COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

SENATE

ENVIRONMENT AND COMMUNICATIONS REFERENCES COMMITTEE

Reference: Protection of the privacy of Australians online

WEDNESDAY, 1 DECEMBER 2010

MELBOURNE

CONDITIONS OF DISTRIBUTION

This is an uncorrected proof of evidence taken before the committee. It is made available under the condition that it is recognised as such.

BY AUTHORITY OF THE SENATE

[PROOF COPY]

TO EXPEDITE DELIVERY, THIS TRANSCRIPT HAS NOT BEEN SUBEDITED

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

Wednesday, 1 December 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, Fifield, Forshaw, Furner, Hanson-Young, Heffernan, Humphries, Hurley, Hutchins, Johnston, Joyce, Kroger, Ian Macdonald, McEwen, McGauran, 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

BOOYAR, Ms Olya, General Manager, Content, Consumer and Citizen Division, Australian Communications and Media Authority 54

CLARKE, Dr Roger, Chair, Australian Privacy Foundation 1

CLARKE, Mr Trevor, Legal and Industrial Officer, Australian Council of Trade Unions 34

FETTER, Mr Joel, Policy and Industrial Director, Australian Council of Trade Unions 34

KELLY, Ms Wendy Anne, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department 47

KING-SIEM, Ms Georgia, Vice-President, Victorian Council for Civil Liberties (Liberty Victoria) 15

MILLER, Ms Kathryn, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, Law Institute of Victoria 23

O'LOUGHLIN, Ms Nerida, General Manager, Digital Economy Division, Australian Communications and Media Authority 54

RITTER, Ms Jonquil, Executive Manager, Citizen and Community Branch, Content, Consumer and Citizen Division, Australian Communications and Media Authority 54

SCOTT, Commander Alan, Manager, Melbourne Office, Australian Federal Police 47

SMITH, Ms Catherine Lucy, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department 47

WHOWELL, Mr Peter, Manager, Government Relations, Australian Federal Police 47

WRIGHT, Ms Andree, Executive Manager, Security Safety and e-Education Branch, Digital Economy Division, Australian Communications and Media Authority 54

Committee met at 11.09 am

CLARKE, Dr Roger, Chair, Australian Privacy Foundation

CHAIR (Senator Fisher)—Senator Cameron, we have Dr Clarke setting up in the room now. We have now opened the doors and it is public.

Senator CAMERON—That is fine. Just for the record, I have had correspondence from Google, who want me to go to their headquarters in Sydney to get a briefing on how Google operates. I just wanted that on the record.

CHAIR—Thank you. It is. I welcome everybody to the second day of hearings of the Senate Environment and Communications References Committee online privacy inquiry. It is the second day of public hearings.

Welcome, Dr Clarke. The proceedings today are public. It is an offence and indeed potentially in contempt of the Senate for anyone to attempt to interfere with evidence that would otherwise be given by a witness to this inquiry, as indeed it is for a witness to give false or misleading evidence. If at any stage you wish to give your evidence in private, make that request known to the committee, and the grounds for doing so, and we will consider it. I think that probably dispenses with the formalities.

Dr Clarke, we have your written material. Do you need to change anything in it before we kick off? Have you made any boo-boos you want to correct?

Dr Clarke—I would like to, in the flow, mention a couple of additional facets that are updates.

CHAIR—I will invite you to make an opening statement.

Dr Clarke—That is all.

CHAIR—As long as there are no errors or anything you want to fix up. I am also referring to the redacted version.

Dr Clarke—Yes.

CHAIR—Do you know what that word means? We are learning!

Dr Clarke—Yes.

CHAIR—It has lots of blacked out bits. So you do not wish to correct anything. Thank you. Then I invite you to make a brief opening statement before we fire some questions at you.

Dr Clarke—My apologies that there is a late submission to you, particularly one of considerable length. Originally we were a little unclear as to what the scope and primary focus of attention of this inquiry would be; therefore we sent a fairly short one in August dealing with four specific matters, which stand. We were concerned and remain concerned about those.

However, seeing the scope of the submissions from other parties, we thought it would be a good idea if we went rather further and provided you with a much more broad ranging approach. What I would like to do is to quickly pick out a couple of specific things as I work through at some speed and update a couple of matters here which were already out of date 24 hours after I submitted the document.

The point does need to be stressed all the time, without going through the philosophy of privacy, that it starts from a human rights perspective. A lot of the problems that have arisen historically over the last 20 years have been because organisations in both the public and the private sector have been seeking to reduce the privacy notion from a human right to an economic right. They have failed to appreciate the crucial role that privacy plays in trust—trust of organisations and trust of organisations' behaviours. This has undermined e-commerce and delayed e-commerce for many years. It has slowed down e-government very considerably. It has held up e-health dramatically during the last 10 to 15 years.

In that regard, one of the points of update is that yesterday Minister Roxon at a conference a short distance from here made statements that were very positive about the importance of privacy and trust in the personally controlled electronic health record initiative. It has been a great relief to us that that has finally been absorbed, because we have been unsuccessful for a decade in getting that through to the department of health and, more recently, NEHTA. We believe that much more progress could have been made. The Australian Privacy Foundation actually comprises people who are very positive about technology and who apply technology—we are not Luddites—therefore we want those positive approaches to be adopted. A common theme right through this submission is the inadequacies in consultation that have occurred across the board from governments and from the private sector and the harm that that has done and continues to do to progress in applications of technology.

Another quick point about privacy is that there is a preference by some US CEOs to pursue 'the privacy is dead' line and, further than that, to indicate that it is dead because the modern generation do not believe in it and have preferences of a different kind—they value things completely differently. I have submitted in here in some detail in background documents the counterargument. The counterargument, expressed very briefly, is this: young people of all generations have always been risk-takers, and as they have grown older and as they have accumulated more baggage—assets, liabilities, responsibilities and things to hide—they have become more risk averse. That has been a given across all generations.

The current generation, Y gens, 15- to 30-year-olds, have had some fairly bad experiences, particularly in Facebook contexts but more generally in social networking services. They are harming their job prospects. They are embarrassing themselves, sometimes quite seriously—beyond embarrassment. They are actually in a position where they are learning faster and absorbing the importance of privacy faster than previous generations did, because they are under greater threat by the modern technology that we are in. The result of that, we suggest, is that the young generation of today, the 15- to 30-year-old Y gens and the zero- to 15-year-old what I call 'I gens', will actually be more privacy sensitive than their predecessors. In other words, we would argue that there is a strong basis for concluding the complete opposite of what these US CEOs would like us to believe.

We think it is very important that that counterargument be much more evident in discussions. It has not been popular with the media. They have not published my quotations nearly as much as they have Scott McNealy's. I would be pleased if they would pick those meanings up and get them out there.

In response to your terms of reference, we have put together two sections which look at the private sector impacts and then at the public sector impacts. There is an enormous litany of these things, and it is of course not clear to me precisely which ones are going to be of greatest interest to you. I felt that I should just highlight a few of these on the way through in order to get something of the flavour.

One of the points we make at 2.2 on page 3 is that it is one thing to think about the cybercrime aspects of malbehaviour, malware and so on, but something that has to be appreciated is that these forms of malware and malbehaviour have become mainstreamed. Corporations do them as a matter of business. It is not just a question of people who would accept that they are conducting criminal behaviour. Corporations do these things. They have taken advantage of such things as web beacons, adware and spyware in order to take advantage of consumers and gather more data.

There are quite a range of specific technologies, which I have listed in section 2.2. I have tried to stress here that this is not comprehensive. There are a significant number of these elements that need to be looked at. Several of them are quite new. Even Firefox and Flash issues are really only during the 2009-10 period. They have to be analysed during that period. The last couple that I have there, the new forms of cookies and the emergent standard HTML5, are current 2010-11 issues which require deeper analysis to properly understand.

What these things have in common is that they are all part of this Web 2.0 philosophy. Web 2.0 has been trumpeted as being all about consumer excitement and delivery of additional services that consumers will love. That is not entirely untrue. However, it was invented by marketers; it was invented for the benefit of marketers; and it involves considerable intrusiveness into consumers' data and consumer behaviour. That has to be appreciated when we are looking at the impacts of these technologies.

I have also highlighted the critical risks that are involved in geolocation and provided some references to that. Because social networking services were specifically referred to in your terms of reference, I felt that we should provide a little information in that area. Depending on what you are interested in, there are many different directions in which you may want to drill down further. In this document I have only given some reasonably superficial analyses, but I have highlighted the way in which the business model of pretty much all social networking services, particularly the market leaders, hinges on having compelling content and, unlike their predecessor businesses, that content is not provided by the organisation itself. That compelling content is provided by individuals and, therefore, it is in the interests of the corporation to encourage, inveigle or trick individuals into disclosing information about themselves and about others—textual information, image or video. That provides a background to the sorts of things that the CEOs of these organisations say.

In both the Facebook approach and the Google approach, being market leaders coming from two different directions, the CEOs make the sorts of statements that serve the corporation's

interest. It is in their interest for privacy to be seen to be dead and for the old ideas of fair consumer terms to be thrown out the window because people are so excited by what they are doing. We believe this is a major source of problem for privacy in the online context.

I have included some brief information on behavioural targeting on the presumption that that will be an area of interest to the committee. I have also directly addressed Google's business model because, in the same way that we had to talk about Telstra when we talked about telecommunications in Australia over the last 20 years, the same thing occurs here. Google is wildly successful. It is not merely dominating markets, it has formed several of those markets and other people have to catch up to even play in the space. A mythology exists—encouraged by the corporation—that Google does not do evil. It is a complete myth. It is not actually a corporate motto and it has no binding impact on the corporation's strategy, and I have demonstrated that in several papers.

I have to quickly look at which of the bits of information that I have here are redacted and which bits are not. A key point I want to make about Google is: the Privacy Foundation has sought over an extended period of time to achieve engagement with government agencies, corporations and industry associations to get out ahead of emerging privacy problems. We have approached Google specifically on multiple occasions over the years, as have our corresponding international organisations and those from individual countries. Google has been resistant to that. We have had a successful meeting on one occasion two years ago, prior to Streetview's launch. The APF was able to identify a succession of aspects with their proposals that were going to be problems. They had some answers to maybe a third or half of them. Google, nonetheless, went live with the product they had at the time they consulted with us—that is, it was not a consultation; it was a briefing session. The media and the public got up and bit them for two-thirds of the points that we made in advance to them. The important point here is not that we are clever; the important point is that, if Google would come out and engage with privacy advocacy and human rights and consumer organisations as it develops new designs, it would be in a position to appreciate the issues that are going to come up with designs and that would at least ameliorate and possibly entirely avoid those privacy problems. That is a common theme through all of the things that we have to say here.

CHAIR—Dr Clarke, have you almost finished your opening statement, because we do have some questions we want to ask you?

Dr Clarke—I am getting close. The one point that I think is important for me to make beyond that is that we did not in this document address employment contexts and, having now read the ACTU submission, it is probably appropriate that we make a quick comment about that as well. Employment has not been appropriately addressed in privacy law in Australia, having been exempted from the Privacy Act. The whole area has been marked by an absence of consultation, not only with the privacy and human rights lobbies but with employee representatives as well. There were, prior to the online context, many problems in the balances that exist between employer power and employee rights.

The online environment has added a range of additional problems to that. One of the concerns the Privacy Foundation has been pursuing recently has been in universities. An increasing number of universities are forcing employees onto Gmail and forcing them to use Google Docs. Each of these has very substantial privacy implications because, in the absence of any

undertakings to the contrary, Google has access to all of that data, which includes personal data as well as corporate employee data. So far we have had very little success in getting progress, even with universities, whom you would have thought would have been the category of employers most attuned to these kinds of problems. That is why we picked on them first. So I would like to quickly highlight that the online context is a significant issue. I think that will probably—

CHAIR—Do? Good.

Dr Clarke—I think so, yes.

CHAIR—I will kick off, Dr Clarke. I have seen reference to some of the Australian Privacy Foundation's board members, but does it actually have members per se?

Dr Clarke—Yes, we do.

CHAIR—Who are they? And what is your membership charter? How do you get to be a member?

Dr Clarke—They are whoever chooses to fill in the membership form and agree to the objects of the association. As with most organisations, the objects are declared in the rules of incorporation, are up on the website and are part of the application form.

CHAIR—How many members do you have?

Dr Clarke—Like most organisations, we do not normally declare those numbers.

CHAIR—Many organisations do.

Dr Clarke—Okay. We do not.

CHAIR—Hundreds? Thousands?

Dr Clarke—We do not normally respond to those questions.

CHAIR—Exactly. It is private, of course.

Dr Clarke—For organisations not subject to privacy it is a different matter. Can I just clarify that there are two different forms of authority from which NGOs can speak. One is representative. An organisation that goes out and seeks widespread representation of membership from particular groups can claim representational authority. That is not the approach the APF takes. We have a membership base but we argue from a competency basis. We put evidence together. We put together evidence based research and make submissions to organisations, particularly to senate committees but also to industry association et cetera.

CHAIR—That was going to be my question. You have talked a lot in your submission about briefings versus consultations. I gather from what you have just said that you do not actually consult with your members on, for example, pulling together the couple of submissions that you

have given the committee. In pulling together the evidence, how do you get to express the views that you have expressed, for example, to this committee?

Dr Clarke—We have put together some scores of submissions on online privacy matters over the last 20 years. We have exposed these ideas on a range of lists. There is a privacy list which is continually active and to which posts are made and on which discussions occur. There is an internet policy watchers list called Link, which is a further source, particularly on the online context. We have exposed substantial segments of the arguments on both of those lists and had feedback from some dozens of people on these matters. I have had feedback in the last 48 hours.

CHAIR—Who are those dozens of people? Are they members, or are they people who chose to say stuff to you? Are they experts?

Dr Clarke—Some are members and some are subscribers to those lists. They are members of communities, because those lists are electronic community based. They are not just throw-together lists. Those communities have histories of 12 and 15 years. We also have people with a range of expertise, whom we use as reference points. The way in which we run the organisation is that we have the board, the subcommittees and the reference groups. The reference group notion is to enable people who do not want to have the public exposure to work with us and provide us with background information.

CHAIR—This is my final question around this: you are a not-for-profit organisation, so what do you do with the dough that people pay you to be members?

