Let's hope we learn an online lesson. What is your view of the flipside of this privacy debate? There is the suggestion that you might have heard me talk about earlier: there is a service industry springing up to protect the identities of organisations that run websites who have non-altruistic or, indeed -legal business motives. Do you have any comment to make about that sort of industry and activity?

Mr Jacobs—Do you mean a particular industry that shields the identities of people who are running websites that have illegal purposes?

CHAIR—Yes.

Mr Jacobs—Given that you can host a website in any country and given that regulations very, the way the internet works is anonymity is something that is probably going to apply to people who run websites as well as people who use them. So I think it is inevitable that such technology will exist. We will see a bit of an arms race when it comes to the technology itself and, perhaps, with the laws; but, no, I do not find that surprising. I think it is inevitable. We will have to have other ways to deal with it.

CHAIR—Should the members of that service sector have the ability to say, 'Thou cannot have access to my client's details, because that's an invasion of their privacy'?

Mr Jacobs—In what sense is it an invasion of privacy?

CHAIR—I think that is the question. Are you saying it is not?

Mr Jacobs—Do you mean the privacy of people operating the service or the privacy of the people using their service.

CHAIR—I mean their clients. The service providers argue that their clients' privacy is invaded if they disclose their details. It is like a doctor-patient relationship.

Mr Jacobs—That is right. That may be fair enough, and I am sure we can conceive of situations where somebody could provide a service and anonymity means that they can be more valuable as a public service.

CHAIR—But in this case the client is not doing good; the client is running a website that is intent on scamming people, for example.

Mr Jacobs—In that case it is less of a privacy issue, in my view, than a criminal matter, and we already have ways, without a data retention regime, to compel service providers to offer up the identities of their clients. If they are hosted in a country or a place where it is very hard to do that legally then we have to look at other methods. We already face that problem today. The Australian Federal Police face that problem today. If your credit card is ripped off by somebody in Eastern Europe, where do you go from there? Whether they are anonymous or not, if you cannot get to the service provider to put a question to them, it is going to be very difficult to take the matter any further. There are no easy answers there, in summary.

Senator LUDLAM—Your submission focused in large part on the A-G's data retention proposal, so I think we should start there. The limited amount of material that is available about this project is mostly open source reporting in the media as a result of an FOI request. The little bit that we do have from the government—and hopefully we will get a bit more this afternoon—has been along the lines of: 'Relax—we're not seeking to log the content of web traffic, just some kind of identifying information about where you went and who you emailed rather than what was in the email.' From your point of view, is that good enough? How much info can you tell about somebody if you have removed the content of the traffic itself?

Mr Jacobs—Clearly, if they are just recording information about the communication, it is better than having the police listen in to every phone call or read every letter that you send, but it is still very, very possible to use information of the kind that you described—when an email was sent and to whom—to build up a profile of somebody's habits. That is clearly why the police might want it in the first place. As we note in our submission, the court in Germany considered this matter specifically and said that, even though the content of the communications was not to be kept, there was still going to be more than enough information to build a very invasive profile of somebody, and we would agree with that. Just as you can imagine that from mobile phone records you could figure out who somebody was calling and why, email would be the same. If you just keep the headers of emails but you delete the body of the email, which has all the

content, you would still have who it was sent to and the subject of the communication, potentially. If you do not consider that a privacy issue then I am not sure what to say. The same would be very true for web communications. Even if you do not know the content of the webpage that somebody viewed or the information that they posted in a form when they interacted with the website, just knowing what websites they go to and the fact that they are using them would enable you to build up a full profile of somebody's interests and habits.

Senator LUDLAM—And relationships. One of the issues that has been brought up as a consequence of this is that it would be an extraordinarily detailed relationship-mapping tool. I put that side by side with the fact that the nation's counterterrorism legislation has very broadly cast the net on criminalisation—for example, association offences. If you happen to be with someone in a listed terror organisation, you can be charged with very serious offences on the basis of who you may have contacted. For me, that relationship-mapping aspect feels just as important as a personality profile.

Mr Jacobs—The jargon that we use in the industry would be 'data mining', 'friendship trees', 'interest profiles' et cetera. Even for benign purposes such as marketing, the technology exists to go through corpuses of information like this and figure out who people's friends are and what their interests are. I am sure Facebook, for instance, would be masters of this. But, as you say, if it were used for purposes of figuring out somebody's associates in a proscribed political organisation like a terrorist cell or something like that, the destination, source and timing of the communication is enough to do that very thoroughly.

Senator LUDLAM—We are not going to have you on this side of the table when the Attorney is here, and you have already given us a couple of ideas for questions, which is helpful, but how much is EFA aware of what the proposal actually is and when we might see it implemented?

Mr Jacobs—We pretty much know what everybody in the media knows. There are anecdotal reports from inside the industry based upon their unfortunately secret meetings with the Attorney-General's Department. Again anecdotally, I have heard that those are correct and that the demands from the Attorney-General's Department were pretty broad. As I believe we noted in our submission, it was characterised by one technical expert as 'if it is logged, they want it'. That is pretty broad. The media were concerned that that involved weblogs, which we think would be more of an issue if and when the mandatory internet filtering comes into place. But, in answer to your question, all we understand is that it has been pretty broad. If you have a look at what is mandated under the similar proposals in Europe, that is very broad as well. It includes pretty much all types of communication imaginable.

Senator LUDLAM—I want to come back to the question that the chair put to you about where the frontier is these days. It occurs to me in a way that the augmented reality services that you spoke of on the location based applications seem to fit that definition for me. How many jumps are we away from the kind of science fiction *Minority Report*-style business where the advertising talks to you by name as you wander past it? Are we really very far away from that kind of application?

Mr Jacobs—No. We might not have it next year but in five to 10 years it is very easy to imagine that something like that will be possible. I think it is almost inevitable that eventually

the augmented reality will be performed by our glasses or sunglasses. There will be something talking into our ear, constantly reminding us about interesting information and, indeed, advertising. The services behind these are going to come from all over the world and people will be making deliberate decisions to opt in to this and in some cases they will not be.

Senator LUDLAM—At the moment, the burden of proof seems to be on us to work out what on earth is going on and then figure out how to opt out of it. We do not have an opt-in model at all, particularly where commercial providers are concerned. I was just reading a little bit about Adobe Flash cookies, for example. I figure that not one person in a thousand would know that when you delete the cookies in your browser there is a whole separate category of identifiers that are not. I have just done a search on my laptop and there are about 12 files there. How was I to opt out of that if I did not even know it was there?

Mr Jacobs—Only a very sophisticated user can manage all of this. There are even more obscure ways than Flash cookies by which website operators could track your movements on the web.

Senator LUDLAM—Do you want to describe some of those for us?

Mr Jacobs—Yes. For instance, you can serve up an image that is cached by the browser and you can customise that image so that it identifies a particular user and then fetch information about that image from the web browser's cache later on. You can use the browser history. Websites are able to analyse that. You can send a user to a page that identifies them in particular and then search the browser history programmatically later on to figure out who that user is. I cannot remember the name of the website at the moment, but there is a proof of concept on the web where you can delete your cookies and your Flash cookies and then come back to this website and it will tell you—

Senator LUDLAM—Who you are.

Mr Jacobs—who you are, because there are ways that are very difficult to deal with. Some browsers have private browsing modes, but even they might be defeated by some of these more sophisticated techniques.

Senator LUDLAM—You used the term 'arms race' before, and that feels to me a little bit like what we are in. What kind of organisations are deploying that kind of cutting-edge technology?

Mr Jacobs—We do not always know. This was a proof of concept. It was put out there for anyone who wanted to use it. Who is using this to recreate cookies once they have been deleted I cannot say. That is not something you would expect Google or Facebook to do or even a mainstream advertising network, but I do not doubt that there are websites and networks that have already adopted this technique. So the next step in the arms race will be for the browser manufacturers to add the ability to delete that sort of information. But then we would be back where we started and they will look for another way to identify people.

Senator LUDLAM—On the image cache that you mentioned before, the last couple of gigs worth of images that I have looked at online are stored in here and not many people know that. What kind of technology may or may not be embedded within any one of those images?

Mr Jacobs—The example that I gave was that you can serve up a very small image that is customised and the website can send a specific directive that tells the browser to cache the image forever and then you can use something in the new HTML specification, which is a canvas, in your website program to look at each pixel of the image. That is information that could encode anything that you wish. That is one technique, but if web users get smart and start deleting all of the cached images on their computer then they will start looking for something else. That is one example of where the arms race is at the moment.

Senator LUDLAM—I have used the word 'creepy' a couple of times today; I am going to use it again.

CHAIR—I think you have been going a lot faster than creeping for Hansard. I hope they are managing to keep up with the lingo.