Senator CAMERON—On a point of order, Chair, I am not sure that this is a matter that comes under the terms of reference. Unless there is some real argument about why these issues should be continually raised with this witness, I think you should move on to the terms of reference.

CHAIR—Thank you, Deputy Chair. I would like to see the witness's answer to my question. I am just trying to get a sense of the Privacy Foundation, because I have not had witnesses from the Privacy Foundation before me in the past. So I ask Dr Clarke to answer the question as he sees fit.

Dr Clarke—Could I just get you to stress again what it is you are trying to find out with this particular—

CHAIR—You are a non-profit organisation, so I presume the membership subscription is utilised by your organisation to run the organisation without any excess. I presume that is what you do with it, but I am asking you—

Dr Clarke—That is how not-for-profits work.

CHAIR—Yes, I would have thought so.

Dr Clarke—We use it in various ways. We run an event every two to three years called the Big Brother Awards, which burns up money—not vast quantities, but we do not have vast

quantities to burn up. We use it on occasions for travel when we have to. We use it for the normal running of an organisation—filing fees and suchlike matters.

CHAIR—Thank you. I have one further question, but I have taken a fair bit of time, so I will go to Senator Ludlam and then I will go to Senator Cameron.

Senator LUDLAM—I will just finish on that thread. You folk, I presume, are largely a volunteer organisation.

Dr Clarke—Correct.

Senator LUDLAM—I am going to jump straight to the last part of your second submission, which was greatly appreciated. I noted the comments you made about not being sure of the direction in which the committee was going. This inquiry was not formed with particular ends in mind but, just because the field is so wide open, it is to get a sense of where the technology is and where the policy is going. You raise a lot of really serious issues in your submission. I want to bring you to page 12, where you have made some proposals, because, between the work that we are doing and the inquiry that I think the Senate finance and public administration committee are doing into the various bits of privacy law that are falling out, there is obviously a lot going on. Your first point is that there is a need for genuine privacy laws. You have made the case for how the laws that we have at the moment are not genuine, but what would genuine privacy laws look like? What are the teeth that we need?

Dr Clarke—At the moment there are no offences, there are no sanctions and there is no enforcement, because there is nothing to enforce. It is a law with principles and no teeth to it. The complaints-handling approach adopted by the Privacy Commissioner, and particularly the immediate preceding Privacy Commissioner, was to avoid even doing complaints investigations wherever possible. So there just is not any kind of control mechanism on organisations, public or private sector. That luxury that we had for a few years is long past. We have highly invasive technologies which need to be the subject of controls, and that means law rather than merely the pseudoregulation that self-regulation entails.

Senator LUDLAM—At the moment we have two sets of privacy principles that I think are really in the process of being merged into one. How has that worked in the recent past? What happens if you breach a principle?

Dr Clarke—Very little. An observation may be made. For example, recently the Privacy Commissioner found that Google had breached the Privacy Act in respect of Wi-Fi sampling, and the undertaking from Google was that they would not do it again. All of us take the attitude that we would like to be able to say that to the policeman who stops us for speeding, but that is actual law. There is actually a control mechanism on our bad speeding habits, but there does not appear to be any such control on corporations' bad privacy habits, and we are calling for real controls.

Senator LUDLAM—Presumably you are making or have made the submissions to that inquiry into privacy principles that are being rejigged. I will take you to your second point, a genuine transborder data protection law. We have been grappling a fair bit with the fact that the internet itself is by definition transborder. It is difficult to tell what law applies, and this is being

confronted at the moment with the WikiLeaks dumping of diplomatic cables. How do we pass law that applies in Australia to a medium that is so transborder?

Dr Clarke—There are separate approaches needed for two different contexts. One is where it is a clearly Australian organisation that is collecting the data, as is the case with all of the Australian government agencies and state and territory government agencies, as is the case with corporations that are operating in Australia. What we are proposing is that those organisations be responsible no matter where the data might be, and any breach that occurs is a breach by that corporation or that government agency and there should be sanctions. That is entirely within Australia's jurisdictional capability and the parliament has not seen fit as yet to do such things. We are arguing it should. The situation becomes more complex when we move to international providers, Facebook being a perfectly good example because you cannot find anyone in Australia to talk to. In those circumstances, what we have to do is to take such steps as we have power to do within our borders. We have to also work on multilateral arrangements around the world.

In the case of the Spam Act, there has been, firstly, law passed in Australia which is fairly effective in respect of Australian organisations that send out spam, and there has been some good l-a-w law applied and enforcement actions have actually occurred. For that to work worldwide, of course, there have to be multilateral arrangements. Other countries have to see fit to pass similar laws such that Australia can reach across oceans and encourage regulators in other countries to apply their laws. Is it easy? No, it is not. Is it something that this committee or the APF can wave a wand and fix? Certainly not, but unless we set out clear frameworks, unless we work out where the boundary is that organisations should not cross, unless we clean up our own act within this country, we cannot go lecturing the rest of the world. The Spam Act has actually provided a model for the rest of the world and is known for that.

Senator LUDLAM—It is helpful that at least we have one useful case study that has had a direct impact. You have addressed the government's data retention proposal here. It was put to us in our last hearing by the Attorney's office and by the Federal Police that the status quo will remain, that there is no expansion of what already exists. Could you talk us through, from your point of view, the difference between a phone company holding onto your phone records for your home landline, which the police can then access with a warrant, and what appears to be on the table now with the data retention proposal?

Dr Clarke—I am sorry, I am not going to be able to speak in detail about that. As you would imagine, with the range of issues that we have, we have different specialisations. That is an area that we have tended to work with Electronic Frontiers Australia on and their submission is much more telling. I note that one of the other submissions—it was the one from the Law Council of Australia, I believe—also addressed this.

Senator LUDLAM—The Law Institute of Victoria?

Dr Clarke—I beg your pardon—the Law Institute of Victoria.

Senator LUDLAM—They put a good submission in.

Dr Clarke—Yes. There is one general point I would make, however, and that is that the information that you are providing to me is new information to me. We have been unable to get a place at the table in discussions on this matter. The government will not consult with us. They will consult with industry; they will not consult with civil society. When I say 'us', there is no reason why the APF has to be chosen as one of the organisations that government agencies interact with if there are other alternative organisations that cross into the same space. Civil liberties organisations do; in other contexts, consumer organisations do. Our argument is that civil society is not being engaged, so I now have to go out and find the relevant part of *Hansard* and then chase to see whether there is a submission which provides that information in the public domain or whether it is one of the several confidential submissions that have been made. We just do not know what the proposition is.

Senator LUDLAM—Actually, the parliament has been left out of that dialogue as well. That was part of the reason for initiating this inquiry.

Senator CAMERON—Google made a submission to the inquiry and since then I have had a look at their privacy policy. Are you aware of Google's privacy policy?

Dr Clarke—I analysed it and compared it against the template in 2005 or 2006. I have only glanced at elements of it in subsequent times.

Senator CAMERON—It seems to me that it is becoming more and more the case that you need to sign up, whether you like it or not, to actually access some of the technology. Would that be a fair comment?

Dr Clarke—Yes. I should say yes and no, to be fair to Google. There are a range of facilities that are accessible without any form of login. There are a range of facilities that are only available if you log in, and in order to log in you must provide an email address—an email address which functions and which you have access to. To give an example of this, I am involved in a number of boards of organisations and a couple of those have considered using Google Docs. It is possible, with some difficulty, to put something up on Google Docs, such as a spreadsheet for shared purposes, and gain access to that without logging in. However, as soon as you try to follow one of the links within such a document you find you are challenged for a login. I for one do not have such a login. So yes, there is an entrapment technique built into the infrastructure.

Senator CAMERON—Would that be considered in general business to be acceptable? I know you cannot talk for business in general, but you have looked at privacy issues generally, outside of the internet. Would that be considered a reasonable proposition?

Dr Clarke—My day job is as an e-business consultant and I have been in the IT industry for 40 years, so I have actually looked at these issues on multiple occasions. To the extent that all suppliers in an industry have a common position, or set a common term, there is no choice left. Alternatively, to the extent that there is a monopolist in the industry or a highly dominant provider in an industry, then if that person has fixed terms and it is a condition of the delivery of service that you accept those terms, such as signing up using a login ID, you are stuck with it. Quite when the law steps in and says, 'This is unconscionable,' is a matter for the courts, a complex matter and not something that many of us are ever in a position to litigate.

Unfortunately, the funds that the APF has at its disposal are insufficient to pursue test cases of that nature.

Senator CAMERON—I understand that there has been some report that litigation took place in the US against Google on privacy issues. This is about the scanning and monitoring of emails. Can you provide us any information on what the outcome of this litigation in the US was?

Dr Clarke—There have been several instances where both Google and Facebook have been found to have been, shall we say—I have to be careful how I phrase this because my memory is vague. They took sufficiently seriously the accusations that were levelled against them, but they chose to enter into a settlement rather than proceed through court cases. They settled for sums of money that to non-government organisations would be significant. It would provide funding that would enable much more research and much more representation of the public interest to be done if figures like US$9 million were available. But they were numbers which were utterly insignificant to a corporation the size of Google. Several of those instances have occurred, but it is a case-by-case answer that I would have to give you in order to be specific, and I certainly cannot do that on the fly, I am sorry.

Senator CAMERON—Google's privacy policy says that they adhere to the US safe harbour privacy principles of notice, choice, onward transfer, security, data integrity, access and enforcement and is registered with the US Department of Commerce's safe harbour program. That sounds pretty good. Should we have some confidence in that?

Dr Clarke—Yes, it does sound pretty good, because it was designed to sound pretty good, and no, you should not have any confidence in it. The safe harbour agreement was the result of a long barney between the European Union and the United States because US law could not satisfy the adequacy requirements of the EU directive. Eventually, not to put too fine a point on it, the EU squibbed and accepted somewhere between half and five-eighths of the EU standards as being sufficient—but without the effective enforcement mechanisms.

The US has actually tried to ratchet the standards down even further than their current five-eighths by coming up with an APEC Privacy Framework. They endeavoured to use the very low regard that privacy is held in in East Asian cultures as a means of coming up with an alternative privacy framework and sets of principles which would be even weaker than their own FTC-administered scheme. Fortunately it has not taken much hold anywhere and nobody takes it very seriously, but this has been a standard approach within the United States because the US values freedoms of corporations to make money extremely highly and, where necessary, values those above consumer rights.

Senator CAMERON—They also say in their privacy centre that you can use Google Dashboard to review and control the information stored in your Google account. Should we be confident that that is a protection for information?

Dr Clarke—There are a couple of different facets here, and I must say that, not being a person with a Google login ID, I do not have personal experience of Dashboard; I have had to rely on second-hand information about it. There are a couple of threat models, as people say in security analysis. One threat is other people and the second threat is the second-party threat that is Google itself. There are serious limitations on how much control you can achieve through

Dashboard or any other means in order to protect yourself against Google. My understanding is that there are some settings of some value and some relevance to privacy in Dashboard. We should be clear about this: we kept caning Google, but there are some facets here and there which are done in ways that we would give ticks to if we could sit down and have meaningful consultative discussions with them. So we would think that there are some features of Dashboard that are quite good, and hopefully Facebook has by now learnt a little bit from this, because Facebook has been the complete opposite until very recently and has scattered their parameter settings all over the place so that it was impossible for a normal human being to exercise any kind of control. It is still not good, but at least Facebook has moved a little bit in that direction of providing a bit of coherent control by individuals, particularly in respect of the threat from third parties.

Senator CAMERON—What I am worried about is the new Android phones. You really need a Google account before you can access the new technological advances in these telephones, and it seems to me that there is more and more control being exercised by—I am not just picking on Google here—companies like Google in terms of breaches of privacy and demands for access that just would not have been considered appropriate in years gone by.

Dr Clarke—Yes, we certainly share such concerns. I have not looked ahead in this document that we have prepared for you, because there is too much present to address without looking forwards, but the iPhone and iPad developments, the lockdown nature of the device and the very strong control that Apple seeks to exercise over its users is a source of serious concern. Google is far from the only organisation that creates privacy concern in the online world. There is hope for a degree of competition in the smartphone environment such that the devices that consumers are going to be using are going to be sufficiently rich and diverse that some of them will be better protected than others. Some of them will have fewer demands for exposure of identity and exposure of location as a condition of doing business. But, unfortunately, the Google model is being copied by a range of organisations because they perceive Google's massive control over personal data to be a major source of corporate benefit. Therefore these other organisations are copying those aspects of the business model and therefore also demanding identity and location.

Senator CAMERON—But what is the legislature doing? We have the problem that—

CHAIR—Senator Cameron, can you bring it to a close.

Senator CAMERON—This is my last question. We as legislators have the problem that, when we have to deal with the banking industry, there is the argument of 'too big to fail'. In relation to these online companies, it seems to me that they are too powerful to regulate in some aspects. Is that a fair observation or am I being too alarmist?

Dr Clarke—I would be very concerned if the parliament of Australia were to take that attitude. If we have reached the point where corporations or megacorps—call them what you will from science fiction—are actually ruling national governments of the size of Australia, a member of the G10 or the G20 or whatever we are, then parliament has thrown its hands in the air and we will be permitting an awful lot of misbehaviour by corporations in the future. I do not believe we have reached that point. That is a political judgment, clearly—one for the parliament, not the APF or me, to make. But the APF's position is that we should not be wasting our time by

coming to committees like this and making submissions for changes to law, because parliament continues to have considerable power.

Google has a substantial footprint in Australia. Google performs many acts in Australia as well as performing many acts about Australians in other locations. There are many things that Google does that are subject to direct controls. Facebook is a slightly different problem, I acknowledge. So I do believe that the parliament should be continuing to take action and should not let itself be sucked into this thinking about it being too large to be regulated.

Senator TROETH—Dr Clarke, in your submission you have noted the importance of encouraging a lifelong respect for privacy among young people, and obviously they do have this tension between controlling their privacy and being part of a social network that all their friends are on. So how can we, as either a government or a community, encourage them to consider privacy—given that social networking is everywhere?

Dr Clarke—Social networking does not need to require people to expose themselves to everyone. The notion of groups of friends is how we normally operated. The attitude of the current generation is that those groups are somewhat more fluid, somewhat wider and somewhat less bound by space than in my generation. But that does not mean to say that groups of friends has ceased to be a notion.

One of the early mistakes that were made—in this case, by Google Buzz when it was released earlier this year—was to make an assumption that everybody that a person dealt with had an interest in having contact with everybody else that the same person had dealt with. This is blatant nonsense because your previous-employer, current-employer and future-employer circles of friends are commonly quite distinct—and need to be kept quite distinct, for a range of reasons. That leaves aside all the different social groups that people belong to. They overlap, but they are not the same thing and they do not merge.

So I think that what we have to do is to ensure that organisations who are providing these sorts of services consult, via focus groups with their consumers, and with advocacy organisations—consumer, human rights and privacy organisations—to gain a feel for what the reasonable expectations of behaviour are of these corporations. In other words, a lot of the projection, I believe, by parliament should be in that direction and, similarly, to the public, conveying these models that match to the way in which human beings operate.

Senator TROETH—As to current government education in the online environment, is it adequate and effective at the moment?

Dr Clarke—Most real education that occurs is by peers, because this is moving so quickly that old people like me are not going to be in a position to educate them. Despite the fact that I have been a university lecturer for 15 or 20 years, I am not going to be in a position to lecture to a first-year university class, and still less to the newbies who are 10 and 12. It is their peers that they look to. So it is about the kinds of features that are available and the way in which those features are used by the people seen by peers as being the smart ones—the leaders within the peer group. That is where the leadership needs to come from. That is why I stress this need for appropriate features in products, because if you make those features available then ‘the street finds its uses for things’—that is the expression commonly used. The young people will learn

and learn quickly, and they have shown signs of learning. That was a point I made in this submission—that the under-15s are much more savvy than the 15-to-30s, because they have seen what happens and they internalised it very quickly.

Senator TROETH—So peer education is of more use than government regulation, you would say?

Dr Clarke—Government support for facilitation of pressure on suppliers to consult and to understand, and to provide features that are suitable for young people—that is the direction, I think, in which government can achieve most leverage and success.

Senator TROETH—Thank you.

CHAIR—Dr Clarke, I have one final question. You refer—in your supplementary submission, I think; I have lost track—to the National Broadband Network and express concerns about what you say is the government's proposed temporary control of the internet backbone and distribution network. You say attempts may be made to embed surveillance infrastructure into the network. Do you have any evidence upon which you are basing those concerns?

Dr Clarke—Once again, we have endeavoured to get evidence one way or the other, and once again, despite our representations to NBN Co., we have been unable to get a dialogue. If I can just declare a position here, as an e-business consultant separately from the APF, I am extremely supportive of the intent and general directions of the NBN initiative. I have participated in other roles in a number of activities related to the emergence of the NBN over the last two to three years. I saw it as my function to raise policy issues, consumer protection matters and privacy matters as part of those discussions. I have put documents in front of the NBN Co. and was unable to stir them into giving any kind of response or involving civil society in any discussions. So I have actually sought evidence, and there are a series of things in the document that I provided—which is a personal document, not an APF policy statement—to do with identity, location, content surveillance and so on. It is feasible for an NBN Co., particularly with a government bidding it to do so, to build surveillance capabilities into the network. I am certainly not making accusations that they are doing so. I would like there to be a dialogue so that NBN Co. are aware of what the policy concerns are and are in a position to say, 'We can give you ironclad assurances that none of those four things you're worried about is being done.'

CHAIR—Are you, in a sense, saying it would make sense to do so but then there should be discussion about the protections to be built around in a privacy sense?

Dr Clarke—We would be very concerned if there were any attempts to build surveillance into the network. It is infrastructure of a fundamental kind. In the same way that building in a need to identify yourself when you drive down a toll road undermines the longstanding freedoms of movement, building surveillance technologies into this kind of infrastructure represents an undermining—

CHAIR—Yet we do it with the tollways, don't we?

Dr Clarke—And we continue to challenge it and to ask human rights commissioners and parliaments to impose a requirement for anonymous payment mechanisms on tollways.

CHAIR—Thanks, Dr Clarke. Your evidence has been valuable. I refer to your comment earlier on expressing, I guess, some frustration about wasting time appearing before committees like this. I for one do not regard your evidence as a waste of time. You can reflect on how you spend your time, but I would put it back to you that it is not a waste.

Senator CAMERON—I would just like to clarify one issue, because I may want to ask other witnesses about this. Was it ASEAN that you said had the lower standards for privacy?

Dr Clarke—The context in which that work was done was APEC.

Senator CAMERON—Thanks.

CHAIR—Thanks, Dr Clarke.

[11.58 am]

KING-SIEM, Ms Georgia, Vice-President, Victorian Council for Civil Liberties (Liberty Victoria)

CHAIR—Ms King-Siem, I think you were in the room when I expressed the formalities to Dr Clarke, so I do not need to do that again.

Ms King-Siem—No, that is quite right; I was here.

CHAIR—Thank you. We do not have a submission from you. Do you want to make a brief opening statement before we ask you questions?

Ms King-Siem—I can do so. It will necessarily be brief.

CHAIR—Good.

Ms King-Siem—I think I said earlier to the secretariat that Liberty Victoria is also a voluntary and non-profit organisation, which means our resources are a little bit thin. It is not because we do not believe that this is an incredibly important issue—I think it is an absolutely essential issue of discussion—but we were not in a position to put together a written submission before the required dates.

CHAIR—Okay. We value you as a thin resource!

Ms King-Siem—I have been overseas for the last six months, so I am not up to date on all the latest happenings, but I will do my best. Please forgive me for any areas that I am not as au fait over as I should be. I suppose the first and most important element is that we believe that privacy is a fundamental human right. It is recognised under article 17 of the ICCPR. We do not believe that it is adequately protected in Australia. There is what I would term a patchwork of legislative protections that we have. For instance, in our federal Privacy Act there is an exemption for small business. Small business is, going on the Victorian Privacy Commissioner's submission, approximately 95 per cent of business in Australia, which means that 95 per cent of business is not subject to privacy regulation. There are employee information exemptions. All this adds up to what we feel is a less than adequate privacy regime in Australia.

The issue of online interactions is a particularly problematic one, as I am sure the committee is aware. Because you are dealing with multiple jurisdictions, it is a really difficult one for any one jurisdiction to grapple with effectively. Presumably, that is why we need greater international cooperation. A starting point would be, and Australia is a signatory to, the ICCPR, yet we have not actually brought in our own protections to an adequate level. I would second Dr Clarke's comment that unless we pull our own socks up it is very hard to point to others to do the same.

In general, in lieu of having our own written submission I have had a quick read through a couple of the submissions already put. I would say that Liberty could endorse the submissions of the Office of the Victorian Privacy Commissioner, the Law Institute of Victoria, the Australian

Privacy Foundation and, probably, Electronic Frontiers Australia as well. Unfortunately, my time has been limited, so I really only picked the major ones that I could find and read through them. I am still halfway through the submissions of the federal Privacy Commissioner and the Information Commissioner.

I will take a step back. In terms of online issues, I think they can perhaps be split in two. The first is where consumers choose to make an online interaction—for instance, they look something up on the web, they use email or whatever it is that they are doing. Then there is the secondary online interaction, which is where the information is used without their direct knowledge. That is where a business has information which goes backwards and forwards or it is a transaction which is secondary to their primary transaction, which involves being online as well—the internet. Care should be taken to recognise both of those.

It should be realised that even education will not deal with the second one. I take Dr Clarke's comments about the youth of today being really quite internet savvy, but they are not aware of half of what is going on with the information around them, with interactions they have with businesses that then go on to use that information in other ways. That is where, presumably, government has a real role to play and should be supporting, rather than taking a prescriptive attitude to what information is out there. A general right to privacy, for instance, would put the power back into the hands of Australians. In a lot of cases they probably would not have the wherewithal to take action directly, but at least it puts it back in their hands and it means that they can enforce their rights against whoever is infringing them, be that a corporation, another individual or any other sort of person. At the moment our legislative regime does not really provide for that at all.

I would also second a lot of the comments in the written submissions about the idea of consent being a bit of a furphy. A lot of the time consent is required, or information is required, before a transaction can occur. A lot of the time, again, there is the idea that you can have an anonymous transaction, which is in line with what will become the Australian Privacy Principles—or pseudo-anonymity—and it does not exist. Take, for instance, Facebook as a good example of that. You are required to give your real name to have an account, yet how this is actually relevant to your interaction on there is not that clear.

This also goes to the idea of the proposal for widespread collection by the government of data by users. Again, why is that information required? It seems a slightly unrealistic act, to be honest, and very much a paternalistic approach to it. I understand security issues, but this is where you take a targeted approach where there is a justification and reasonable suspicion that that information is required, not collect information and worry about it later. I think there is a tendency both at government and at corporate level—and in fact it is perhaps just a natural tendency—to collect more than you need and then swallow it later. Corporations are guilty of that all the time. Even other people collect a lot more information than they necessarily need; it may prove useful later on. Until you have adequate privacy protections, that information can be sold off and used in other ways.

I would also pick up and use as an example even something like WikiLeaks. That is an example of what was considered to be secure data getting out to the public sphere. You can argue about whether it is a public good or not, but the reality is that that information was considered to be secure. In the same way that there is an argument that all this data that is going to be collected

by government under this proposal will be kept secure, I suspect the security measures will be fewer than those afforded to the US Department of State, and it is more than foreseeable that that sort of information could be sold off—not necessarily deliberately by government, but information has a way of reappearing out there at a later date. Again, this is a classic example of where you really want to be careful about what information you collect, because then you really should be responsible for it, and that can come back to bite you later on.

Also, I want to pick up on the comment about smartphones. I would probably go along with the Android comment. I have an Android phone. I put applications on it. Every time I put a new application on, it gives a huge list of all the things that it will be collecting about me and using. Most of those have got nothing to do with the application that I actually downloaded or the purpose for which I downloaded it. The only way I can install and use it is to agree that it can wake my phone up when it wants, take my network data and my contact list and use them, even though it will not be a gain. Increasingly you see this sort of thing, and where there is no strong privacy regulation you will continue to see this. That is what a natural market will do. Corporations will exploit where there is a possible market, and of course there is one. This information has a value, so of course you would expect corporations to be taking advantage of it.

CHAIR—Can we ask some questions?

Ms King-Siem—Certainly.

CHAIR—You are saying way too much interesting stuff! Are you saying that it is not possible in the online world for consent to be properly—however you define 'properly'—given? In answering that, can you reflect also on the example of when you go to a doctor or a specialist and you sign the form that says 'yes, you can use this information'. I would suggest to you that many people, like me, do not necessarily read that, but know that it is the price of seeking that expert opinion or getting that expert service. No. 1, is it ever possible to provide consent in the online world? No. 2, how is it any different from the offline world and the things that we all accept and do currently?

Ms King-Siem—I will answer the second part first. That is dealing with the difference, perhaps, in your example of going to see a doctor. That case is governed under the Health Records Act in Victoria, and there are very prescriptive requirements about what can be done with that data. That does not exist in the online world. So that is the major difference. To deal with the first part—

CHAIR—That is after the event. So that is your separate point about how, once you have that information, you must be responsible with it. But the nature of the consent itself—

Ms King-Siem—That is what I am coming to.

CHAIR—Sorry, I should have let you finish.

Ms King-Siem—All I am saying is that with the second part, the difference between the two, there is a regulatory regime which deals with data within the one jurisdiction, so it makes it a lot easier to deal with. When you are dealing with online you are dealing with multiple jurisdictions, and enforcement is therefore that much more problematic.

CHAIR—Is that your answer?

Ms King-Siem—It is the answer for the second part of your question, which was the difference between an online interaction and a traditional interaction that you would have down the street with your doctor or—

CHAIR—Okay. Then your answer to the first bit—

Ms King-Siem—I have not dealt with that bit yet—that is, can you actually have informed consent and free consent in that case? Yes, I think it is possible, but you have to be wary about blithely saying there has been open and informed consent to it, where in fact there may not have been. Where you have no other choice for that service, as a condition of service a lot of the time that is not what I would call 'consent' in a free and open manner. Where you have a choice of providers, then if you do not like the terms and conditions offered by one you can go to another, as you would in a normal marketplace. Where you do not have that choice or where that information is deemed to be essential but is not, I would argue there is not the same level of consent. So, yes, I do believe it is possible to have consent—

CHAIR—In the online world?

Ms King-Siem—Yes, in the online world, but I think it is far too freely 'bartered' around. That is a term where organisations will say that there is consent and that there is information. I will use Facebook as a well-known example, but not because I am that familiar with their terms and conditions, so I may be wrong in part here. In order to have that account, if you wish to interact with 95 per cent of your friends who are on there then you are consenting to an awful lot of things being done with your data and you do not necessarily know what is happening with it.

CHAIR—I might ask you to take on notice, then, my question about this issue, then I have one more question. In answering the first bit and the second bit you have identified two factors at the very least that might influence a person's giving of consent, which is the nub of it. You have said in the doctor example that in Victoria there are enforcement and protection things. I would question whether the individual when giving that consent actually thinks about that, even if they are aware. Secondly, you have also identified an array of choices. So they are two factors that you would argue make it different.

Ms King-Siem—Can I clarify a point there. When I was dealing with the issue of the difference between an online interaction and one down the street, I was not dealing with the issue of consent. You asked how the interaction was different, and I was—

CHAIR—Okay.

Ms King-Siem—Sorry, I misunderstood.

CHAIR—Then maybe take that on notice, because I have taken up a fair bit of time. If you have anything to add, how is the notion of consent different? Sorry—poor phraseology.

The final area of my quick questioning is about you referring to small business and employees. The ACTU give their views on this issue in their submission, but they do say that

there is no basis for employers to monitor the personal communications of employees on their personal equipment outside of work hours. Even if you agree with that statement, which many may, where do you then draw the boundaries before that? Or do you draw the boundaries at that?

Ms King-Siem—First I should start with the disclaimer that I have not seen the submission. But my initial thought is that that is actually a very difficult issue because you are often dealing with the same devices used for personal and for business communications, and drawing a line between those two is going to be quite difficult a lot of the time. I can see that an employer might argue that, particularly where it is an issue which could come to the security of the device or the information held on the device, they then have a vested interest in seeing the nature of communications that are used otherwise on that. For instance, if an employee is sending off a personal email with attachments including a spreadsheet of the organisation's database, that is obviously no longer just the realm of a personal use, because it is in breach of their terms of employment.

I do recognise that that is a difficult issue. That is not to say that I do not agree with the in-principle idea that what you do in your own time should be a private affair—absolutely. But I do recognise that it is a difficult issue, given the increasing interplay between private and business interactions, devices and communications.