Senator CAMERON—Thanks, Mr Jacobs. Some of the evidence we have had demonstrates that, for instance, when you go on Google, information is collected from emails. They have a view that you can opt out. If you know the process, you can opt out of the collection of this information. Is there an argument for an opt in, or is there a technology such that you could opt in? So, if you say, 'I don't mind Google collecting this information,' you could opt in to that. Why is the default the opt out?

Mr Jacobs—I think the answer is: for commercial reasons. In the scenario I described with the Facebook ads before, for instance, if people have opted out or they have to opt in to a system whereby the advertisements can be served up based on what you know about them, then it is much, much less valuable. Google, to their credit, are very good at what they do, which is selling advertising. Being able to show somebody who is reading an email about the Bahamas an advertisement for a trip to the Bahamas has enormous value for the advertisers and for Google. Therefore it is not in their interests to put up an opt-in model. There is no technological reason why it could not be opt in, but there is a very compelling—from Google's case—business reason, and that is the pressure that we are always going to be dealing with.

Senator CAMERON—Isn't there software now where you can clean the cache out?

Mr Jacobs—You can, but, if you are reading your emails, Google has to know who you are in order to only show you your emails. If you are using Google's services anonymously, you can make sure that there is no cookie, for instance, and your cache is cleaned, but, if you are coming from the same IP address, such as your home internet connection, and you are using the same web browser, then you can make a pretty good guess that it is the same person as well. So, unless you are one of the tiny minority of people who are so concerned about privacy that they run special software that will disguise their identity in all of these myriad ways which are much more difficult than just being logged in or not, you are leaving breadcrumbs behind that enable a smart operator to put two and two together.

Senator CAMERON—That comes to the issue of: when do you believe it is appropriate for police, law enforcement agencies, to have access to information?

Mr Jacobs—I have not heard a compelling case that the system we have now is broken. With a warrant, with a court order, a law enforcement agency can go to a company that provides email

services, like Google or Yahoo, or to an internet service provider and determine the identity of somebody who was at a particular IP address or view their emails. Until I hear a compelling case that that is just not enough data, that we need to go further back in time, that we need to have the information on everybody, whether or not they are of interest to law enforcement at the moment, we certainly cannot support the data retention proposal. Again, ISPs and email providers keep information as part of their operational duties and for billing purposes and what not. That is already a lot of information, and police have access to that with judicial oversight. That seems to be working pretty well, and at least there are some checks and balances there.

Senator CAMERON—But I understand from reading newspapers and stuff like that that people say intelligence services have access to all of this anyway. Is that your understanding?

Mr Jacobs—It is hard to say. If your traffic is flowing through another country, for instance the United States, we have definitely heard reports about widespread real-time monitoring of communications in there. There was a lawsuit filed against AT&T for their complicity in installing massive hardware at the behest of the National Security Agency to monitor all of the real-time communications on AT&T's network, and that court case did not go anywhere because eCongress passed a law giving them retroactive immunity. What is going on in Australia in terms of real-time monitoring of people's communications? I do not have any information to suggest that that is occurring, but, when you send somebody an email, you do not know where it is going to go. It could certainly be in another jurisdiction where that is occurring. I communicate with China, for instance. It is a public fact that information sent to China goes through the so-called 'great firewall', which does keyword monitoring, for instance.

CHAIR—Thank you very much, Mr Jacobs. That was very interesting. Thank you for your time and your evidence.

Mr Jacobs—You are very welcome.

CHAIR—Hansard may have some questions about some of the things you have said.

Mr Jacobs—I will speak more slowly next time!

CHAIR—No, not at all.

Senator CAMERON—I wouldn't underestimate Hansard!

Mr Jacobs—I tried to keep the buzzwords to a minimum, until pressed by the senators.

CHAIR—That's right—you have got Senator Ludlam here who is right up with you! Thank you very much.

[2.45 pm]

YOUL, Mr Trent B, Chief Executive Officer, Fraudwatch International Pty Ltd

CHAIR—Welcome. I think you would have heard the niceties earlier today.

Mr Youl—Yes.

CHAIR—Is there anything you would like to add about the capacity in which you appear today?

Mr Youl—I am the CEO of Fraudwatch International, a private company based in Melbourne.

CHAIR—Thank you. You have given us a submission; do you need to change anything in it?

Mr Youl—No.

CHAIR—Okay; how about a quick opening statement?

Mr Youl—Sure. As I understand it, the committee is looking into a range of issues to do with protection of privacy for Australians online. My, and our company's, area of expertise really is in dealing with internet fraud and in particular the issue of 'phishing', which is basically criminals impersonating companies to steal the personal information of their users. I made this submission—and I was asked—because I understood that the Senate committee had some interest around the issue of an industry that is protecting the identity of those who own dubious websites, in relation to a newspaper article a number of weeks ago.

CHAIR—Was that the one in the *Age*?

Mr Youl—I do not have that with me; I apologise.

CHAIR—No, it is okay.

Mr Youl—The information that I can offer is probably very limited and very specific, in dealing with that particular issue, as opposed to the rest of the scope of your committee's hearings. Basically our company specialises in anti-phishing. We protect and work for the banks—financial institutions, mainly, worldwide. Specifically we address the threat of phishing when criminals are impersonating their brands to steal their customers' login and account information. As part of that, we actually monitor the internet or, specifically, spam emails and a number of other methods. We are looking specifically for phishing emails that might be targeting our clients. Once we identify the emails, that leads us to a phishing website which is almost a direct copy of the genuine website. Part of our process in actually taking those websites down, which is the next step in what we provide for the banks, is to look at contacting the domain registrars, internet service providers, web hosts and website owners, because we find that approximately 80 per cent of all phishing websites are hosted on hacked websites.

CHAIR—'Hacked'?

Mr Youl—Hacked—so a website that has been hacked into by criminals and then had the fake phishing web pages, which are impersonating a bank's, uploaded onto that website, without the owners of the website actually knowing about that.

CHAIR—Yes; I was just checking that it was 'H-A-C-K-E-D'.

Mr Youl—Yes, hacked. That is why we are interested in the industry that is protecting the identity of website owners. In my submission I delve into one example, which is an organisation called PrivacyProtect. It is based apparently in the Netherlands, although we can never be too sure. It is the privacyprotect.org website. It is basically a third-party which will step in between the website owner and place their information in a whois database. I am not sure if you are familiar with a whois database. Basically, around the world anyone who owns a website needs to have contact information for that website. Specifically within Australia—and I do address that in my submission as well—there are regulations around making sure that that information of the registrant, the owner of the website, cannot be hidden; however, across the rest of the world it can be.

One of the issues we face when we are trying to have phishing websites taken down is that we find a hacked website and suddenly we cannot contact the website owner because their information is hidden. If the website owner has subscribed to this type of service that is apparently protecting their privacy and they do not have any contact information on their website, which many websites do not, it makes it very difficult for us sometimes to do our job and get these fraudulent websites taken down as quickly as possible. In particular, that is why I am here to help educate you on that issue as well.

Senator LUDLAM—Thanks very much for coming in. I appreciate your submission. This for me is probably the most interesting example where we are effectively asking: what right to privacy do the people who would seek to invade our privacy have? Where do you draw the line? What solutions do you propose for these folk who have made themselves invisible within whois?

Mr Youl—It is a very difficult issue to address. In answer to that question of what right those people have to protect their privacy, logically you would think: not a lot. Specifically within Australia I think it is reasonably well addressed in that the regulations with auDA actually provide that that information cannot be hidden. We can go on to whois now and find an owner of an Australian website and at least get their email address. The big issue there is that as an Australian I can register a dotcom domain, I can subscribe to this type of service, I can be running a dotcom domain and focus on trying to attract Australian visitors to try to market to Australia. I am Australian here, but if I register a dotcom it is regulated by the US domain registry regulations, so I can subscribe to the privacy protection and I can hide my information. I think many Australians when browsing the internet are quite aware that a lot of Australian companies anyway will use a dotcom website as opposed to a dotcomdotau as well.

Senator LUDLAM—And not necessarily for dodgy reasons.

Mr Youl—Absolutely.

Senator LUDLAM—Just to make the distinction absolutely clear, I can be sitting here in Australia and have paid money to an offshore company or host the data overseas as a dotcom site and then go completely behind a screen as to who I am and what I am doing there.

Mr Youl—Correct. Just to take that one step further, you can be an Australian here and pay someone overseas to actually register the domain, but you can have that registered here in Australia if you like and still be behind that screen of privacy protection.

Senator LUDLAM—You have focused on this specific issue in your submission. How big a deal is this single issue of people hiding their registry details? Is it the biggest issue that you confront in your work of pulling these sites down?

Mr Youl—Not the biggest issue. The biggest issue would probably be what we call 'bulletproof web hosts', which are web hosts that essentially work with criminals—in China, Russia, South America. This would probably be the second biggest issue for us. However it is not the end of the road for us. Just to give you some idea of our company, we probably take down anywhere from 500 to 1,000 phishing websites per month.

Senator LUDLAM—What does a 'takedown' look like—

Mr Youl—Taking down basically means to bring them offline, off the internet, so that they are no longer accessible by consumers. Different web hosts that we deal with and ISPs deal with that in a different way. Some of them might suspend a website or completely block access to it. They are the two main things that they do.

Senator LUDLAM—The reason I am going to a bit of detail—and it is a digression specifically from the privacy argument—is that no doubt you have been following the net filter debate here over the last couple of years. The biggest single example, and probably the only legitimate example advanced by the government in defence of that proposition is what you do with an offensive or illegal site hosted overseas that Australian law enforcement agencies do not have access to. You issue some sort of takedown notice.

Now your line of work is around financial institutions—you said before that you work principally for the banks—but I would have thought that your techniques of investigation exactly aligned with those that would be most relevant in the filter debate. So have you got anything to teach us? Is there anything that you folks do that the Australian government could learn from in that parallel domain—pulling down sites that are hosted in other parts of the world?

Mr Youl—Specifically with the internet filter I would probably have to say first up that if that were to go ahead with some of the proposals that I have heard, in particular if the filter were to block or to filter phishing websites, I would need to take my business offshore.

Senator LUDLAM—I do not think that was ever a proposition, but who knows—

Mr Youl—I think it was Alastair MacGibbon who made some point that was picked up in the media that phishing sites should be blocked. So, yes, that does concern me to an extent. We employ Australians here. We also have an office in the US. But I have started the business and I prefer to keep the business here in Australia, predominantly. So from that perspective it would

certainly restrict banks, law enforcement and any other companies that are trying to perform takedowns, if they could not actually have visibility of the site without going through proxy servers, that is, accessing that particular website through another server outside Australia or outside a filter. That would certainly cause a lot of issues.

On the takedown side of things, the main thing that we have worked on—and our company has been around for seven years—is building relationships with various web hosts and internet service providers around the world. We are trusted. When we contact them—and a lot of them we have direct contact points—to issue them a takedown notice, they trust us and will go ahead and do that. We do not issue court subpoenas, we do not have any legal ability to put pressure even on web hosts within Australia. A lot of the time it has simply been a matter of helping them identify that their resources have been abused as well and they are more than happy to take action.

Senator LUDLAM—I guess the point I was making was that precisely the expertise that you have is what the government is looking for if it does not get its filter. It is that ability through relationships and so on to specifically target foreign hosts of offensive material or illegal material and have it pulled down as an alternative to the blocking strategy that the government has been pursuing. That is not a question but a statement, but I just found it a very interesting observation that you are doing what the government is seeking to avoid doing in simply filtering this material out, but in the financial sector. I suspect you might find your expertise on call for a broader range of material.

Mr Youl—Sure.

CHAIR—Is that an online ad?

Senator LUDLAM—No, I don't do commercial endorsements. But I still find it very interesting that those techniques are targeted directly at the government's sole justification for the filter. What do you do about the offshore offensive content where we cannot issue a takedown notice to a server in Australia? That seems to me to be your bread and butter.

Mr Youl—Yes, that is exactly what we do. That is what we specialise in. Also, as far as I understand it, to some extent the Australian Federal Police address the issue of getting sites taken down overseas as well. I am not completely up to speed on what their current processes are but, yes, that would be the process there. I guess it all comes down to resources.

Senator LUDLAM—Indeed. Thanks very much for your help today.

CHAIR—Mr Youl, you referred to those who own dubious websites and you have touched on this in both your opening statement and your discussions with Senator Ludlam. Ian McIlwraith wrote this in the *Age*:

> The big issue for regulators is not that the unscrupulous exist—that will never change—but that an industry has now sprung up to protect the identity of those who own dubious websites.

What would you be saying, from your experience, to regulators to deal with that?

Mr Youl—It is a very tough issue. We already have in Australia the regulations to stop that on Australian domains, the .com.au domains. It then becomes a broader issue—

CHAIR—But the industry that is seeking to protect the unscrupulous may be just as full of rogues as those that the regulations are already set up to deal with. It is about staying ahead of the game.

Mr Youl—Yes.

CHAIR—Running ahead of the rogues, if you like, as they move from one part of the techo-sphere to another.

Mr Youl—Sure. Some Australian domain registrars do provide this service, just not for .com.au domains. They provide them for the dot com domains. I will also say that our main website is fraudwatchinternational.com, so not a .com.au. We have registered through an Australian registrar. I can go onto their website now, tick the box and say, 'Yes, I would like privacy protection' and they will charge me $100 for the next three years, so they can then provide that cloak. I am an Australian, I have the dot com website and the Australian registrar will help me protect my privacy.

I am not too sure of the exact answer. It is definitely an issue that I think needs to be looked into. I do not even know if there is necessarily an answer to try to stop it. We might be able to address it with Australian domain registrars potentially and say, 'Let's not even make that allowable, that an Australian domain registrar can provide that service to Australians,' but it does not stop me as an Australian going to a register in a domain in the US.

CHAIR—So is it an issue or is it conjecture?

Mr Youl—I think it is an issue. Maybe it all needs to come back to consumer education as well to trying, to an extent, educate consumers to be aware of who they are dealing with and to be aware of who is out there and if you cannot see who owns a website maybe do not deal with them. I started our website based purely on consumer education. For the first two years we were not providing any commercial services. To educate the bulk of consumers to any great level is, I think, a very difficult task. It is one of the answers. I do not think it is the answer though. To be honest, I am not too sure what the answer is.

CHAIR—Thank you.

Senator CAMERON—I have had a look at your website. I see you have got a James Bond look-alike up on your home page. It is not you?

Mr Youl—It is not me.

CHAIR—Are we talking about Sean or Daniel?

Senator CAMERON—I am not sure what his name is but he looks like James Bond. You say in your submission:

FraudWatch also performs Site Shutdown services on websites that are abusing brands online, not just for phishing, but the misuse of brand logos, brand names, implied association with brands and direct copy of websites.

And then you also have, on your website, a take-down.

Mr Youl—A one-time take-down.

Senator CAMERON—Is that a one-time take-down?

Mr Youl—Yes.

Senator CAMERON—If you are going to take a site down, what do you do to make sure that it is not a legitimate website?

Mr Youl—It is very easy to identify a phishing website—a website that is claiming to be a bank or another brand. We have processes for our staff to go through, and one of the processes is actually checking the Whois—who has registered that domain, that website. If we cannot say who it is because it is hidden, that could be one red flag to go, 'Okay, maybe,' in comparing that to our clients. Basically our clients will enter into a contract with us and, as part of that initial set-up of a client, we will be looking at their legitimate websites, their legitimate Whois information so that we can easily match.

As far as the brand abuse information and brand abuse type websites are concerned, where we do take websites down—and we have taken a range of websites down that even have a logo that is exactly the same, a direct copy, or has a slight modification. We have even seen examples where a complete website has been copied and just the name changed, but the people who copied it have left imprints within the source code to show that it was a direct copy. There are a range of processes that our staff will go through in verifying whether or not it is a legitimate website, whether it is a brand abuse related issue, and we will gather as much information with the brand abuse issues as we can from the client to then basically go and present that to either the domain registrar or the web host, wherever that might be hosted or registered.

Senator CAMERON—Do you have lawyers on your staff?

Mr Youl—No, we do not.

Senator CAMERON—Do you consult lawyers before you take action against some brand abuse websites—that you think are brand abuse?

Mr Youl—No.

Senator CAMERON—It is a bit of a vigilante operation to some extent, isn't it?

Mr Youl—There have been a number of sites where we will go back to our clients after we have reviewed it and had a look and we will say, 'No, we (a) don't think we're going to get anywhere or (b) don't think we can convince anyone that this is a genuine brand abuse issue.'

Senator CAMERON—Can I give you an example?

Mr Youl—Sure.

Senator CAMERON—Ugg boots. I live in the Blue Mountains, and there was a little company up there which had the name Ugg Boots, and they had about a 10- or 15-year dispute with an American company which had the name. They took legal action against it. What if this American company had contacted you guys and said, 'This is our brand; here is where we are; take these people down'? How do you know there is not that ongoing dispute? Is it just shoot first and ask questions later?

Mr Youl—No, it has never been shoot first. To be honest, we have never really encountered a situation like the one you described.

Senator CAMERON—But couldn't you? You could.

Mr Youl—We could potentially.

Senator CAMERON—So how would you deal with that?