CHAIR—Thank you.

Senator LUDLAM—Thank you for coming in. I will pick up on the distinction you drew right at the beginning of your evidence. You drew a distinction between things you had chosen and things that were going on behind your back. I am interested in the grey area, where people do tick the 'yes, I consent' boxes and waive 50 pages of legal rights and basically sign that over. Is that in the former or the latter category or is it somewhere in the middle? You have legally consented; you are just not sure what to.

Ms King-Siem—I think a lot of those terms and conditions that then follow from that tend to be that your information may have been used by subsidiaries or third parties of your organisation to further what they believe is in your interests either for the primary transaction or for the relationship you have. I would characterise that as a secondary flow of information, if you like, rather than a deliberate one by the person.

Senator LUDLAM—Even though legally you might have said, 'I'm fine for that to happen.'

Ms King-Siem—Absolutely, but I think probably 99 per cent of internet users really do not think about what it is that they are handing over and, if they do, they certainly do not think about where it may end up down the chain of organisations.

Senator LUDLAM—Given that the cat is really out of the bag, this committee has been considering what the role of law reform is and what government can do. Ironically, some of the marketing companies and ad companies told us at the last hearing that there is a huge amount of crowdsourcing, if you like, of people sharing information in forums of who is burning your privacy and that can actually hurt the reputation of companies. What is the role of a parliament given that (a) the cat is out of the bag and a lot of this information is out there already, (b) it is very transnational and (c) people are taking some of these things into their own hands already?

Ms King-Siem—I would have thought that the role of government is to support where possible the users' right to privacy. The fact that we do not actually recognise the right to privacy is slightly problematic in that regard. That would probably be the first argument I would put if we had an independent right to privacy, which the Australian courts have said for a long time that we should have but have been unwilling to step forward and recognise that in a meaningful way because they have been sitting back waiting for the legislature to do it, which so far has been rather unwilling. If that were the case then you would probably see an awful lot of class actions jumping up here and there and that would bring corporations into line a lot faster. That is where you are really letting market forces determine where privacy would lie.

Senator LUDLAM—Do you have a view on the larger and more substantive work on privacy law reform that is going on at the moment where they are amalgamating the two sets of principles and so on? Do you have any comments on that?

Ms King-Siem—At this point it is premature. I will in a few days time. Unfortunately, I really only hit this in the last week. I have read through some of the written submissions, which look to be quiet promising. I suspect an awful lot of what I would have to say would be repetitious, incorporating an awful lot of what other civil liberties organisations have said. But at the moment it would be premature for me to make an overall comment.

There are difficulties I suppose. Having the IPPs and the NPPs originally was a convenient way for the government to introduce regulation of the private sector and take a far softer approach between the private sector and the public sector. I note already in some of the written submissions that have been posted that there is concern that the APPs are taking a slightly more watered down approach than they could otherwise. Without having really been up to speed on this, I would say that any watering down of what I think is already inadequate protection is probably not a good thing. That is probably all I can say at this point.

Senator LUDLAM—That is fine. We can leave it there. Thank you very much.

Senator CAMERON—The previous submission from the Australian Privacy Foundation raised the question of the watering down of privacy protection under APEC. Do you have any knowledge of that or do you have any knowledge of reductions in privacy as a result of bilateral trade agreements?

Ms King-Siem—In broad terms, yes. I have not seen the second submission by the Australian Privacy Foundation—I have only seen the first one and heard Dr Clarke's evidence—but I would probably second his comments. The original was under the EU directive and the safe harbour scheme was concocted by the US as a mechanism to allow US organisations to trade and continue in the billion-dollar personal information industry. The US has at times sought to weaken the safe harbour, which I might add is already less than the EU directive had stipulated, and there was certainly an impression that APEC was being used as a bit of a cat's paw for the same purpose. Whether or not that is actually the case, I do not know that I could really comment.

There is an interesting article by an Israeli researcher, I believe, who puts forth the ongoing different models between the EU and the US and does discuss APEC in a bit more detail. If it

would be helpful, I would be happy to forward that to the committee. It is not a particularly long article and it is certainly written in layman's terms.

Senator CAMERON—That would be very helpful. Thanks. We have had some discussions about behavioural marketing, where there is a collection of the web-browsing history. Users of the data argue that the web-browsing history is not for personal information as it does not identify a particular individual. Do you agree with this position?

Ms King-Siem—This comes back to the classic problem of defining what is personal information. If you take what would be alleged to be an anonymous web user's browsing history but if you only have one person living at a particular address then that effectively means that that is personal information because it is identifiable or ascribable to a particular person. It is a very convenient way to say that it is actually anonymous data when, by the nature of where it has come from or other relevant factors, it is easy to determine who it actually belongs to. That point, strictly speaking, is when it becomes personal information. Before that point it is not, even though all the tools are at hand to make it personal information.

Senator CAMERON—The Australian Privacy Foundation submitted that the concept of consent is probably the single most serious weakness in Australia's privacy regulation. They recommended the implementation of consumer protection measures similar to the Trade Practices Act. Do you have a view on this?

Ms King-Siem—To be honest, I have really have not turned my mind to it sufficiently to comment. I do agree that consent is a very big issue, probably because it is bandied around so much as something that consumers have, when in fact I really question whether they do. What mechanism could be used to protect consumers more or to define consent in a more practical manner I am not sure at the moment. I know that there is some discussion of the issue of consent. I think it is in the Australian Privacy Foundation's submission. I suspect the Victorian Privacy Commissioner's submission will also deal with the issue of consent. I would probably point to where that has been picked up in the written submissions rather adlibbing.

Senator CAMERON—Thank you.

Senator TROETH—The Australian Law Reform Commission, in its review of Australia's privacy laws, found that because of the increasing use of technology the risk posed to online privacy by small business may not necessarily be low. In your view, should small businesses be subject to the requirements of the Privacy Act?

Ms King-Siem—Absolutely. My initial point that small business comprises 95 per cent of Australian businesses—if that figure is correct—means that Australian businesses are largely unregulated by the act, at least insofar as their dealings with that information go. The argument against the lifting of that particular exemption has always been that it would be too onerous on small business to comply.

Senator TROETH—We did hear that, yes.

Ms King-Siem—It is heard time and time again. However, if you look at the cost of regulation now or later on—which I would say is probably going to be inevitable, given the way

we are going—the cost to small business will be a lot lower now, as an early adopter, if you get in and get it out of the way, than later on.

Senator TROETH—What about Australian organisations sending data to overseas companies which are not covered by the Privacy Act? Is that a concern to your organisation?

Ms King-Siem—Absolutely, and it is a reality, particularly with cloud computing, having servers offshore. For almost any given interaction there is a good chance that your information is shooting its way around the world and some along the way may or may not be captured. I think there was a news article recently saying that in April this year, for something like 15 or 17 minutes, 15 per cent of all internet traffic was routed through China. They will be spending the next couple of years breaking that information down. That included NASA and the US Department of State. You name it; it all went through China.

I imagine that, with our data here, there and everywhere, it is not that secure. It is not even that secure, probably, in Australia. Again, you run into the jurisdictional problem of how do you then enforce that. Even if we have the strongest privacy laws in the world, if we cannot enforce them it does not do us much good. That is where international cooperation is key. It is very hard for us to argue greater protection if we do not offer it within our own jurisdiction.

Senator TROETH—Thanks for that.

CHAIR—Ms King-Siem, thank you very much for your time today. We look forward to you endeavouring to apply your mind to some of the questions we have asked you, now that, hopefully, you have a bit more time. Could you reply by 16 December, as that is the deadline that the committee has set. Thank you very much.

Ms King-Siem—My pleasure.

Proceedings suspended from 12.25 pm to 1.22 pm

MILLER, Ms Kathryn, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, Law Institute of Victoria

CHAIR—We look forward to hearing from you, Ms Miller. I will read you the riot act in terms of the formalities because you were not here earlier today. These proceedings are public. If at any stage you want to give evidence in private, you can make that request of the committee and we will consider that, together with your grounds for doing so. It is an offence and potentially contempt of the Senate for anybody to attempt to interfere with evidence that would otherwise be given by a witness before this committee, as indeed it is for a witness to give evidence that is in any way false or misleading. We have your submission. Do you wish to make any amendments to it?

Ms Millar—No.

CHAIR—I invite you to make a brief opening statement before we ask you some questions.

Ms Millar—I am here today representing the Law Institute of Victoria. The LIV is the peak body for lawyers in Victoria and those who work with them in the legal sector. We represent over 15,000 members.

The starting point from the LIV's perspective when talking about issues of privacy is the Privacy Act of 1988 and in particular the Information Privacy Principles, which apply to government agencies, and the National Privacy Principles, which apply to private organisations. I note that the Privacy Act and in particular the IPPs and NPPs are currently under review with a proposal that they be changed into the Australian Privacy Principles. There is a review of the exposure draft of the APP currently being undertaken by the Senate Finance and Public Administration Legislation Committee. That inquiry may affect issues of online privacy as well as offline privacy. The Law Institute of Victoria has made a submission to that inquiry as well. I note that that committee began its public hearings last week.

In the submission that the LIV has made to this committee, we chose to focus on what we understand is the proposal by the government, and we have based it on some possibly unsubstantiated media reports that the Attorney-General's Department has been in discussions with industry on implementing a data retention regime in Australia that might require internet service providers to log and retain customers' browsing history and email use. The reason that we chose to focus on that issue in this inquiry is that we consider that that proposal, if it exists and is real, represents a significant departure from the National Privacy Principles that would ordinarily apply to ISPs and also that it proposes to treat online privacy in a way that is different to the way that offline privacy is treated.

In summary, the policy would be a significant departure from the National Privacy Principles first because it would collect information not for the purpose of actually providing internet services but because the information might be useful at some time down the track to law enforcement agencies. The LIV suggests that the collection of this information and the scale on which it is going to be collected is unnecessary for the functions of ISPs and also, to an extent,

law enforcement agencies and also that it is unreasonable because it would involve a large-scale collection of information in relation to people who are not suspected of committing any crimes, and never will be, in order to identify information that might be relevant to a few suspected criminals.

There is also a concern about the sheer magnitude of the information that needs to be collected. That would all need to be stored somewhere, and the ISPs would have obligations under the National Privacy Principles to protect against the misuse of that data. The sheer scale of the information collected raises questions about how that would happen.

There is also a concern about the application of National Privacy Principle 4.2, which relates to the period for which information is retained. Our opinion of that principle when applied to this policy is that this information could potentially be retained indefinitely because, basically, how is an ISP to know when a law enforcement agency no longer needs the information that is being collected for them?

There are also a couple of concerns with NPPs 8 and 10. NPP 8 provides that users have to have the option of not identifying themselves when transacting with an ISP, if that is practicable. The problem with the amount of information that is being collected about people is that it renders it almost impossible to be anonymous, because of the profile that can be developed about you. Also, some of the information may include 'sensitive information', as defined under the principles, which is things such as gender, political opinion, sexual preferences and health information.

Also, the proposal treats online privacy differently to offline privacy. The best way of illustrating that is simply to point out that if this proposal was that all mail sent and received within Australia be logged and retained for seven years, or that all phones be intercepted and recorded, then I think it is not stepping outside the bounds of my expertise to say that there would be significant public outcry. What we have here is the electronic equivalent, and it really means that the government is proposing to treat online privacy in a way that is different to offline privacy simply because the technology makes it possible.

Finally, our submission states that the proposal, if it exists, is arguably unnecessary. Law enforcement agencies can currently apply for warrants to obtain information such as browsing histories from ISPs. If there is a concern that some ISPs do not contain significant browsing history, then the LIV considers that that can be dealt with on a case-by-case basis. In particular, if there is a suspect in an investigation, a warrant can be obtained to obtain the browsing history from an ISP and an ISP can be requested to log and retain the browsing history for that particular individual from that point forward. That is essentially what happens when warrants are granted for intercepting telephone calls.

I note that since we provided our submission there have been some developments. For example, I note that the Senate Standing Committee on Finance and Public Administration have begun their public hearings. I understand there has not been a further response to the recommendations of the Australian Law Reform Commission report. I should just note that that is the report that essentially preceded the Australian Privacy Principles. There has been a response to the House of Representatives Standing Committee on Communications report, which was titled *Hackers, fraudsters and botnets: tackling the problem of cyber crime*. That response

was announced on 25 November 2010. One of the aspects of that response was that the Australian government is working with the Internet Industry Association to develop a voluntary ISP code. I welcome any questions from the committee.

CHAIR—Then I shall take the liberty of kicking off. Thank you. You talked in your opening statement about data retention and about the government treating offline situations differently from online. I think you suggested, in terms of online, trying to search for the electronic equivalent, if you like. Some of the evidence given by some witnesses, and indeed some of the criticism of attempts to police online or apply regulations online, is on the basis that it is trying to apply offline thinking and offline rules to online systems and behaviour and that that is not appropriate or does not work. There has been that sort of criticism with respect to the government's proposal for a net filter—what is being called censorship. Do you want to reflect on that? I understand you to be saying that collection of telephone data would be the subject of a hue and cry, yet it seems to be different with online data. So is it a proper criticism to say that you cannot regulate online with offline thinking? If so, how do you reconcile that with your earlier comments?

Ms Miller—I am open to the suggestion that there will be circumstances and applications where what works in the non-electronic world just does not work in the electronic world. For example, it may be that law enforcement agencies need to change their techniques and their investigation methods for online situations. However, the Law Institute's comments are really coming at the situation from the perspective of privacy. We do not see any justification for saying that there is online privacy and that is different from offline privacy. I do not think that people make that distinction in their personal lives, their private lives, their professional lives. We do not think that it is appropriate that the parliament make a distinction in legislation between online privacy and offline privacy.

CHAIR—Okay. You talked about doing stuff just because technology makes it possible. In the second last paragraph, on the middle page of your submission, you refer to the large-scale collection of personal information by governments. You also referred to it in your opening statement. You say:

> The large-scale collection of personal information by governments because it *may* be helpful to some government functions, rather than because it is necessary, constitutes a serious threat to online privacy. The power of the internet should not be used by governments to achieve measures of control that would not be possible without the internet.