Mr Youl—For us to take the action on the brand abuse issues, it needs to be a very clear-cut copy, and a recent copy, of the logos or that, or a recent website that has just gone up. Our clients will come to us if they have found it and say: 'We've seen this website. It has taken our logo. It is almost basically claiming to be us.' So we will then have a look at that and determine—

Senator CAMERON—I am nearly as worried about you guys as I am about some of these other issues!

Mr Youl—Sure. I understand. With the brand abuse science, it is something that is not a decision made on whether we do it or not taken by our—we have 24/7 staff working; it is not a decision they make. It goes up the ladder to make sure we do not take down sites we should not be.

Senator CAMERON—It goes up the ladder to you?

Mr Youl—In some cases it does.

Senator CAMERON—But you have more legal people employed? Who determines whether you are acting legally in relation to a brand? Because there arguments on brand abuse, on logos; people argue about them. But if you get contacted, how do you determine that this company you are acting for has the legal rights to the brand?

CHAIR—While you are—

Senator CAMERON—Just wait a minute please.

CHAIR—I am trying to add to the question.

Senator CAMERON—No, I would like this answered first before we go any further, please, Chair.

Mr Youl—Brand abuse is not something that we take lightly. The predominant things that we do are related to the phishing take downs. But what I would also say is with all of the take downs, be it with phishing or brand abuse websites, all we are doing is contacting the relevant people in abuse departments within web hosts, ISPs or domain registrars. We then present the information to them and it is up to them to take action. We are requesting them on behalf of our clients to have a look at that and take action if they believe they should.

Senator CAMERON—So you technically do not take the site down?

Mr Youl—Physically we cannot. We are just a third party. Any of our clients, if they had the resources, could do it themselves, it is just that we have built up the contacts. We are not physically going in and taking the sites down. In order to do that, we would need to hack into websites or do something illegal. Essentially, what we are doing is providing the information to the people who can take action, the web hosts who can suspend a website.

Senator CAMERON—You present a case, do you?

Mr Youl—Yes, we would present a case.

Senator CAMERON—Without any lawyers?

Mr Youl—Yes.

Senator CAMERON—Fair enough. It is not fair enough, I just do not understand it.

CHAIR—I have a further question following on from the Senator Cameron's. To the extent that it might be suggested you a vigilante outfit, that you take the law into your own hands, would you care to reflect on similarities not in that context between an organisation like yours and a union, for example?

Senator CAMERON—Come on!

CHAIR—Hear this out, Senator Cameron.

Senator CAMERON—This is a long bow.

CHAIR—No, I think not, hear this out. A union decides that what is happening at a particular workplace is not appropriate, so arguably it takes law into its own hands and organises the withdrawal—

Senator CAMERON—What a pathetic performance from the chair to do that.

CHAIR—Settle down, Senator Cameron.

Senator CAMERON—I just do not understand this.

CHAIR—I let you finish your question.

Senator CAMERON—God.

CHAIR—Yes, because you have not heard it yet. It organises withdrawal of labour and effectively black bans a workplace.

Senator CAMERON—Look at the *Hansard* on this one.

CHAIR—Ultimately a union and that activity is subject to the laws of our land, so you have to operate within that, but still is there not an analogy where a workplace can be black banned—

Senator CAMERON—That is the worse I have heard yet!

CHAIR—and labour withdrawn—that is, a site shutdown—by an organisation that may or may not be using legal advice in making a decision that it is appropriate that that workplace be black banned or shut down. Do you reckon there is some sort of an analogy?

Senator CAMERON—Mr Youl, you can take it on notice.

CHAIR—Can you hear my question over the rabble, Mr Youl?

Mr Youl—I can hear your question, and I can appreciate that. I apologise that I have not been extremely clear on what we actually do and the outcomes of—the distinction between what we do with a brand abuse website and with a phishing website.

CHAIR—Yes, because really the issue is the extent to which you shut things down yourself. You have to appeal to others to get that done, don't you? But you have also made the point that if the very people you are trying to help could help themselves and knew how to do it, they could do it themselves anyway.

Mr Youl—Correct.

CHAIR—Sorry, continue telling us about it. Senator Cameron is listening.

Mr Youl—Just to clarify: in particular it is phishing websites that are a direct copy of mainly financial institutions' internet banking login sites, it can be other online portals as well, which we work with. If it is a direct copy—mostly on a hacked website, sometimes on a newly registered domain that is registered that might be similar to a genuine website—in those cases we are trying to get that website taken down or blocked from public access, at least until the web

host or the domain registrar can review it in more detail. So in those cases we are looking to get the sites shutdown.

Brand abuse cases, if it is a very clear, direct abuse of the brand as far as a direct copy of the website, which might be similar to the issue of phishing but they may just have different motives—they might not be trying to get consumers login details, they might just be simply trying to say, 'Hey, we are this brand'—those cases are reasonably easy to ask the domain registrar or the web host to take that site down.

Where it is issues of logos or fonts or any other potential brand abuse issue, we are working for that to be remedied, for that to be removed. So if we are talking about a logo, that the logo might be removed or changed. And we have had success with that purely because the people who were using that knew that they were using it illegally. In those cases we are not looking to get the websites completely shut down. I probably was not very clear with that. We have had a number of cases come back with web hosts and they will come back and say, 'Look it is an issue.' Even domains that might be similar to a brand's domain, the domain registrar will come back and say, 'There's nothing more we can do; it needs to go through the proper legal process,' and we convey that to the clients. We are not looking specifically to get websites shutdown just because we do not like the picture that is on there or things like that. I just wanted to clarify that and I apologise for the—

CHAIR—No, that is part of what these exchanges are about.

Mr Youl—Sure.

CHAIR—As there are no further questions, thank you very much for your evidence, Mr Youl.

Proceedings suspended from 3.17 pm to 3.31 pm

BESGROVE, Mr Keith, First Assistant Secretary, Digital Economy Services, Department of Broadband, Communications and the Digital Economy

GAUGHAN, Assistant Commissioner Neil, National Manager, High Tech Crime Operations, Australian Federal Police

KELLY, Ms Wendy Anne, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department

McINTYRE, Mr Duncan, Assistant Secretary, Consumer Policy and Post, Department of Broadband, Communications and the Digital Economy

SHEEDY, Ms Joan, Assistant Secretary, Privacy and Freedom of Information Policy Branch, Department of the Prime Minister and Cabinet

SMITH, Ms Catherine Lucy, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department

WHOWELL, Mr Peter, Manager, Government Relations, Australian Federal Police

CHAIR—We welcome the Attorney-General's Department, the Federal Police, BCDE and the Department of the Prime Minister and Cabinet. Mr McIntyre, I believe Mr Besgrove is midair. Is that correct?

Mr McIntyre—Yes, he gives his apologies. He is hoping to be here while we are in session.

CHAIR—Thank you. Would any of you care to make a quick opening statement on behalf of your respective bodies?

Mr McIntyre—Yes, I will begin. The Department of Broadband, Communications and the Digital Economy welcomes the opportunity to appear before the committee. A key outcome for the department is supporting Australians to safely and securely realise the full potential of the digital economy, ensuring the availability and reliability to consumers and businesses of reasonably priced basic and essential communication services.

With the uptake of the internet exceeding 78 per cent of all Australian households, it is important that appropriate protections are in place for individuals in the online environment. The department acknowledges that online services and technologies are of enormous benefit to Australians. However, they also raise concerns for individuals in relation to security, safety and privacy.

The department's role in privacy policy is primarily in relation to telecommunications privacy through oversight of the Telecommunications Act 1997, the Spam Act 2003 and the Do Not Call Register Act 2006. These acts operate alongside the Privacy Act to provide more specific protections around the use and disclosure of personal information in the provision of telecommunications services.

Part 13 of the Telecommunications Act contains important provisions to protect the privacy of people using telecommunications services, including telephone services, the internet and telephone services over the internet. The act requires carriage service providers, including internet service providers, to protect the confidentiality of information that relates to the content of communications over the services, services supplied by the provider and the affairs and personal particulars of other persons. The act ensures carriage service providers are limited in how they can use and disclose such information.

The Spam and Do Not Call Register Acts were established to assist individuals to take control over how their private information is used for marketing purposes. The Spam Act sets up a regime in which recipients must opt in to receive commercial electronic messages such as e-mails, instant messages, SMS and MMS and prohibits the supply, acquisition or use of address harvesting software. The Do Not Call Register Act allows individuals to opt out of telemarketing phone calls and faxes by placing their number on the register.

The Australian Law Reform Commission's review of privacy law in 2008 made 34 recommendations relating to these three acts and telecommunications privacy more generally. The department has carriage of the telecommunications-specific recommendations and is responding to the report in two stages, with the telecommunications-specific parts to be responded to during stage 2. The department is currently in the process of reviewing the recommendations and is planning to undertake appropriate consultation to develop advice to the government to respond.

As part of this review, both the telecommunications and privacy acts were found by the ALRC to have a role to play in regulating privacy in the telecommunications industry. The Law Reform Commission came to this conclusion based on a number of key considerations, including that the telecommunications industry handles sensitive personal information, which includes information about when, how and with whom individuals communicate and the content of the communications. The ALRC concluded that it is therefore appropriate to continue to subject the handling of this information to the more stringent rules and penalties set out in part 13 of the Telecommunications Act in addition to those available in the Privacy Act.

In relation to new and emerging technologies in the telecommunications industry such as location based services, voice over IP and electronic number mapping, the ALRC recommended guidance be developed by the Australian Communications and Media Authority and the Office of the Privacy Commissioner to address new and emerging privacy issues.

Through the department's work in encouraging individual engagement in the digital economy and enabling access to the internet, the department is involved in a number of initiatives that provide education for individuals about privacy online, including cybersafety and cybersecurity issues. Emerging issues such as cloud computing continue to raise new privacy issues and the department continues to include these in its ongoing cybersafety efforts. Thank you.

CHAIR—Thank you. Mr McIntyre, before I invite Ms Smith to make her opening statement, a point of clarification: in terms of what could be regarded as online media, are there any that fall outside the department's purview?

Mr McIntyre—There are some specific provisions in the Privacy Act and other acts represented by people here that provide specific provisions, but the general issues associated with the information economy belong to my department.

CHAIR—Thank you. Ms Smith?

Ms Smith—Thank you for the opportunity for the Attorney-General's Department to appear before the committee today. I understand the committee is interested in data retention, so I will provide some background information in this area. I should say that no decision has been made by government about a data retention proposal.

First, I would like to provide the committee with the context within which data retention arises. Telecommunications data is information about the process of communication, as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details. It includes account identifying information collected by the carrier or the carriage service provider to establish an account. It includes information such as the time and date of the communication as well as the duration, location and type of communication. Telecommunications data does not disclose the content or substance of the communication, so no details of the contents of a text message or an email would be stored under any proposal.

Access to telecommunications data is currently governed by the Telecommunications (Interception and Access) Act 1979. The interception act allows access to telecommunications data that carriers and carriage service providers keep for business purposes such as billing and taxation. The ability to lawfully access telecommunications data held by carriers and carriage service providers is a vital tool for agencies in the investigation of serious and organised crime and the protection of national security.

The disclosure of telecommunications data can be authorised by a senior officer of a security agency, or any agency that enforces the criminal law or a law that imposes a pecuniary penalty, or an agency that protects the public revenue. This ranges from law enforcement agencies such as the Australian Federal Police to investigation agencies such as ASIC, Customs, ATO, ACCC and Centrelink. Agencies such as these utilise telecommunications data to ensure the integrity of financial markets, to protect Australian borders, to protect the public revenue and to enforce pecuniary penalties. Many of these investigative agencies rely heavily on telecommunications data as it is the most useful tool available to them in their investigations.

The legislation contains restrictions on both the access and use of telecommunications data. The restrictions reflect the interception act's focus on protecting the freedom to communicate, and protecting the privacy of parties who are not the subject of criminal investigations, while still facilitating investigations. Balancing these competing needs is a key role for government as public concern about the use of telecommunications data crystallises around privacy issues.

Having outlined the broad context in which the data retention proposal exists, I would like to provide the committee with an understanding of the importance of telecommunications data, and the rationale for the development of a data retention regime proposal in Australia.

Telecommunications data is an important investigative tool, as I have previously said. It can provide important leads for agencies, including evidence of connections and relationships within

larger associations over time, evidence of targets' movements and habits, a snapshot of events immediately before and after a crime, evidence to exclude people from suspicion, and evidence needed to obtain warrants for the more intrusive investigative techniques such as interception or access to content. Access to telecommunications data is one of the most efficient and cost-effective investigative tools available to law enforcement. There are no operational risks, and it raises fewer privacy concerns than the other covert investigative methods.

Targets of interest continue to utilise a wider range of the telecommunications services available, to communicate, and to coordinate, manage and commit crimes. The proliferation of new services and ways to communicate is impacting on agencies' opportunities to utilise telecommunications content. There are also ever-increasing levels of technology-enabled crime and cybercrime such as child exploitation and online fraud that can only be investigated by access to historical, internet based telecommunications data. These are some of the reasons for the increased reliance on telecommunications data by our investigative bodies.

Industry has acknowledged that, depending on the circumstances, telecommunications data can be as important as, or more important than, telecommunications content. However, despite the increased reliance on telecommunications data and the acknowledgement of the importance of telecommunications data, industry have confirmed that there will be changes to and reductions in the type of telecommunications data which will be retained into the future. They indicate that this is a natural evolution as a result of advances in technology and business models. For example, the telecommunications sector is quickly migrating from the traditional telephone network to internet protocol based networks.

Traditionally, telephony services retained detailed billing information on who called who, when and where, and the time of each call. Internet based service providers tend to charge on the quantity of data used rather than on a per call basis. Over time, as telecommunications services such as voice-telephone migrate to voice-over-internet based services, less and less information will be retained and stored. Therefore, this means that traditionally available telecommunications data—as: 'Person X called person Y at this time'—may no longer be available.

The development of a data retention proposal is intended to ensure a national and systematic approach is taken for the availability of telecommunications data for investigative purposes. Data retention would not give agencies new powers. It would ensure that existing investigative capabilities remained available. The interception act provides a high level of accountability and strict access requirements to obtain telecommunications information. These constraints recognise the responsibility of government to manage the competing interests of privacy and the expectations of the community that unlawful activity will be investigated and prosecuted, as well as the important role that the telecommunications industry plays in supporting law enforcement and investigative activities. Thank you.

CHAIR—Thank you very much, Ms Smith.

Senator CAMERON—Ms Smith, could you table that document? It is a very extensive opening statement and it would be handy if we could have it.

Ms Smith—Most certainly.

CHAIR—Thank you. Federal Police, do you have any opening statement?

Assistant Commissioner Gaughan—No thank you, Madam Chair; we are comfortable with what Attorney-General's had to say.

CHAIR—Thank you. Then let us have some questions.

Senator LUDLAM—Assistant Commissioner, maybe since you did not give us an opening statement I will direct my first questions to you.

Senator CAMERON—That'll teach you!

Senator LUDLAM—I am just wondering if you can first of all clear up some ambiguity, perhaps. I have a quote from you here that was in one of the submissions we received, which said:

… the regime revealed earlier this year would have little effect on how the AFP curbed crime.

That is very literally pulling you out of context. Can you just tell us what you meant by that and what your view is of the importance of as much as we know about the data retention regime.

Assistant Commissioner Gaughan—I think what I was trying to say there is that, as Catherine rightly pointed out, all we are asking for here is for the status quo to remain, and, if the status quo remains, the ability of the AFP to conduct its investigations will continue as it is today. If there are any changes, obviously that will have a significant impact, as Catherine rightly pointed out, on our ability to do investigations after the event and time.

Senator LUDLAM—What Ms Smith has just given us, I think, to paraphrase, is that you are not seeking greater powers over the way in which telecommunications intercepts are obtained, but what we are talking about is the collection of a vastly expanded volume of data of different kinds. So you would have the same powers that you currently have to investigate telecommunications data; there would be an enormous amount more there. Is that the right distinction to be drawing?

Ms Smith—No, that is not the correct distinction. In fact, the volume of information is already available in a lot of cases. What we are seeking is to get certainty from industry that they will retain in future practices the information that in many cases they already retain in their current practices.

Senator LUDLAM—That is directly contradicted by what industry has been able to put into the public domain—because I understand that their discussions so far have been confidential: that they do not currently retain these logs for years and years at a time, and there have been all kinds of costings about how much it would cost to retain this material. So I do not think it is true at all to say that these practices are extant already and we would just be formalising them.

Ms Kelly—I think there needs to be a distinction about what we are actually talking about here. We have had discussions with industry over a period of time to look at the data sets that may be put in place. The data set has changed over time. The first point I would like to make is

that all of the information that was in the original data sets has changed over time, so the current thinking around the data set has changed. But also, too, we did ask industry for information about the data that they currently retain, and we did receive some information back that indicated that the majority of the data was retained. The difference was the period for which the data was retained. It varied from days to years.

Senator LUDLAM—So you are seeking consistency, I suppose, right across the industry.

Ms Kelly—Correct.

Senator LUDLAM—Who else did you consult with apart from ISPs? I am just wondering why in your consultations so far—as far as I can tell the statement that you just read in, Ms Smith, probably doubles the sum total of public knowledge available about the proposal; thank you for that—there has been such a restrictive approach taken?