It is that bit of your statement and observation that I want to ask about. You talk about measures that would not be possible without the internet. Why not do it, if you can? Are you in fact talking about measures that would not be possible and necessary or appropriate? If you can do what is necessary or appropriate, why the heck wouldn't you? I am wondering whether you want to add something to that statement in the submission.

Ms Miller—Where that part of the submission was coming from was this idea that, when it comes to the benefits of technology and the internet to government agencies and law enforcement agencies, the question can sometimes appear to be, 'Can we do it?' rather than 'Is it appropriate or reasonable to do it?' What we were trying to get across in that paragraph was that the question should always be 'Is it appropriate and reasonable?' It should not be the case that just because we can we will.

CHAIR—'Is it appropriate? Is it reasonable? And, by the way, we can.'

Ms Miller—Exactly. If it is appropriate and reasonable but you cannot do it, then of course you cannot do it. We say that you should always start with the information privacy and the national privacy principles and then go to questions of practicality and possibility later.

CHAIR—That is helpful. Thank you.

Senator LUDLAM—Thank you very much for your submission. Possibly my questions will cross over into the larger privacy review that is going on at the moment. The Attorney's office and the Australian Federal Police were saying in the last hearing that we had on this that basically there is no expansion going on here and that this is the status quo; they are moving into being able to log the kinds of data that exist these days because the home landline records are fading away as people give those services up. How do you see this as being any different from the status quo, which is the Attorney-General's Department argued last time?

Ms Miller—It is true that currently telecommunications providers retain records of phone calls that are made between people. The first distinction that I would make between call charge records and metadata of internet websites is that a phone number is just a phone number unless you have other information to interpret what the phone number is. And even if you know who owns the phone number and who the usual users of that number might be, you still know very little about the content of the conversation. I would suggest that when it comes to websites the website address and the type of information that is commonly found on that website can in fact be readily ascertained, even just from the metadata. So, even if the proposal is restricted to metadata as opposed to the actual web pages, there is still a great deal of extra information that can be obtained that you could not get from something like a call charge record.

Another difference—and this might be stepping outside my area of expertise—is that call charge records and similar telecommunications information is held for billing purposes. The main reason that telecommunications providers need to know who has called who and for how long is so that they can charge appropriately for it. With internet service provision, it is really just about how many gigabytes you are downloading. They do not need to know which websites you are visiting. The only reason that they would be collecting this information is because it might be useful to law enforcement agencies not because of how they provide or charge for their service.

Senator LUDLAM—That is a useful distinction. You pointed out three or four of the privacy principles that this proposal would appear to violate. I have been a bit hesitant with my language as well—I do not know whether this is a proposal, a thought bubble or a program. With the way that the law is structured at the moment, what are the consequences for breaching its principles?

Ms Miller—Breaches of the principles are investigated by the Privacy Commissioner. My understanding is that the Privacy Commissioner often utilises things like conciliation or mediation to resolve concerns about privacy. There is no separate course of action for privacy. You cannot sue someone for a breach of privacy and get damages or anything like that.

Senator LUDLAM—Do you think that we should change that? Should there be?

Ms Miller—It is one of the obvious questions when looking at privacy. I am just having a look at our submission on the Australian privacy principles to see if we addressed this.

CHAIR—While you are looking—and maybe Senator Ludlam is going to go here—if so, how do you substantiate or measure damages?

Ms Miller—I do not think we have addressed it in our submission, so it would probably be something that I would feel more comfortable taking on notice. It is a live question should there be something more enforceable than an inquiry by the Privacy Commissioner. A statutory cause of action is a one-off possibility, but I do not feel comfortable speaking for the LIV on whether that should be something that is pursued. In terms of assessing damages, that is something that would need to be explored. There are a number of options. It may have something to do with the loss that has been suffered through the breach of privacy. Potentially there would be some consideration—almost like a 'hurt and anguish' experience through loss of privacy. Of course, when breaches of privacy happen, it is not always that there has been a quantifiable financial loss. Sometimes it is just that feeling of violation because your privacy has been breached.

Senator LUDLAM—I guess that is the sort of thing courts are good at figuring out. We might watch to see if you provide any other submissions, not necessarily to this inquiry but to the Finance and Public Administration Legislation Committee's inquiry on the privacy legislation. Are there other jurisdictions overseas that we should look to who are better at this than we are? I figure everybody is trying to work this out as they go—the technology is changing so quickly. Are there places elsewhere that we should be looking to?

Ms Miller—Again, I would probably take that on notice. Everyone is trying to grapple with the issue of privacy and everyone is doing it in a different way. It is affected by issues of treaties that people have. I know that the EU has got a data retention program or directive similar to that which we think is proposed by this government. That is in a lot of ways very context specific. There are a lot of things happening in the EU and they are affected by the EU arrangements and all of their treaties and everything like that. That is going to affect the way that they respond. So, again, it would have to be something that I would take on notice and provide a written answer to, giving a summary of what other countries are doing and looking at whether there is any model that is better than another.

Senator LUDLAM—Have you sought a briefing from the AG's office or have you put your concerns to them directly, or is this the first time you have put some thoughts on paper about the data retention proposal?

Ms Miller—When we first saw the media reports about it at the beginning of the year we did write to the Attorney-General and we had a response. I do not know if it was a satisfactory response but it was a response.

Senator LUDLAM—I will ask more questions later if there is time, Chair.

Senator CAMERON—Ms Miller, you said that you wrote to the A-G's department?

Ms Miller—Yes, that is right.

Senator CAMERON—And you said you were not happy with the response. When did you get that response?

Ms Miller—I do not recall.

Senator CAMERON—Weeks, months—do you have any idea?

Ms Miller—I think we sent the letter to them in the first quarter of the year and a response was received before the election, so probably in the second quarter of the year—a period of a couple of months, I think.

Senator CAMERON—Since then have you taken any steps to have further discussions with the A-G's department?

Ms Miller—I do not believe we have.

Senator CAMERON—Why not?

Ms Miller—The impression that we got from the letter that we received from the Attorney-General's Department was that perhaps further discussions with the Attorney-General's Department would not be the appropriate avenue to pursue this issue and that it might be one that would be better pursued in other avenues. That is why, when this inquiry came up, we thought this would be a good opportunity to pursue the issue.

Senator CAMERON—Other than this inquiry, you have not stopped to have discussions or given your views to the minister?

Ms Miller—Aside from that initial correspondence, no.

Senator CAMERON—Why not?

Ms Miller—As I said, the content of the letter suggested that this was an issue where it was not going to be an efficient or productive course of action to seek further audiences with the Attorney-General. We raised the concerns that we had in the letter. The Attorney-General provided responses to those concerns and it did not really look as though it was an issue in which further conversation was going to be encouraged or necessarily worth while.

Senator CAMERON—So they actually said it would not be efficient or productive to try to pursue your political concerns. Is that correct?

Ms Miller—No, that is not what the Attorney-General's officer said.

Senator CAMERON—But you just said that you took the view it would not be efficient or productive.

Ms Miller—That is the opinion that the committee formed that was responsible for preparing the correspondence and engaging on this issue after it reviewed the letter that we sent and the letter that we received in response.

Senator CAMERON—You guys are easily put off the trail, aren't you?

CHAIR—You are doing your best to put them off, Senator Cameron.

Ms Miller—We do not like to think that we are easily taken off the trail, but we do have limited resources and we like to apply those where we think they are going to create efficiencies.

Senator CAMERON—I have to say to you: one letter and that is the end of it is very interesting. You also said you were not really sure what was being proposed by the government.

Ms Miller—That is right.

Senator CAMERON—You thought it might be similar to what is being proposed in the EU.

Ms Miller—That is right.

Senator CAMERON—If you are not sure, what brings you to that conclusion?

Ms Miller—There was an article published—

Senator CAMERON—Don't tell me it was the *Australian* or that will be the end of it.

Ms Miller—No.

CHAIR—In your view, Senator Cameron, maybe.

Ms Miller—It was an article published in February or March in an online magazine called *ZDNet* and then in another one on 11 June 2010. That reported that there had been meetings between the government and representatives of ISPs to discuss this proposal. As happens with these sorts of things, someone alerted this online magazine to it and they wrote an article about it.

Senator CAMERON—Your views are checked by two online articles.

Ms Miller—Our knowledge of the proposal if it exists is based on those two online articles. Our views are based on our understanding of what such a proposal might look like based on the EU directive on this issue. We would of course be thrilled to review those views and also to review our views about whether such a policy would comply with the Information Privacy Principles and the National Privacy Principles if the government were to release that proposed policy publicly.

Senator CAMERON—You will have to be a bit more persistent than you have been.

Ms Miller—Well, we certainly wrote to the Attorney-General and asked for details of the proposal and they were not forthcoming.

Senator CAMERON—Okay.

Senator LUDLAM—There was also some reporting in the *Sydney Morning Herald*. One of the journalists there submitted a freedom of information request that came back drenched in black pen and that is where some of the secondary reporting has come from as well.

CHAIR—Take that, Senator Cameron.

Senator CAMERON—Who was that?

Senator LUDLAM—It is Senator Ludlam being helpful.

CHAIR—We need a chair and another participating senator as a balancing antidote to the deputy chair.

Senator CAMERON—The Attorney-General's Department claimed at the committee's last hearing that data included under the proposed scheme is similar in nature to telephone logs of who called whom and when. Telecommunications companies keep that for billing purposes and it is not necessarily kept for the new technology. Is this retention of information about an email any different from telephone call logs?

Ms Miller—As I said in response to Senator Ludlam's question earlier, I think that there is a distinction to be drawn between call charge records—records held by telecommunications providers about who called whom—and metadata of websites visited and emails sent or received. When it comes to telephone call charge records, the phone number itself is just a phone number until you have additional information such as who owns each of those phone numbers. Even if you know that person A called from phone number 1 to person B at phone number 2 there is really not much you can say about the content of that conversation. In contrast with things like websites, the name of the website can in fact disclose a great deal about the content of the information that has been obtained from that website, even if you only retain the metadata and do not retain the website itself.

The other point of distinction is that call charge records are retained by telecommunications providers because they need to charge the users of the telephone for making the calls. That is in contrast to this proposal, where internet service providers, who do not need to retain this information for billing purposes, would be retaining it solely because it might be useful to law enforcement agencies.

CHAIR—Regarding small business and the exemption for small business, do you think small businesses should be subject to the privacy legislation?

Ms Miller—I do.

CHAIR—It is that simple, so there should not be an exemption—full stop?

Ms Miller—I think that when you have something like privacy, which is a principle or a protection that has a broad application—privacy touches on just about every single aspect of our lives—the more exemptions you put into the legislation, the more unwieldy it becomes to apply it. This is an issue that we have looked at as part of the review of the exposure draft of the Australian privacy principles. I understand that it is not being addressed as part of the Australian

privacy principles or the current review that is being conducted by the Senate Finance and Public Administration Committee. My understanding is that that is going to form part of a second response to the ALRC's review, but in the discussions that the LIV had about this there was a comment that it seems a bit inconsistent that small businesses are exempt from this, particularly when you consider that some small incorporated organisations such as charities or community groups that are not in business may still actually have the national privacy principles apply to them.

CHAIR—Can consent genuinely be given to the use of personal information that might otherwise be regarded as private in the online world?

Ms Miller—This is a very interesting question. I think that there are two different types of consent when we are talking about the provision of information, whether it is online or offline. There is what I will call formal consent, where you have a question asked of you—'Do you consent to provide this information?'—and someone says yes. That is one way of looking at consent, and I think at the moment the national privacy principles and the information privacy principles really do look at consent in that situation. There is a deeper question to be asked, and that is: how real was the consent or what was the context of the consent? If someone is saying to you, 'You can't access this service,' or a certain product, 'unless you give us this information,' then I think the nature of the consent starts to become a little bit different. It is particularly a concern—

CHAIR—We currently have that, for example, for medical and other specialist services.

Ms Miller—That is right. What I was going to say next was that it is not necessarily a bad thing to say that you need to provide certain information to be able to obtain a service. For example, it is difficult to get a tax refund if you do not have a tax file number. It is difficult to access medical services if you have not provided your medical history. Where it becomes a bit different is where organisations request information that is not necessary for them to provide the service or the good that the person providing the information wishes to obtain—where they ask for additional information not because they actually need it to provide the good or service but because it might be useful in the future or they could use it for some sort of ancillary purpose such as marketing. I think that is where consent starts to get a little bit hazy.

CHAIR—You used the word 'real' and talked about discerning whether consent was real. In the workplace relations world, which is close to the heart of the next witnesses—and also Senator Cameron, if I might—there has been discussion about 'genuine consent'. Surely those sorts of factors do not affect the genuineness of the consent, which is really the nub of what I am asking about, rather than the protections and other things you might put around the use of that information et cetera once and if consent is able to be genuinely, properly, really—whatever word you want to use—given.

Ms Miller—'Genuine' is probably a better word for it. Formal consent does involve genuine consent. If somebody provides information and says, 'Yes, you can collect that information,' they are genuinely consenting. They know what they are doing.

CHAIR—Do they and does it, because we have had evidence from other witnesses that people do not necessarily read before they sign? I would like to say that I always read before I sign.

Senator LUDLAM—Do you?

Ms Millar—I would like to say the same thing. I agree. When presented with pages and pages—

CHAIR—It is the price of access, isn't it?

Ms Millar—It is. I think with online access everyone wants it to be quick and is used to it being quick. When confronted with a 20-page document that still seems to be written in 1950s legalese and which has not been touched by the trend towards plain English, I absolutely agree that people just click through.

CHAIR—You just click yes, don't you?

Ms Millar—That is right.

CHAIR—For example, when you are booking with Qantas—

Senator LUDLAM—You just hunt for where it says to tick yes.

Ms Millar—Yes, absolutely. That is right. That would be more a question about consent to the terms and conditions of using the site which will include issues of privacy but will also extend to other issues. I guess from my perspective the genuineness of the consent and why you can say that there is genuine consent when it comes to providing information to websites is because you have to be the one typing that information in. For most of the information that we provide online I suggest we have to actually input it, so we have to provide our name, our address, our date of birth, our mother's maiden name—

CHAIR—There was evidence given by others about the advertisers and marketers who work stuff out from our footprint online, which is not necessarily actually information we input. Given the time constraints, you might take on notice—only if you have something to add—whether proper and genuine consent is able to be given in terms of information online and, if so, how and what would you define it as. The committee has set 16 December as the deadline for answers to questions taken on notice. If you have something to add, that would be helpful.

Ms Millar—Yes.

CHAIR—In discussing how far employers should be able to go to access information about employees, the ACTU suggests it is not appropriate for an employer to access information to do with an employee's use of personal equipment for personal reasons in personal time. Do you think that that boundary is able to be drawn and, if so, would you draw it right there and say that everything else is up for grabs for an employer or would you draw it earlier than that and, if so, where?

Ms Millar—I think it is really difficult in a privacy situation to draw any sorts of stark lines. I think it is always going to be based upon context and the facts and circumstances. The difficulty with a personal device is that most personal devices are in fact used for work purposes these days. We are getting the merging of work and private lives. I think it is clearer for employers to be able to access devices that they have purchased and paid for. I think they are on less safe ground when it is a personal device even if it is used occasionally for work calls, work emails or something like that. I would not necessarily draw the line at where they are because these days all of our communication is very mobile. I do not think that is very useful for people. I think it really needs to be looking at what was the use of the device at the time, whether it was for a personal use or for a workplace use, and then looking again at who pays for the device.

CHAIR—I suggest that you think about whether it would be cut and dry in many situations, whether it would be black and white, or, if not, how the individuals involved—whether it is the boss, the worker, a union or a cop on the beat—easily discern that, given that these sorts of interfaces are happening more and more. If you can turn that into a question, you are doing better than I did. You might want to comment on that now or take it away. If you do not have anything to add, you can just say you have nothing further to add. I do not want to give you work that you do not need.

Ms Miller—It is all very well and good for me to sit here as a lawyer and say, 'That depends on the circumstances,' as we like to do, but I also understand that both employers and employees want firm boundaries because they want to know what is acceptable and what is not. I think it has been firmly established, and is common practice now, that employers are entitled to look at certain information that is done on their own work computers and work phones, what information is being exchanged there. I think the blurry line comes when there is a mobile or a laptop or something that is used for both purposes. As you state, where does the line get drawn? I do not know that there is a line but I can go away and check that out.

CHAIR—It may be workplace policy that 'you can also use this thing for personal stuff because it does not cost us anything directly' and what that means in a privacy context.

Ms Miller—Yes.

CHAIR—Thank you for your time, Ms Miller; it has been very helpful.

[2.00 pm]

CLARKE, Mr Trevor, Legal and Industrial Officer, Australian Council of Trade Unions

FETTER, Mr Joel, Policy and Industrial Director, Australian Council of Trade Unions

CHAIR—The committee welcomes representatives from the ACTU. The evidence you are about to give is public and the proceedings are public. If at any stage you want to give evidence in private, please request that and the committee will consider your grounds for doing so. It is an offence for anyone to give false or misleading evidence to the committee and potentially a contempt of the Senate, as it is for a third party to attempt to influence evidence that would otherwise be given by a witness. Senator Troeth and Senator Ludlam are here with me, and senator Doug Cameron is in the ether.

Mr Fetter—I am sorry, chair, does that mean that Senator Cameron is listening in?

CHAIR—Yes. He will no doubt ask questions of you, once I let him. We have your submission; is there anything you would like to amend?

Mr Fetter—There is not.

CHAIR—Then, how about an opening statement?

Mr Fetter—We thank the committee for receiving our written submission and having us along today. The ACTU, through its affiliates, represents two million working Australians and it is on their behalf that we appear today. The ACTU has been thinking about these issues for a number of years now and we addressed some of those points in 2009 in our congress policy. It has been apparent for several years that new technology is changing the world, really, but in particular the workplace, with devices and facilities such as the internet, mobile phones and, indeed, tracking devices. It is not only the work of white-collar office workers that is changing but also the work of manual or blue-collar workers. We acknowledge, of course, that the new technology provides enormous opportunities for society to work smarter and more efficiently and also to free ourselves as working people from some of the traditional confines of being locked in the office.

CHAIR—Yes. It should all be good, shouldn't it?

Mr Fetter—That is right. If managed properly, it could be a wonderful boon to the quality of people's working lives and productive enterprise. But with opportunity always comes risk, and the major risk that the committee is considering is the risk to employees' privacy. As the previous witness pointed out, there is increasingly a blurring of work and private lives, particularly for those workers who sit in front of computers or who have employer issued mobile phones and other devices where they are using the device for both work and personal reasons.

There is also enormous risk from the fact that now more and more of what employees do is recorded in writing through these devices and through various websites and that the written

information is there, potentially, for posterity. Alongside that, of course, comes the increased capacity on the part of employers to monitor what employees are doing. So, putting all of these things together, we think that there is a potentially risky mix of factors which, if not controlled properly, would lead to an erosion of people's legitimate interests in having a degree of privacy at work. So the challenge for the law is obviously to balance workers' rights to privacy, particularly of their personal information, against the employer's interest in managing their business and having people perform appropriately and efficiently.

We come to this committee from the point of view that the law as it currently stands is clearly inadequate, in our view, in that the whole class of employee records is exempted from the provisions of the Privacy Act. So, as a matter of practice, there is very little protection for people—whether at work or outside work, frankly—in relation to the privacy of things that occur in the course of their employment. The current state of the law shows that, in a sense, no attempt to balance those two interests has been undertaken to date. Essentially, employers have carte blanche, at least in relation to most of the issues that we are concerned about, to decide what they will monitor and what they will not, subject to some state based legislation in relation to surveillance.

So we think that the time is ripe to reassess these issues and to try and strike a better balance. My colleague Mr Clarke can go into a bit more detail on our concerns about the interests that workers have in their privacy at the point at which they are candidates for jobs, at the point when they are in employment and also towards the end of their employment. But I should say up front that, while the ACTU has been considering these issues and has attempted to develop some principles, we ourselves are not at the point where we have a specific call for law reform on this issue. We would like to have more consultation with the peak employer bodies, because we think that there is a sensible way forward here in terms of delineating what a reasonable employer may do, and we hope that our employer friends will agree with us on the appropriate boundaries. We also would like to explore whether some of this could be resolved through bargaining. We think that, apart from questions of what the law should impose, it is obviously very important that the workplace context is given to these issues and that there is capacity for bargaining at the workplace. So, with those remarks in mind, either I can throw to my colleague or we can take questions from the committee at this stage.

CHAIR—I think we might kick off the questions. I will start with one, and then we will see if Senator Cameron wants to give his two bobs' worth. 'Consider these issues in a workplace context' was part of what you were suggesting at your end point, Mr Fetter. Haven't these sorts of issues been considered, at least to some extent, by policymakers and also by organisations like yours and business organisations in a workplace context in respect of employee records and the fact that there is a separate sort of policing system and 'cop on the beat' to access those records for the benefit of employees? Hasn't there been, to some extent, workplace consideration given to issues that will involve the privacy considerations? What are your views of the way those deal with privacy considerations?

Mr Fetter—I am sorry: I am not sure I follow. Are you saying that this has already been dealt with because there is that provision in the Privacy Act?

CHAIR—No. Do you want to have a go, Mr Clarke? I am asking the ACTU—so either of you. I can rephrase it if you need me to. Mr Clarke, do you want to comment?

Mr Clarke—I think what you might be getting at is the ability of permit holders to inspect the records.

CHAIR—And the Fair Work Ombudsman.

Mr Clarke—Yes.

CHAIR—There is a system. Basically an employer needs to keep records so that a third party can access them to work out whether or not an employee has been dudded—to put it in layperson speak. So there is a separate regime allowing access to information that might otherwise be regarded as private, and that is being dealt with in a workplace context.

Mr Fetter—Yes.

CHAIR—It is not simple, is it? Underlying what I am asking about is the fact that it is not as simple in the workplace world to try and regulate the privacy stuff in the privacy legislation. I guess that is why we are in the situation we are in.

Mr Fetter—Yes, Senator.

CHAIR—Answer that how you will.

Mr Fetter—Those provisions deal with access, both by registered organisations and the Fair Work Ombudsman, for the purpose of investigating a suspected breach of people's legal rights. But it is a very limited range of rights, essentially, that people have under the system. At the end of the day the area that is not regulated at all is the scenario where workers are accessing information—whether it is through Facebook, Google or whatever sight—and then the employer is seeking to monitor what is going on and potentially discipline workers for using those facilities inappropriately. I do not think the Fair Work Act has anything to say about those issues. It is true that in relation to workplace issues it is not obvious that these matters ought be dealt with under the rubric of the Privacy Act rather than be dealt with as an integrated part of the Fair Work Act. That is why I suggested, before, that workplace-specific consideration of these issues would be required—because what goes on in the workplace often has a very different flavour to what goes on in the broader community.

CHAIR—Before I invite questions from others, find a way to convince me that the ACTU is not—I am sure it is not—happy with access to information that might otherwise be regarded as private when it is aimed at protecting the rights of employees versus doing something else. You used the example of an employer wanting to monitor access. So find something to convince me that the ACTU is not only being mindful of the need to protect employees.

Senator CAMERON—Can I indicate that you can take that on notice and give it some serious consideration, if you like.

CHAIR—Of course, Mr Fetter can. That remark was from Senator Cameron speaking via teleconference; I did say he would make his presence felt.

Mr Fetter—I am happy to provide you with a long answer on notice but, in short, when the Fair Work Ombudsman or a permit holder investigates suspected breaches of the law, first of all, usually the information that they are seeking to access is not health records or intimate records. Probably the most private thing there would be disclosure of is a worker's salary. So it is a very different thing to what workers might access on the work system—they may access their personal banking information or they may send an email to their doctor. So I think it is of a different nature. Second of all, permit holders are overwhelmingly investigating at the request of affected employees. So the employees have given consent for the trade union to investigate breaches of their rights and obligations. So again, I think that is a very different situation to the much more serious issue of where employers are monitoring truly intimate details that relate to employees' personal lives. That is often done without consent or in circumstances, as the last witness pointed out, where the quality of consent is very questionable.

CHAIR—This is my final question on this part: are you saying that business privacy is different from personal privacy? In the example that you used, an employer might regard that as an invasion of their business privacy, and yet it is the law that they must allow access. Is their a difference between an employer's business privacy and somebody's personal privacy? I would like to hear you reflect on that.

Mr Fetter—In that circumstance there certainly is, because nobody can invoke their business privacy as an excuse for why there ought not be an official investigation, whether it be by they police or some other authority empowered by statute to investigate. In that circumstance, there certainly is.

CHAIR—So you are saying it is good that there is a lack of that sort of privacy.

Mr Fetter—In the enforcement space.

Mr Clarke—The other distinction that needs to be drawn is that those sorts of investigative rights have come about by the parliament making a conscious decision to work out where the public interest lies and creating a public right based on the public interest. They have said: 'This is the employment or labour market and this is the way that it works. We think that there is a policy case for a public right for a regulator or somebody with de facto regulatory authority as a permit holder to make sure that the laws are being observed.' There has been a conscious decision to look at those issues, whereas I understood this inquiry to be directed at this because everyone has been ignoring this for a while and they want to answer the question of how to fix it. In the case of pay sheets and leave records and all those sorts of things, they have been the subject of a very targeted policy decision to create a public right for what is seen as a public interest.

CHAIR—Indeed, the terms of reference could be why we have not had any submissions from employer or business organisations to this inquiry. It is all very well for you to see it as appropriate, but we do not have their views.

Senator LUDLAM—I want to follow on along those lines. One thing that has been bugging a bit as this conversation has gone on, given that we have just had national go home on time day is that we apparently donate six weeks of unpaid overtime to our employers every year. As much as people might say that Facebook and personal time is bleeding into work hours, the reverse is

happening to a much greater extend, with work bleeding into personal times. Maybe our social lives are becoming a little bit intertwined with our work lives. You said that there ought to be greater controls on employer monitoring of the contents of online communications made while at work. Given the fuzzy boundaries of what 'while at work' may mean these days with some of these technologies, how do we do that? What kind of controls should we put on workplace snooping?

Mr Clarke—The difficulty in answering that question is because of the point in time that we are at already. We have taken a long time to start thinking about this. As long ago as 10 years ago there was a survey by Freehills, one of the major law firms, that indicated that 64 per cent of Australian employers who responded covertly monitored the emails of employees. What we are trying to do now is articulate what the interest in privacy and justify why it is that we should limit what has been taken for granted as the right of employers. But the starting position in other places, such as Germany, has been that you enter the workplace with your rights intact and so you are not in the defensive position there that you are in here. We are in a defensive position now, rather than being in the position of assuming that there is a right to privacy, asking an employer to articulate a business need that they have and then explain why the meeting of that need necessitates invading privacy and then going through the balancing exercise. There is a first principles question here. We have waited so long that the privacy advocates have to make their case in a defensive way rather than there being any sort of assumption about where you start in principle.

Senator LUDLAM—Spell it out to us: whatever the ethics or operational reasons might demand, it is not at all unlawful for an employer to spy on an employee's email. Is that a fair thing to say?

Mr Clarke—I do not think that that represents the legal position. A couple of the state governments—New South Wales and Victoria at least—started to put some statutory controls in place in relation to workplace privacy and monitoring et cetera.

CHAIR—What about the victimisation provisions of the Fair Work legislation? If an employee were to argue that they were being victimised, that is potentially unlawful in the workplace space already—potentially?

Mr Fetter—Only if it is related to one of your workplace rights, and you do not have a workplace right to, for instance, access your bank online and pay your mortgage. That is the problem.

CHAIR—What if an employer were singling out someone? What if I was your boss, Mr Clarke—God forbid—and I was singling you out for online monitoring and I am only monitoring you? You could argue—

Mr Fetter—The employee is only protected if the employer has singled him or her out on one of the proscribed grounds.

CHAIR—Yes. But by and large there is not, but there are some scenarios in which you could say it is already—

Mr Fetter—Yes. If you had selected Mr Clarke because he was a union activist in the workplace and—

CHAIR—Never!

Mr Fetter—you were trying to contrive a reason to discipline or dismiss him then that would raise questions. But some of the problems with this go to the workplace context. The capacity to monitor means that an employer can dress up wrongful grounds for investigating an employee with legitimate grounds. There are some difficult intersections between the traditional rules and laws of employment and the new technology. For instance, it has been a traditional rule under common law that, if an employer dismisses an employee for one reason which is illegitimate but after the dismissal finds a legitimate reason—for instance, because the employee was guilty of some misconduct a long time in the past—then the dismissal is regarded as legitimate. This is even if the employer did not know at the time that there had been a breach.