Ms Smith—We actually did consult with a broad range of people and have done so over some time within the industry. We have a list which I can table, which shows the extent to which we did seek people's interest in coming to speak to us or attending one of our sessions that we provided. We had two sessions in Sydney and Melbourne. However, before that time we were in contact with particular industry bodies. We did not limit our consultation to ISPs. In fact, a wide range of the carrier network was also consulted. We also sought to consult bodies like the Internet Industry Association, the Communications Alliance and the AMTA so that we got a feeling for their particular membership, which covers a very broad spectrum of the telecommunications industry. We consulted broadly with state and Commonwealth agencies and non-interception agencies like ASIC and ACCC and suchlike to get their views on what a proposal should look like as well. As I say, I am happy to table this. Many of these people received the discussion information through the Communications Alliance, who sought to go out to a broad range of membership.

Essentially, the department listens to industry views regularly. In fact, a day does not go by that we are not dealing with industry about some aspect of the legislation. Essentially, we consulted with a broad range whom we normally consult with, but we also went out much broader than that in this context. The normal people we consult with—this is sounding very convoluted; I apologise—

Senator LUDLAM—That is all right.

Ms Smith—are the main carriers, obviously, who have a lot of interest in law enforcement matters because they get a lot of requests from law enforcement. But we broadened it to the ISP industry because we believe the future is that ISPs will carry a lot more traffic than they have in the past, and so law enforcement will need to talk to them. We were very interested in their views. We also of course consulted with the Department of the Prime Minister and Cabinet, Ms Sheedy's privacy area and the Office of the Privacy Commissioner. It was very broad consultation within government and industry.

Senator LUDLAM—I would accept your definition of 'broad' if we were talking about a purely commercial proposition, but we seem to have inadvertently missed out all of civil society, the public and the parliament, and the industry participants that you did speak to were all bound

by confidentiality and could not say anything under these meetings. So it may be very broad, but it is a peculiar definition of broad in my book, in that there is no reliable information in the public domain apart from a document obtained under FOI that had been splattered with black felt marker. We will accept your tabling of the list of agencies and industry players that you did consult, but my definition of 'consultation' is evidently a little bit different to yours.

Could we come back to the Federal Police. Can you describe for us, obviously without giving away anything sensitive, some kinds of offences or a particular crime that you could not or cannot currently solve without access to the kind of material that we are discussing.

Assistant Commissioner Gaughan—It is in relation to the access of information we currently get. I will give you a prime example from the Operation Centurion, which was a child pornography investigation, to use the vernacular that is most common. Centurion was a 2008 investigation in which the AFP received a number of referrals in relation to a particular activity. All we received to commence our investigation with were a number of Australian IP, internet protocol, addresses. As a result of that investigation we were able to go back to the metadata and ascertain that there were a large number of Australians who were involved in possessing child abuse material, because the ISPs had retained that information, which enabled us to then take actions in progress. As a result of that we executed in excess of 340 search warrants, we arrested in excess of 140 people, we seized 400,000 images and, more importantly from my perspective, we actually saved four children who were potentially at risk from child abuse. Without that metadata being retained, the AFP cannot do those types of investigations because we will not have that information to backtrack.

I might add that not only does it impact upon the law enforcement ability of the AFP to exercise the right of the community to make them safe but it also has an impact on state and territory law enforcement agencies. Murder inquiries and things such as that rely on phone calls that have been made in the past, information that we can then use to track offenders, keep the context of what the victim has potentially undertaken et cetera. If we do not have that metadata then the possibility of progressing that investigation becomes quite limited.

Senator LUDLAM—Thank you for that. Again, these are the first concrete examples that we have had, so I appreciate that. Can I just draw a quick distinction. From a law enforcement perspective, ideally we would all be walking around with video cameras attached to ourselves. Is anybody at the table willing to acknowledge that there are very important privacy implications in, effectively, treating the entire Australian population as suspects in unknown or unprosecuted offences to retain that data just in case anyone of us at any given time turns out to be a child abuser? I would have thought that, in the light of this expansion of data to be retained, you would be talking to civil libertarians or privacy activists—take your pick. We come back to the question of why the consultation, if indeed this task is so worthy, has been so restricted.

Ms Smith—The consultation was for the purposes of developing a model, not to actually consult on a model. We were talking to people who understand the technology far better than we do and getting a real appreciation of what was viable, what they currently assist law enforcement national security with and what does not work. In fact as a result of that, as Ms Kelly said, the data set has changed.

I am more than happy to provide the committee with an in confidence version of the current data set, which is still a developing proposal. I am sorry; it obviously cannot be public, for the reason that it contains information that could be prejudicial to law enforcement investigations if it was released. What our consultation was for was to talk to both law enforcement and industry about what is needed into the future and what is viable under their systems in the future. It was not to actually consult them on a proposal that anyone was putting forward on data retention.

Senator LUDLAM—On behalf of the committee, if it is not inappropriate, can I accept the offer of a private briefing, if you are able to do so.

Ms Smith—Certainly.

Senator LUDLAM—At what point do you launch the public consultation phase, if not now?

Ms Smith—At the moment the department is considering the merits of a comparative data retention proposal. As I mentioned in my opening statement, no decision has been made on the process of details of any further proposal. The department is committed to an open, transparent and consultative approach acknowledging there is a very strong public interest in these issues, but decisions concerning the timing of any public consultations will be a matter for government.

Senator LUDLAM—All right.

CHAIR—Please give us clarification, Ms Smith. Were you seeking to go in camera now or were you offering to provide a confidential document or a briefing in future?

Ms Smith—I think, given the time, it is probably more appropriate that we have open questions now. We are more than happy to provide more briefing in camera at a later date or an actual briefing. We do have some information that we can give to you as well, but it has to be on an in-confidence basis.

CHAIR—That sounds good and sensible, so we will work with you outside this hearing on a future date for a briefing which may well be private. In terms of the information to hand, please provide that to the secretariat in appropriate course and appropriate form for us.

Ms Smith—Certainly.

CHAIR—It is best that we not look at confidential information today. Let us proceed publicly as you have suggested, if everyone is happy.

Senator CAMERON—Ms Smith, I might be a bit naive on this, but if you post a letter you would expect that letter to be private and not opened unless there was some police investigation or a reason to use the available laws to open the letter. I am really surprised that, according to Google's evidence this morning, emails are routinely scanned. Those emails are scanned by a software program that can extract not everything that is in the email but certain data in the email that allows them to decide what they need to do for advertising and the like. What is the difference between a letter and email?

Ms Smith—I am not an expert on the postal act, but I know a lot about telecommunications interception. The act protects a communication and there can be no access to that communication, an email, unless it is specified under the legislation. I cannot comment on Google's particular circumstances. I am not sure whether they do that scanning in Australia or the US; I was not here for their evidence.

Senator CAMERON—On that point, if they do it in Australia, would that be legal?

Ms Smith—No, it would be subject to the Telecommunications (Interception and Access) Act.

Senator CAMERON—What about if they do it in the US?

Ms Smith—I cannot comment because that would be potentially subject to US law.

Senator CAMERON—That is interesting.

Ms Smith—All I am saying is that I cannot comment on that because I am not aware of their actual technology. However, if they are doing certain things for network protection purposes, in that there are obviously—as you would all be well aware—a lot of cybercrime out there that mean that networks need to be protected, the interception and access act does provide for certain activities to be undertaken by system administrators for that purpose. So it may be that by software they will scan emails—not read them, look at them or do anything with them, but have some sort of the electronic scanning for that purpose.

Senator CAMERON—There was no evidence this morning that it was for anything other than commercial reasons. Could you take on notice whether that is legal under Australian law.

Ms Smith—Yes, we will review the evidence to see if we can do something on that.

Senator CAMERON—They put to us that you could opt out of this, but it is quite a complex thing to do. Maybe not so complex if you know how to do it, but finding out how to do it is a different matter. Would it be difficult to have a legislative change to make this type of activity subject to opt in if people want to do it? If a client of Google wanted to opt in to the scanning, would that require any changes to the law?

Ms Smith—At the moment the nature of the interception act is such that it requires for any reading of an email et cetera to happen within the act, except for law enforcement related to security purposes, that the parties to the communication must be aware something is being done. If it is the case that I have sent you an email, and we are both aware that our service provider looks at them because they have told us that, then arguably that could be. I am not providing any legal advice on that, obviously.

The interception act is very strict on what you can and cannot do, but you would know better than I how easy it would be to change legislation. The reality is that I am not quite sure what they are going to do, so I do not know whether it is currently in breach of the act.

Senator CAMERON—When you say 'reading', is there a definition of reading?

Ms Smith—No, there is not. Reading is not actually mentioned in the legislation.

Senator CAMERON—I just wondered, because they argued that it was a scanning type software program that just goes in. They say they do not know what is in the email, but people do not know what is going on. I think the new android telephones rely on a google.com service to be part of the actual telephone before the telephone can use all its features. I just wonder what the implications are there and whether there is some scanning going on there as well?