CHAIR—But it may subsequently be found to be procedurally unfair, mightn't it?

Mr Fetter—Unfortunately, the commission and now the tribunal have in some cases picked up this old rule to say that an employer can justify a dismissal based on facts not known to them at the time of the dismissal and even if the dismissal was for a wholly different reason. In a world in which people are making comments on the internet that are permanent, it is very easy for any employer, we would submit, who wants to get rid of any employee to manufacture a legitimate dismissal in terms of that rule. Either that rule has to change in light of the greater capacity for employers to do this or parliament has to intervene.

CHAIR—One employee could manufacture a reason in respect of another employee, couldn't they?

Mr Fetter—Yes.

CHAIR—Anybody can, really.

Mr Fetter—We are happy to admit that it cuts both ways, too. Once a manager may have just had a word in the ear of an employee where there was a problem, now there might be a written record on the email system. An employee is entitled to rely on that record if they objections to what was said.

CHAIR—Or a disgruntled spouse or friend of an employee. There are really no limits to the mischief that can be done.

Mr Fetter—That is right. Some of these things are not new in terms of the underlying concepts. What has changed is the cost and the capacity. It is now very easy for an employer to monitor everything that its workforce does second by second. Once upon a time, you could have done that by having a person stand over every worker at their desk. But that would have been very expensive. The reduction in the cost of technology means that it is now available to every employer.

CHAIR—Very easy? We have not got business groups here, but they might still regard it as headache; a pretty easy headache to get, maybe, but a headache nonetheless.

Mr Fetter—We were hoping that they would agree with us that a reasonable employer would not do some of these things because they constitute bad industrial relations practices and bad people management practices. At the end of the day, employees who feel that they are spied upon and that they might be entrapped at any moment do not make good workers; they will not commit to the business. In fact, that is the other intersection with the law that is quite interesting. From a legal point of view, there is an emerging and recently accepted implied duty in the employment relationship, which is the duty of mutual trust and confidence between the employee and the employer. That has been accepted by Australia in the courts. Some of this does raise serious questions about the extent to which any of these practices that we have raised would constitute a breach of these duties and in fact might entitle an employee to remedies under our common law. It is an interesting question. It shows that ultimately this is not a question of an employer's right to control but about the trust that is inherent in employment relationships and without which we could not have good and healthy relationships that lead to a productive economy. We would rather that this not be litigated in the courts. We want the voice of reasonable business to sit down with the trade union movement to agree on some principles for where this boundary might lie.

CHAIR—If it were as simple as being about rights, that would be one thing. But isn't it also, for example, arguably about an employer's duty—for example, their duty to have a safe workplace? An employer might argue that they were monitoring because they need to provide a safe place of work both for you, my hapless—sorry, very happy!—employee, Mr Clarke, and your colleagues.

Mr Fetter—That is right. That is why the language of rights is often difficult when there are competing rights in play. Here the employer certainly has an obligation, legal and moral, to have a safe workplace. Unions in particular take that very serious. Monitoring to ensure that policies in relation to accessing of obscene material is one thing, but monitoring on a routine basis to see what people are writing about the company in personal emails is a very different thing. But there is a balance to be struck. It is difficult to say with any certainty in the abstract how it should fall. But we gave some examples in our submission. There are clearly cases that in our view are outside the pale for which you can draw a bright line. We hope that the employers would agree with us on those. To use that example, where an employer does—and we think that they should—allow employees to access personal email and personal banking from the work computer, that should be completely off limits from monitoring at least in the absence of any complaint that is brought forward about abuse. Clearly, if there was a complaint that someone was accessing pornographic material via their personal email account, you could look into it. But it is the covert and routine monitoring of communications which we think is beyond the pale.

CHAIR—I am not trying to debate the sentiment. It is more the practicalities of it. Is it so cut and dried? For example, a truck driver must get a certain number of hours of rest. They are on the road. It is in the boss's interests; it is in the worker's interests; it is in everybody's damn interest. I appreciate that many of these guys will be owner drivers and you would want them to be members of your affiliates, and maybe they are not at the moment. What if an employer suspects that the truckie, rather than having some shuteye, is using work provided equipment to

catch up on emails et cetera rather than making sure that he is safe to get back on the road? It is not black and white, is it?

Senator CAMERON—Not in that example.

CHAIR—That is right. It is not black and white in all scenarios.

Senator CAMERON—Ask the witnesses a reasonable question.

CHAIR—Mr Clarke was getting ready to answer it, Senator Cameron, so I reckon that they thought—

Senator CAMERON—I think that you mistook an answer for laughing. I am not sure.

CHAIR—Get your butt here if you want to assess the visuals.

Mr Clarke—The beauty of it in relation to those types of monitoring that are directed towards compliance with what are now statutory regulated health and safety requirements is that it needs to be done on the basis of consultation with the workforce. That dovetails nicely into the point that Joel was making before about bargaining. Sure, we can have some kind of overarching guideline and agreement with the employer associations—which we would very much like to have—but, when it comes to the nitty gritty details of what is appropriate for a workplace from an implementation place, there are those structures and health and safety laws that encourage and require that type of consultation. Bargain instruments are the subject of in some cases quite protracted negotiations with employers and their representatives. There might not be a necessity to go to that level of detail in some sort of broad way, because once you get the principles right the industrial stakeholders can figure out the detail in a way that is more appropriate to the circumstances in their workplace.

CHAIR—Thanks.

Mr Fetter—The other difficult issue here is that it is not only a question of what can and cannot be monitored. In our view, it is also the quantity and quality. Many of the concerns expressed in our submission are about the oppressiveness of surveillance. Something that is done once might be all right. But obviously if employees are in a situation in which every move of theirs is being watched in some capacity it destroys the trust that I see as being at the heart of productive working relationships. There are many examples of where employees are requiring employees to wear or carry tracking devices that the employer assures them is for their own protection. That may well be the case. In fact, an employer who stuck to that as a rationale for monitoring people's whereabouts would be fine. For example, the Armaguard people who fill ATMs have a shared interest in making sure that the employer can call the police and inform them of their whereabouts. It is very different where the employer has secondary purposes, such as to check that people are where they should be at every single moment of the day. We do not have the answer of how to separate legitimate tracking from illegitimate tracking.

CHAIR—That is the difficulty, isn't it?

Mr Fetter—Some of it goes to motive. Some of it goes to the process and whether it is agreed between employees, employers and unions. Some of it goes to intensity and frequency. They are the sorts of difficult aspects to this issue which we do not have a single answer for. Hard cases, with respect, do not help.

CHAIR—But they exist.

Senator TROETH—How common would you say it is for employers to monitor the online activities of employees? Would you say that it is very common, occurs sometimes, is not common or occurs never?

Mr Clarke—There was some statistical stuff about that. The Australian stuff that I referred to from that Freehills survey is quite dated. In that survey, 64 per cent of the respondents were monitoring emails. There is some international research from the US. I think it was the International Institute of Management. They found that 12 per cent of employers were monitoring internet blogs and 10 per cent were monitoring social networking sites. My recollection is—and I do not have the figures in front of me—was that in the US literature somewhere around 60 to 70 per cent monitor email.

Mr Fetter—We will provide the figures that we have to you on notice.

Senator TROETH—That would be very good.

Mr Fetter—Two things are clear: one, a majority of employers that monitor; and two, because of the pace of change even figures that are a couple of years old are likely to be out of date.

Senator TROETH—It is growing.

Mr Fetter—We looked at figures from both Australia and the United States. A majority of employers monitor internal email. Then there are smaller proportions that monitor personal email and activities outside the workplace. We drew attention in the lead up to our 2009 congress to where this process had reached in America. In a number of cases, employers have made it a condition of employment that employees be microchipped with a device that transmitted their location at all times to the employer.

Because consent was given as part of the terms of the job, then on a very formal basis there was no problem with that under American law as it stood. But I believe that a number of states, including California, moved quickly to outlaw that.

Again, the cost of those devices halves every 18 months, probably like every other piece of equipment these days, and the risk is that if we do not do something about that in Australia in a comprehensive way the temptation for an employer to do it remains. The incentive is there, and there is a serious risk that the law will lag behind what is happening out there in industry and that people will be harmed through it.

So it is very timely that this committee is looking at the issue. We certainly would not want to follow the American precedent, where, because the law was not there in the early stages and the

law took a while to catch up with the developments, there was a period of open slather. In the absence of regulation that is often what happens. Unfortunately, it is the unscrupulous who push the boundaries and more reasonable employers hold back, but it is the unscrupulous ones who set the pace. This is a good opportunity, while we are still relatively early in the IT revolution, to set some new boundaries, because we do not feel that the Privacy Act deals with this adequately at all. It just avoids the issue.

As Senator Fisher said, there is a balance you recognise between rights and interests. We do recognise the right of an employer to exercise some supervision over what employees are doing, but that has to be balanced against the fundamental right of employees to have privacy of truly private information and not to have an oppressive workplace where they are under the scrutiny of Big Brother. We say that that is bad for the relationship of trust between workers and management, and without that trust it is hard to see how we could end up with the dynamic workforce of the 21st century that is going to be able to take advantage of some of these technological innovations.

The problem, though, that you have as members of parliament is that if you agree that this is about trust it is very difficult to legislate for trust. It is difficult for the law to say that employers must give employees a measure of trust, should presume that they are doing their jobs responsibly and appropriately and give employees some leeway in what they might do with their time during down time at work. I am not sure how you can write that into the law, but at the same time the law will be very important around the fringes to control some of the worst abuses, we think.

Mr Clarke—I will add to that. I have located the stuff I wanted to refer to before. The most recent stuff we had out of the US was in 2007. The figure from the American Management Institute was that 66 per cent of employers monitored internet connections and 45 per cent monitored computer use by tracking keystrokes and time spent at the keyboard and so forth.

A more recent indication, and it is a local one, comes in our own 2009-2010 state of the public service report, which indicates that, of the disciplinary investigations of public servants conducted for the last two years, the largest group was for improper use of the internet or email. That represented a third of all disciplinary investigations, which would indicate that in public sector employment, at Commonwealth level at least, that sort of monitoring is probably prevalent.

CHAIR—It is happening. Thank you. We have Senator Cameron on the phone.

Senator CAMERON—Mr Fetter, you spoke about trying to deal with this in bargaining outcomes. There are impediments to enable bargaining in these issues. What is the ACTU's preferred position—legislative standards or bargaining outcomes?

Mr Fetter—I suspect that both will be important. As I just said, I think legislation will be needed to control some of the abuses here, and the states have already taken some steps to control surveillance of people that is oppressive. But I think bargaining will be important to give these rules some workplace context. However, as you point out, it is true that, in the view of the ACTU, the bargaining system is perhaps not up to this task in two major respects. First of all, there are very significant barriers to any sort of bargaining or negotiation at the industry level. So

that clearly constrains our ability to come up with common-sense solutions that ultimately would be agreed by industry under the Fair Work Act. Secondly, even at the enterprise level, there is a question mark about the extent to which all of these matters are matters which pertain to the employment relationship, which is of course the criterion for legitimate bargaining under the act. We would always argue that these were all matters that were pertaining to the relationship, but I could predict that our opponents would say that some of these matters—particularly what people do in their private time—lie outside the field of joint interest and joint regulation, so that is a difficulty that potentially will be faced.

CHAIR—Indeed, you say it should, as part of your submission. Sorry, Senator Cameron—I do not want to take away from your time. But you say that if it is private equipment and private time for private things, then it should be hived off?

Mr Fetter—No. I think that it is a very complex issue. When it comes to employers seeking to control what people do in their private lives, we have very serious reservations about that. There is a grey zone though where you might seek to negotiate what you do and say in your private life that may affect your employer's business. In fact, we have provided some examples of where employees have been dismissed in precisely those situations. The employers assert in those cases that their interests in controlling what their workforce say about the business override an employee's right to free speech, really, outside of the workplace. So that is a very contested area. But there is a core that we hope the employers would agree should be the subject of negotiation and ultimately joint determination. But potentially not everything—

CHAIR—I guess it is a matter of definition. Senator Cameron?

Senator CAMERON—In relation to international experience, what is the international best practice on this--either bargaining outcomes or legislative outcomes?

Mr Fetter—Do you want to answer, Trevor?

Mr Clarke—It is not something that I am able to answer—

CHAIR—Perhaps they might take that on notice.

Mr Fetter—Yes. Senator, we will provide a detailed answer on notice, but we have looked at a number of systems, mostly for legislation that applies in those jurisdictions, and there does seem to be a dispersion between some countries that have got onto this issue early and regulated it—and probably, some would say, overregulated it—and other countries that have not even begun. But we have not at this point done any extensive investigation as to the progress of bargaining in this area. We will do that and provide the answer on notice.

Senator CAMERON—Has there been any consultation with the peak employer bodies on the issue of workplace privacy?

Mr Fetter—To date we have only had informal consultations with them. It is a very busy time for all of the industrial players, of course, following the passage of the Fair Work Act, especially because of remaining differences between us in relation to award modernisation. The climate is probably not yet conducive to sitting down and having a constructive dialogue on an issue like

this, which is not sort of core, hard IR with contested positions but still requires a degree of trust and goodwill between the players. So we were going to wait a little bit before engaging in further consultation with them.

Senator CAMERON—You raised the issue of—

CHAIR—Senator Cameron, Mr Clarke wanted to add something.

Senator CAMERON—Sorry.

Mr Clarke—Thank you, Senators. To some extent, things are likely to progress as a result of development by the Standing Committee of Attorneys-General of these draft guidelines for workplace monitoring and privacy, which I understand have been delegated to the Victorian Department of Justice to produce the draft and consult on. We have made a submission to that. I think that the Department of Justice here have indicated that they want to have further discussions about that, which will obviously also involve employers. So one would expect that early in the new year, once the caretaker side of things has settled down in this end of the country, these types of discussions will come on.

CHAIR—All right. Senator Cameron.

Senator CAMERON—Mr Clarke, you just went to the point I was going to raise because your last point in your submission goes to the Standing Committee of Attorneys-General. You raised some concern about the voluntary guidelines and now you have said you have put in a submission. Can you take us briefly to your concern and is your submission a public document?

Mr Clarke—I am not sure what the procedures are for the Victorian Department of Justice submissions—whether they are public or not.

CHAIR—Perhaps you could find that out and let the committee know.

Mr Clarke—Yes, I can find that out. The document that was circulated as a consultation draft—I emphasise that: a consultation draft—was one that in our view was an explanatory document of the types of technologies that were available for employers to implement workplace monitoring and privacy. It was more of a step-by-step guide as to how to actually implement it, without much of a first-principles policy consideration of how you make the decision about whether you should or you should not, what process you should go through and who you should talk to about it. Those were the nature of our concerns and we hope to be able to put some meat on that in those consultations.

Senator CAMERON—Could you provide a copy of your submission to the committee?

CHAIR—They are taking on notice the extent to which it is confidential or whatever, Senator Cameron.

Senator CAMERON—Why would it be confidential?

Mr Clarke—I have no idea. I would be very surprised if it was.

Mr Fetter—Sometimes, I think even in relation to this committee, documents that are provided are for the use of the committee and generally should not be distributed, at least without permission of the committee.

CHAIR—If you can ascertain that and inform the committee, that would be helpful. Senator Cameron, do you have a final question.

Senator CAMERON—I am fine, thanks.

CHAIR—Then my final question, which I hope you can answer because I have grappled with evidence that has been given by some other witnesses. In respect of your contention that private activities by employees in their private time on their private equipment should remain private: in principle, yes, but is it possible to apply that in practice? How do you draw the line? Evidence from others that I have tried to ask about that today is that maybe there is a way but they do not know.

Senator CAMERON—Chair, just before they answer that question, can I just get some idea from you about this. I was very, very patient in waiting for my questions. I got a few minutes at the end of a 45-minute question time; you had most of that question time. We have now gone over the time when I understood the ACTU were finished. I just need some clarity from you about how flexible you are going to be in applying time and applying access to other senators to ask questions.

CHAIR—Settle, Senator Cameron. I am very happy for the ACTU to take my question on notice, if that is what you wish.

Senator CAMERON—That is good.

CHAIR—Senator Cameron, do you have further questions? I did ask you and you indicated no. I took you at voice value. Do you have further questions?

Senator CAMERON—We are over time. If I have questions I will put them on notice.

CHAIR—All right—that is your choice, Senator Cameron. Thank you. Gentlemen, it is up to you: you might prefer to answer my question now rather than having to come back on notice. I am entirely relaxed. If you would like to do so on notice, in respect of that question and others, the committee has set 16 December as the time by which we would like responses. Handle it as you wish.

Mr Fetter—If you do not mind, Senator, I will take it on notice, principally because by now I have forgotten the gist of the question. We will look at the transcript and come back to you.

CHAIR—I hope you have an answer. I would like there to be some clear criteria. Thank you for your testimony and your submission and for all the work that has gone into it. We wish you well with this issue, which will go beyond the life of this inquiry.

Proceedings suspended from 2.50 pm to 3.46 pm

[4.13 pm]

BOOYAR, Ms Olya, General Manager, Content, Consumer and Citizen Division, Australian Communications and Media Authority

O'LOUGHLIN, Ms Nerida, General Manager, Digital Economy Division, Australian Communications and Media Authority

RITTER, Ms Jonquil, Executive Manager, Citizen and Community Branch, Content, Consumer and Citizen Division, Australian Communications and Media Authority

WRIGHT, Ms Andree, Executive Manager, Security Safety and e-Education Branch, Digital Economy Division, Australian Communications and Media Authority

CHAIR—The committee welcomes ACMA. I do not think I need to state the formalities for you ladies, unless you tell me so. Please introduce yourselves.

Ms O'Loughlin—My division is responsible for, amongst other things, the range of education and research programs we do around cyber safety.

Ms Booyar—My division's responsibilities, among other things, include the spam pack, the Do Not Call Register, and content classification matters.

Ms Ritter—I deal with the content classification within ACMA.

CHAIR—Do you wish to make a brief opening statement noting that the committee has your submission to the Joint Select Committee on Cyber Safety?

Ms O'Loughlin—The ACMA welcomes the opportunity to appear before the committee today to discuss a range of key programs and responsibilities that we undertake to help Australians have online experiences that are safe, secure and rewarding. We consider these responsibilities to be especially important as the internet has become an integral part of the lives of most Australians. Research from June this year showed that, for example, 77 per cent of Australians had internet access at home, nearly one third of Australians went online for more than 15 hours a week and about 8.7 million Australians accessed social networking or user generated content sites in June 2010.

The key legislation covering privacy is, of course, the 1988 Privacy Act administered by the national privacy regulator, the Office of the Australian Information Commissioner. However, the ACMA has a number of regulatory responsibilities, which we think will be relevant to the committee's work. These provide specific protections for the use and the disclosure of personal information and include ensuring broadcaster compliance with codes of practice provisions relating to personal privacy, administration of the Do Not Call Register Act 2006 and the Spam Act 2003and ensuring compliance with some elements of the Telecommunications (Interception and Access) Act 1979.

Last year the ACMA announced its intention to review its privacy guidelines for television broadcasters after an investigation into the coverage of the boat explosion in Melbourne where two people died and others were injured. This case highlighted to us the potential for more comprehensive guidance to the TV industry and the public in dealing with privacy matters. These guidelines are currently under review. Under the Spam Act the ACMA collects data and intelligence information to identify spam campaigns and investigates and prosecutes individuals and entities responsible for sending spam. In the last financial year alone the ACMA obtained penalties totalling $22.25 million for violations of the Spam Act as well as numerous declarations and injunctions against spammers.

The ACMA's Do Not Call Register provides registrants with protection from receiving unsolicited telemarketing calls. By June this year a total of 5.04 million people were on the register. In relation to telecommunications, the Telecommunications (Interception and Access) Act obliges carriers and carriage service providers to ensure that their networks and carriage of services are capable of enabling communications to be intercepted when presented with an interception warrant. While that act is administered by the Attorney-General's Department the ACMA does have a role which is confined to enforcing compliance with the requirements on carriers to submit an annual interception capability plan to the Attorney-General's Department by 1 July each year. These regulatory roles are complemented by the ACMA's broad-ranging research and education function.

To us online privacy spans a range of issues. There are potential safety concerns associated with posting too much personal information, for instance, revealing one's address or location could increase the risk of predation or stalking. Posting the wrong type of information such as revealing photos can cause damage to a person's reputation and possible misuse of that information for cyberbullying or sexting purposes. Disclosing financial information through a disreputable personal web site may lead to identity theft and fraud. Under the brand name of Cybersmart, which I know senators will all be very well aware of, the ACMA distributes a diverse suite of cybersafety and cybersecurity programs. These target young people and those who are best able to influence young people's online engagement such as parents, teachers, trainee teachers and librarians. Our goal is to ensure that Australians have the skills, tools and knowledge to engage in the digital economy fully with trust and confidence. We recognise that building messages about privacy and the protection of personal privacy into education programs is central to achieving this goal.

We would be happy to provide the committee with a full list of our programs, and I know you have that from our submission to the Joint Select Committee on Cyber-Safety. I would just like to mention a couple of highlights. Earlier this year we partnered with the then Office of the Privacy Commissioner and the Department of Broadband, Communications and the Digital Economy to produce a 'Z-card'. This is a credit card sized fold-out pamphlet containing tips on how consumers can increase the security and privacy of their mobile phones. Additionally, in time for Valentine's Day this year we targeted users of online dating sites with a postcard promotion designed to help them protect their identity and personal information when interacting with others online.

In addition to these, we have our outreach program and our Cybersmart website, each of which contain material on how to protect privacy. In developing our programs, we work closely with key international child protection agencies, Commonwealth and state and territory

education departments, universities and industry. We welcome the opportunity to provide further information on our programs, our research or our other activities to the committee, either today or during the course of your consideration.

Senator LUDLAM—Thanks for coming along. What is the degree of coverage of the programs that you are describing for primary and secondary schools? Is it mandatory, or do schools get to opt in? That is, is it possible for a kid to go through Australian primary and secondary school education today and miss all of that stuff?

Ms O'Loughlin—These things are not mandatory, but our experience is that there is a very strong focus in most schools these days on embedding cybersafety and cybersecurity issues as much as they can in their work programs. The materials that we offer also complement other materials offered such as the ThinkUKnow program which, as you will know, the AFP have a strong role in with Microsoft. They are also doing work within schools. I think you will also be aware of the program that the Alannah and Madeline Foundation is running, which really is an accreditation program for schools so that they know what material is out there and go through a process of making sure that their schools are e-smart. I think they are getting a significant take-up of that program, which for us ties together a lot of other programs in the field and ensures that schools know what is out there and undertake a systematic program of updating their skills internally.

Senator LUDLAM—Is there any way of evaluating how many schools have taken it up and how many have not?

Ms O'Loughlin—We would have that material available for our own outreach program, and I am happy to take that on notice and provide that information to you. From memory—and I might ask Ms Wright if she has the figure with her—I know that more than 250,000 people have attended but I cannot remember how many schools.

Senator LUDLAM—Don't take too much time over it.

Ms Wright—In 18 months we have so far had nearly 7,000 teachers undertake our one-day training module. Having concerns similar to those that you have expressed, we are developing an e-learning module so all teachers can access it.

Senator LUDLAM—All I am looking for is the order of magnitude of the coverage. The 7,000 teachers are how much of the total? And, of the number of schools, how many have you reached? I am just trying to get an idea. Is it 50 per cent, 95 per cent?

Unidentified witness—We can take that on notice. We have a comprehensive database of all the schools we have visited and also all the schools that we have lined up for our program next year.

Senator LUDLAM—Thank you.

Unidentified witness—I am not sure whether the AFP have provided any information to you on the ThinkUKnow program.

Senator LUDLAM—No.

Unidentified witness—They would have that detail.

Senator LUDLAM—Thanks. We did not ask them, to be honest. ACCAN recently commissioned a report by the New South Wales Cyberspace Law and Policy Centre, and there were some quite sharp recommendations there that related to your work—not criticism, I would not have thought, but certainly strong recommendations. Can you tell us what you have done in response to that study? Is there anything that you want to draw out for us?

Ms O'Loughlin—ACCAN has produced quite a number of reports recently. Which one were you referring to?

Senator LUDLAM—It is the online privacy one in particular. They looked at you folk, the TIO and the Privacy Commissioner.

Ms O'Loughlin—Oh, yes. This is the one about complaints. In that regard we were aware of the ACCAN research. The point that ACCAN made we had some questions about because we were very much aware that they were comparing quite different responsibilities against each other in their dataset. For example, they looked at our privacy complaints, being the general privacy complaints for spam and do not call. I think there were about 16,000 complaints in the previous year for that one. Those complaints were dealt with very swiftly, so they were quite complimentary about how quickly we acted in those areas. Where it was more difficult for us was when they went to look at people like the Privacy Commissioner and compared what we do against what the Privacy Commissioner does about complaints. I would just like to draw the distinction that each of us, when we are working in regulatory spheres, have different responsibilities and different issues that we look at. Some investigations are quite straightforward. Things like the Do Not Call Register are quite straightforward: either somebody is on the register or not on the register or has given consent or not. The Privacy Commissioner, I would expect, would have quite complex investigations from time to time and they always take a bit longer. So, while we welcomed ACCAN's research, as we always do, we felt that there were some areas in there that could have been fleshed out a bit more to point out the differences in people's regulatory responsibilities.

Senator LUDLAM—If you are planning on providing a formal response, particularly to the bits that relate to ACMA, it would be interesting to see it.

Ms O'Loughlin—Certainly.

Senator LUDLAM—The Spam Act was put to us earlier in the day as a ready good example of a legislative response that had had a direct impact on the volume and kinds of spam that we get. We have been grappling with some of the really difficult issues to do with online privacy, the transnational nature of it and so on. What can you tell us about your experience of the Spam Act, which, obviously, you have a fair bit to do with? Does it provide us with a good model for law reform in other areas—those that relate to privacy, for example?

Ms O'Loughlin—I think the Spam Act does have some benefits for us in dealing with Australian generated spam. But, similarly to the difficulties we face increasingly with online

material, it is the difficulty of what you do with overseas based material. While the Spam Act has given us some good, strong powers to deal with things domestically, and we have used those quite strongly in the court action we have taken over the last couple of years, I think it is fair to say that dealing with things that emanate from outside the country always presents a problem for us jurisdictionally and practically.

Senator LUDLAM—It was put to us that one of the reasons it was effective is that there is good international collaboration and that we are part of that, so Australia has done its bit but also collaborated with overseas agencies. How do spammers get our email addresses exactly? What is all this stuff and how are they getting hold of us in the first place?

Ms Booyar—The spammers harvest addresses by a number of means. A lot of it comes from the fact that people answer spam. Our usual advice to people who receive spam is: don't open it, delete it, disregard it and report it. Unfortunately, the more people that open spam, the more spam they get. The harvesting of emails comes from all sorts of nefarious means of getting into certain databases, and they are usually illegal means as well. It is very difficult for us to determine how this happens. In my division we have a security operations section which works to break down some of the malware codes and some of the botnet activity that happens around that very thing, which is usually the case with criminal entities around the globe working together to harvest names, numbers and all sorts of other personal data.

Ms O'Loughlin—Senator, going back to your earlier point about the international connections for spam, yes, we do find that there is strong cooperation internationally on spam. We are also finding that those approaches of dealing productively with overseas jurisdictions are becoming increasingly important as internet content becomes global and as we are all looking at quite similar issues around spam, child sexual abuse material and, in quite a lot of jurisdictions at the moment, privacy as well.

CHAIR—Thank you. I have a further quick question. At what stage is the development of the industry code of practice?

Ms Booyar—Which industry code of practice are you referring to?

CHAIR—As I understand it, there is one under development in terms of online safety and privacy. No?

Ms Booyar—You might be referring to the icode, which I think comes into operation this month.

CHAIR—All right. We have already had the shouting match in respect that then.

Ms Booyar—This is a voluntary code and it is not registered by us. It will start operating this month. We have told the industry bodies and the ISPs that we will be looking to them for implementing the code as it is, particularly in relation to them acting on the reports that we provide to them for websites that have been affected, and that if they do not do that then we may move to a code that we will register and it will be a much harsher code. So we will give them some time to see how it is being implemented and whether we are satisfied that the consumer

safeguards are in place with that code. If we are not satisfied with that then we may move to register our own code.

CHAIR—Okay. Thank you very much, ladies. That completes the hearing today and it also completes at this stage the public hearings listed for this inquiry.

Committee adjourned at 4.35 pm