Ms Smith—As you suggested, I am more than happy to take that issue on notice. My colleague from the department of broadband may have a better idea on what is allowed as far as requiring services to be on phones. I am not really sure. All I can talk about—

Senator CAMERON—I am not a technical expert by any stretch—

Ms Smith—Nor am I.

Senator CAMERON—So could I ask you to have a look and see whether I am completely off beam about this requirement to have a Google email address if you use an android phone, which is the cutting edge new phone that is coming out?

Ms Smith—There you go, I just learnt something—I did not know that. I will certainly take that on notice.

CHAIR—If reading is not defined, what is the closest terminology to that? Is it 'viewed', 'accessed', 'would not be published' or 'scanned'? What is it?

Ms Smith—The act talks about listening—

CHAIR—Perhaps you could come back—

Ms Smith—There is a clear definition in the legislation.

Senator CAMERON—I am also aware of the assistant commissioner's view that there needs to be some balance between law enforcement and privacy. But it seems to me that what normally happens is privacy gives way to law enforcement, and I think there is a lot of concern that we just try to get that balance right. Have you got any view on that?

Assistant Commissioner Gaughan—I think you are right, there needs to be a balance. Ultimately, that balance will be determined by the parliament. I hear the concerns of the privacy groups in relation to the fact that law enforcement has access to data that, potentially, they think we should not have. But we need to weigh that up in relation to the public good. As I have said, if we do not have access to that type of information, certain types of investigations will not be able to be undertaken. Obviously, the parliament has given the AFP and state and territory law enforcement agencies powers to investigate those types of crimes and we need the tools to enable us to be able to do that.

Ms Smith—I can just respond to that earlier question. Interception of communications is actually defined in section 6 of the interception legislation as being:

… listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

Senator CAMERON—So it is listening—

CHAIR—Or recording by any means.

Ms Smith—Or recording by any means.

Senator CAMERON—So electronic scanning would be recording by any means, would it?

Ms Smith—I am not in a position to answer that question.

Senator CAMERON—Can you take that on notice?

Ms Smith—Certainly.

CHAIR—We need to stay abreast, don't we, Senator Cameron, if not ahead. What if the recordings were temporal—say, that the definition of recording was satisfied but the data or information was recorded for a period and then deleted. Would it still be captured by the legislation or for only so long as it exists? There are those sorts of issues that we need to think through given the sorts of evidence we have heard today.

Ms Smith—I think it would be more appropriate if I take that on notice, because the complexities of the telecommunications system are such that there are very many ways in which this is done. To give you a better answer that would be more useful to you I would like to take that on notice.

CHAIR—Okay. Are we doing too much in terms of the theme that I have been hammering a bit today—applying offline thinking to online behaviour?

Assistant Commissioner Gaughan—I will have a crack at that to start with. Our thinking needs to be different.

CHAIR—From what it is today?

Assistant Commissioner Gaughan—Correct. I think you made a point earlier about trying to get ahead of the game and that is what we need to try to do because if we currently stay where we are then basically we are paddling our feet and not actually catching up: we are going to continue to have these discussions moving forward whereas I think we need to try to get ahead. How we do that is a very good question.

CHAIR—Yes, how do we tool ourselves to do that?

Assistant Commissioner Gaughan—I know there is some work being done at the moment by the department in relation to the TI Act which I think will go some way to actually addressing some of those issues.

Ms Smith—The legislation is constantly under review. As soon as new technology comes out we are constantly looking at the act to see how appropriate it is to, firstly, provide appropriate protections and, secondly, appropriate access for law enforcement. We are looking at all the new technologies out there to ensure that the act still appropriately applies to those.

CHAIR—Are you staffed with enough nerds—and I mean that in an entirely complimentary way because we need such people?

Ms Smith—In this area we are very well resourced! We also get great assistance from the Australian Federal Police in offering us technical and operational advice.

Senator CAMERON—I said to myself, 'Don't go there'!

CHAIR—Who rushes in when Senator Cameron fears to tread! It's scary.

Senator CAMERON—So there is no nerd deficit in the department!

CHAIR—Thank you for your brave evidence, Assistant Commissioner. Would anyone at the table care to reflect on the suggestion by the journalist in the *Age*, Ian McIlwraith, that the biggest challenge for regulators—of which you guys are part and parcel because you are either doing it or assisting the government to formulate the policies to do just that—is not so much that the unscrupulous exist but that there is an industry that has sprung up to protect the identity of those who own and operate dubious websites. My first question is: have you seen evidence of that? Secondly, what should we be doing about it, if anything, given the flipside of protecting the privacy of individuals online. The argument being utilised by those who look after the dubious operators is that the dubious are entitled to their privacy—returning to one of Senator Ludlam's comments.

Assistant Commissioner Gaughan—There is no evidence that we have dubious content service providers—ISPs—operating in this country that I am aware of and certainly we have not been doing any investigations on those. It is probably a fair comment that some of those exist offshore and we work with our international partners as best we can to try to address those areas. Certainly I heard an earlier witness who was talking about phishing sites and the like and we work with our international partners to take those phishing sites down. We also work with the department of broadband and ACMA and others to assist with that endeavour.

CHAIR—Just pull up there. Senator Ludlam said earlier on in the day that they are everywhere but they are nowhere. So when you talk about 'here' and 'offshore' do you mean the physical location of those who own and operate?

Assistant Commissioner Gaughan—That is correct. Basically what we rely on there is the dubious ones being brought to our attention by either consumers in this country or offshore, and then we work with international agencies to bring those down. As I said, we work with the Australian Communications and Media Authority to assist with that process as well. The AFP last year assisted in taking down 70 phishing sites alone. That is an area of concern; probably more of an area at the moment is actually malicious software coming through. We work with partners both in the industry and other government agencies to address that, but there is certainly

no evidence of operators physically based in Australia that are undertaking the type of activity you refer to.

CHAIR—Any other views?

Ms Smith—I would just say that the premise of the interception legislation is that all communications and information about a communication are private, and that certainly is under the Telecommunications Act as well. The act provides that balance in giving law enforcement the powers to be able to investigate anyone of a dubious nature.

CHAIR—All right. Senator Ludlam?

Senator LUDLAM—I will start with something a little bit provocative. If this data is so important for law enforcement purposes, why have we ruled out the idea of including the conversations themselves and the web traffic and the material that you looked at, rather than just the header information? Why not just go the whole hog while we're at it?

Ms Smith—They are very different things. The actual content of the communication is a very thing to the information about a telecommunication call, and they are used for very different purposes within law enforcement agencies. It is critical investigation for a very broad range of investigations. The contents of communications are very important as well but for very serious crime. In essence, this has come to us because of the needs of law enforcement and the views of industry, and that is why we are looking at that particular proposal.

Senator LUDLAM—Surely, Assistant Commissioner, you could use all the data you could get.

Assistant Commissioner Gaughan—Yes.

Senator LUDLAM—Why not catch all this material rather than stripping all the personal stuff out?

Assistant Commissioner Gaughan—I think it gets down to one of the issues that Senator Cameron raised earlier about the balance of privacy versus the balance of law enforcement wanting access to the information. I think the balance is right as it stands at the moment. We get access to the metadata, that is what we have asked to be retained, and rightly so. If a law enforcement officer requires access to the actual content of the telecommunications, the emails et cetera, we go to a judicial officer with an affidavit and we obtain that information through a judicial process. I think that is the way it should be. There needs to be the balance, and I think that balance is accurate.

Senator LUDLAM—I am interested to know, Ms Smith, if you did not consult privacy experts or civil libertarians in the process you referred to before—not consultation; I forget the word that you used. You have asked the industry: what is possible? You have asked law enforcement: what do you need? But at no point do you seem to have asked anybody: is this a wise idea? How did you strike that balance?

Ms Smith—I certainly consulted on privacy in that we did consult privacy experts in the Office of the Privacy Commissioner and also in Ms Sheedy's branch in the Department of the Prime Minister and Cabinet.

Senator LUDLAM—The Privacy Commissioner was pretty uncomplimentary when we asked him about it this morning. I presume you are aware of that.

Ms Smith—I have viewed his evidence. I did not take that—

Ms Kelly—I thought he was more uncommittal rather than uncomplimentary.

Senator LUDLAM—Let us call him a data retention sceptic. I apologise for interrupting you.

Ms Smith—I would like to reiterate that we were consulting at that stage to come forward with a proposal which we have not yet developed. We are still looking at all of the options. To take something out to a broader range of people before we have a view, we thought was not appropriate. We take consultation at this point very seriously about getting our facts right and getting a very good understanding. But, as I said, we consulted at length with the Office of the Privacy Commissioner. I listened to the evidence this morning and thought that he was just noncommittal rather than anything else. I do not know if Ms Sheedy has anything to say.

Senator LUDLAM—I will not seek to verbal the commissioner either; he is not here to present his point of view now. In their submission the Internet Safety Institute—they have not appeared before us today, but their submission is on the committee's website—pointed out something that I think perhaps contradicts some of the positions you put this afternoon, and that is that the threshold tests for law enforcement agencies to gain access to online data versus offline data are currently quite inconsistent and out of balance. Could you clear that up for us. In my understanding, it is substantially easier to get a copy of an electronic document than it is for somebody to find out what is in my notebook. We have mentioned the Telecommunications (Interception and Access) Act a couple of times. We get amendments to that in parliament about every 20 minutes and I have not seen one yet that increased privacy protections for people; it always seems to be rolling out the other way. Assistant Commissioner, is it your understanding that it is accurate that law enforcement officers would find it quite a bit easier to obtain access to telecommunications records than they would to a physical piece of evidence?

Assistant Commissioner Gaughan—Yes.

Senator LUDLAM—So I am not sure why we keep hearing that it is stringent and that it is very difficult when, in fact, for the kinds of requests you would need to put forward, the bar is substantially lower for telecommunications.

Ms Kelly—I think you might find that access to a hard copy piece of paper also includes the content of that information, whereas access to telecommunications data under the telecommunications interception act is only the metadata—that is, the information about the communication—so you are getting less information.

Senator LUDLAM—You can get quite a bit further. If I am suspected of a serious crime you can pretty much have the entire contents of my Gmail, can't you?

Assistant Commissioner Gaughan—We would have to obtain a warrant.

Ms Smith—And it is a very high threshold, an extremely high threshold, for getting contents of communications.

CHAIR—Mr Besgrove, welcome and thank you joining us.

Mr Besgrove—I humbly apologise, on behalf of Qantas, for arriving late.

Senator LUDLAM—Assistant Commissioner, coming back to Operation Centurion that you mentioned before as case study A of how this data can be extremely valuable to law enforcement agencies, specifically what data did you use to put the case and prosecutions together? Was it web proxy logs, was it emails between offenders and, if so, was it just the metadata or the emails themselves, and were you mapping IPs to specific customers? I am interested in those sorts of second-order questions about what exactly it is that you need to put those kinds of prosecutions together.

Assistant Commissioner Gaughan—We will have to take that question on notice. I do not have that detailed information in front of me.

Senator LUDLAM—That is okay; I think that is appropriate. Can we get a 'where-to from here' from somebody. Ms Smith, have you been tasked to put a proposal or a set of options together to go to the Attorney and then a policy decision will be made at that level?

Ms Smith—Basically we are still considering the merits of any proposal and there has really been no decision made on where, how and if we will take this forward in what process. I do not have any particular instructions on where we are taking this at the moment. We are still gathering information.

Senator LUDLAM—That was not quite what my question was, but let us take it a step further back. Did you receive an instruction from the Attorney's office to investigate such a proposal or did the idea come from within the department or the AFP?

Ms Kelly—I think this issue has been around for a long time. There have also been international developments in this area. It has been in response to both advice from law enforcement and the industry in relation to changes to the retention of telecommunications data and the importance of the access to it.

Senator LUDLAM—That was not quite an answer either. It sounds like we are heading more towards it being a bottom-up initiative rather than a top-down one. Is that reasonable paraphrasing?

Ms Smith—It has been around for a very long time and I cannot actually recall where it began. We can take that on notice.

Senator LUDLAM—Presumably the Attorney-General did not wake up one day to find out that your office was investigating data retention. What is the cause and effect here?

Ms Smith—I think Ms Kelly's answer was exactly that. We were told very early on by industry that they may not be retaining this sort of information into the future. They told law enforcement that and, as a result, we immediately had a look at what was happening in industry and internationally as well. As I said to you, I do not have with me the timings and where it actually started, but I am happy to take that question on notice.

Senator LUDLAM—I would appreciate that. Perhaps this is a follow-up of what the assistant commissioner put to us before. When the industry came to you and said, 'We may not be retaining this data into the future,' that is interesting. What were they formerly retaining that they are proposing to no longer retain?

Ms Smith—In the good old days when we all had a fixed-line phone there was information kept about—for example, I called someone, their phone number, for how long, how much it cost, all that sort of information. Then I got a mobile phone and bought a contract which lets me have a few hundred dollars worth of calls a month. In those cases they do not retain exactly the same sort of information, and now I will be able to move to a new VoIP communication where they certainly will not have any of that sort of information retained for their billing purposes. That is essentially the kind of database that they gained this information from. They still create the information but for other purposes, for trafficking information.

Industry are very good in coming to us and giving forewarning on when technology is going to change that may have an effect on law enforcement's views. They are always wanting to make sure that we can keep pace with technology; they are very helpful in that respect. Given that they service a lot of requests from these particular databases, if those databases are not going to exist, they are moving into new technologies, they want to know if law enforcement will want access to the new technologies.

Senator LUDLAM—Okay, that is helpful. So it is more the phasing out of older technologies where we had certain kinds of recordkeeping—

Ms Smith—Correct.

Senator LUDLAM—will no longer exist. It is not that ISPs are moving to a system where they would no longer be retaining web server logs and that kind of stuff that they have always been doing.

Ms Smith—No.

Senator LUDLAM—Okay. I think that is a useful clarification. Finally, because I think we are approaching the end of the day, I have a question about the issue of the freedom of information request that came back drenched in black ink, and the comment that flowed from that, that the reduction had occurred to prevent premature and unnecessary debate. I think that phrases like that tend to inflame the situation, quite frankly, but when do you think it will be time for the necessary and appropriate debate?

Ms Kelly—Again I think that is a matter for the government to decide when there will be any public consultation on that. We are not really in a position to comment on that today.

Senator LUDLAM—But the government did not initiate this; it sounds as though the department did. That is an interesting shifting of responsibility. This was not a directive that came from a political level to investigate a set of technologies. It is coming from the other way.

Ms Kelly—We cannot publicly consult without the approval of the government.

Senator LUDLAM—You can quietly gather intelligence, I guess.

Ms Kelly—To date we have not been able to quietly gather intelligence on this issue.

Senator LUDLAM—We had to put a Senate inquiry referral through the Senate chamber, and media organisations had to put freedom of information requests about an issue that concerns every single Australian. In good faith, rumours flourish in a vacuum and you have created a vacuum. That is why people are saying, 'What is this about? It sounds important.' The way that it was put to me earlier in the day is, 'If you do not trust us to tell us about what it is that you are doing, why should we trust you to have all this data in the first place?' Maybe we will leave you with that to ponder. I have no other questions. Thanks, Chair.

CHAIR—Thank you, Senator. I have one further question in respect of advertisers essentially vacuuming for information that they can then use for marketing purposes. We heard evidence from the privacy commissioner and, if I understood correctly, the privacy commissioner said that the use of an ISP address was not within the purview of the Privacy Act. Do any of you have any comments to make on that sort of behaviour?

Ms Sheedy—Not so much on the behaviour but to clarify what Timothy Pilgrim was saying. The ISP address alone may not be personal information that is captured by the Privacy Act.

Ms Smith—Then that address is captured by both the Telecommunications Act and the telecommunications interception act. Depending on its use it may fall within the jurisdiction of the Telecommunications Act.

CHAIR—With what sort of consequences?

Mr McIntyre—It depends on for what purpose that information is being used. If it is an IP address and that is the only information then, if it is not being used for a purpose that is linked to an individual, it might not be covered by privacy legislation. But if it is being used for a purpose that links it directly to an individual then it might be captured by part 13 of the Telecommunications Act.

CHAIR—Yes, the consequences of which could be?

Mr McIntyre—The sanctions under that part of the act could apply but it depends on for what purpose it is being used.

Mr Besgrove—If I could elaborate further on that. At the moment most IP addresses are IPv4. As we move to what is called the internet protocol version 6, you move to an area where many IP addresses are actually attached to machines rather than to persons, that issue could actually become still more problematic.

CHAIR—If there is nothing else that anyone wants to add at this stage I thank everyone for their attendance, and I thank my colleagues. In wrapping up today's proceedings can I have a motion from a fellow member of the committee to accept any tabled documents and also to receive on a confidential basis the documentation tendered by Ms Smith. The committee has set 26 November for the return of answers to any questions on notice taken by witnesses here today.

Resolved (on motion by **Senator Ludlam**, seconded by **Senator Cameron**):

That, pursuant to the power conferred by section 2(2) of the Parliamentary Papers Act 1908, this committee authorises publication of the evidence given before it and submissions presented at public hearing this day.

Committee adjourned at 4.27 pm