COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

JOINT SELECT COMMITTEE ON CYBER-SAFETY

Cybersafety for senior Australians

FRIDAY, 23 MARCH 2012

SYDNEY

BY AUTHORITY OF THE PARLIAMENT

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

JOINT SELECT COMMITTEE ON CYBER-SAFETY

Friday, 23 March 2012

Members in attendance: Senator Bilyk and Mr Hawke, Ms Marino and Mr Perrett

Terms of reference for the inquiry:

To inquire into and report on:

1. the nature, prevalence and level of cybersafety risks and threats experienced by senior Australians;

2. the impact and implications of those risks and threats on access and use of information and communication technologies by senior Australians;

3. the adequacy and effectiveness of current government and industry initiatives to respond to those threats, including education initiatives aimed at senior Australians;

4. best practice safeguards, and any possible changes to Australian law, policy or practice that will strengthen the cybersafety of senior Australians.

WITNESSES

BALSAMO, Ms Fabienne, Senior Policy Officer, Australian Human Rights Commission

RYAN, The Hon. Susan, AO, Age Discrimination Commissioner, Australian Human Rights Commission

Committee met at 10:00

CHAIR (Senator Bilyk): I declare open the public hearing for the Joint Select Committee on Cybersafety's inquiry into cybersafety for senior Australians. This is the first public hearing held in Sydney and I am pleased to note that it takes place during the NSW Seniors Week, so it is a timely beginning for the committee's inquiry hearing schedule. The committee is very pleased to be here today in the NSW Parliament to take evidence from some of our key stakeholders for this inquiry. The hearing today will be broadcast and I would like to ask a member of the committee to move that the committee authorises audio broadcasting of the evidence about to be given at the public hearing this day.

Ms MARINO: So moved.

CHAIR: Thanks, Ms Marino. Before I invite our first witness to address the committee, I would also like to ask a member to move that submission No. 31 from Communications Law Centre be accepted as evidence to the inquiry into cybersafety for senior Australians and be authorised for publication.

Mr HAWKE: So moved.

CHAIR: Thank you. I am now pleased to welcome representatives from the Australian Human Rights Commission. Thank you for your submission, which has been received as No. 2 in the committee's inquiry. Before proceeding I remind you that this is a public hearing and is being recorded by Hansard and audio broadcast. The formal requirements are that I notify you that, although the committee does not oblige you to give evidence under oath, this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Thank you once again for attending today. Commissioner, do you wish to make an opening statement before we proceed to questions?

Ms Ryan: Thanks, Chair. I want to start by congratulating the committee for setting up this inquiry. In my experience as Age Discrimination Commissioner, now an experience of about eight months, I have come to recognise what a crucial issue this is in particular for older Australians and how vulnerable they are to exploitation and abuse on the net if they do not know how to look after themselves. On the other hand, we see what important opportunities there are for improving their quality of life, sometimes in essential services, if they become confident and safe to use the net. Our research has shown that we still have underutilisation of the net. Of people over 65, probably about half of them, on the most recent research we could find, are not net users or frequent users and of people over 75, of course, it is an even higher proportion. What that means is that those people are missing out on all of the benefits that the rest of the community is enjoying—services like shopping online, banking online, but more and more the access to essential information, including the information that the government provides to Australians on their websites. Often now you find that the information is exclusively available or the service is exclusively available on the net. So it really becomes an equity issue. If older Australians cannot get access then they are missing out on the benefits that the rest of us can enjoy. We also know from our research that one of the reasons why there is such low use of the net by older Australians is that they are very nervous about frauds and scams. As the committee will have seen with the other submissions that have come forward, they have good reason to be nervous because there are a lot scams, there is a lot of money lost, and the older you are the more likely you are to be scammed. So we have two challenges here: (1) to ensure that older people can access the net, and (2) to ensure that the safety of everyone accessing the net, but particularly older Australians, is much better protected than it is at present.

CHAIR: Ms Balsamo, have you got anything to add to the opening statement?

Ms Balsamo: No, not at this stage, thanks.

CHAIR: We will just move on. Thank you for that statement. Article 19 of the Universal Declaration of Human Rights talks about being able to 'seek, receive and impart information and ideas through any medium'. A number of European countries have codified access to broadband as a legal right for all citizens. Where does Australia stand on this issue?

Ms Ryan: I think we need to look to what has been happening in Europe. In Finland, for example, there is a legislated right to have access to the internet, in Spain there is a right to have access at a controlled low price, and other European countries have followed suit. We have not done anything like that. We need to look at that as one of the ways in which we can overcome this inequity that older Australians are now suffering from.

CHAIR: What implications do you see for the rollout of the NBN?

Ms Ryan: Many implications. At the Australian Human Rights Commission we can see that the rollout of the NBN should bring many new rights and many new opportunities to Australians, including Australians in regional areas, housebound Australians and Australians who are not geographically well located to receive services. We see all that potential, and we particularly see it in relation to older Australians.

One of the objectives of the new digital world for the NBN is access to health services, and of course older Australians need this more than any other age group. We understand that we are moving into a world where, through the NBN initiative and so forth, older Australians could access their GP, nursing advice or pharmaceutical advice, or could get hooked up with their local GP centre should they have one in their area. That is all extremely valuable for an older person. You can imagine that would save them having to physically go to find the services, saving them money. Sometimes they have some impairment with their movement. Jumping on a bus and going to the next town is not simple; it is a challenge for them.

We see all the potential but, if they are not online, they will not get it. So, while we are very enthusiastic about the opportunities these new services will present, it is absolutely crucial—in terms of the human right of all to have equal access—that older people be now given the tools whereby they can take advantage of this great new investment that is being made on behalf of all Australians.

CHAIR: I noticed in your submission you talked about training in Ireland and in the UK and talked about a program that BT have. Do you have any more information on that that you can share with us?

Ms Ryan: We looked around to see what other countries were doing to see if we had an opportunity to learn and we did find programs in both the UK and Ireland. The UK has the silver surfers program and Ireland has the age connect program—I think that is what it is called. They have moved ahead of what we are doing here. They are using the community and engaging the community, particularly older students, in instructing the older people. They are also finding free ways of getting this training to older people, and that is an important aspect. One of the reasons for its success is a lot of older people, virtually 80 per cent of people not in the paid workforce, are drawing a part or full age pension, which means they have restricted assets. We think it should be a service free to the older person. I would suggest that the committee, if they are able, get some more information from those who are running the programs in Ireland and in the UK. I do not think we have anything else, Fabienne, apart from what we were able to put in our submission, for the committee at this stage?

Ms Balsamo: Just that there are also some very good materials through the BT online for tutors to work with older internet users. They are very good step-by-step guides that people can use with relatives and family should they need to. The only other thing I would say about the Age UK website is that it is incredibly user-friendly. When you go to that website all you need to do is put your postcode in on a big front page and it tells you what services are available in your region and what supports are available. The Broadband for Seniors website has much more embedded information and is much harder to navigate. It took me a while to find where my local services were. I think they have got some really good usability stuff happening in the UK.

CHAIR: I agree. Although there are great concerns and people need to be aware of security and personal settings, we also really want to encourage senior Australians to be online. As the commissioner mentioned, there are benefits with e-health and the committee has heard from the e-health people about those. There are some concerns about privacy and things. I was wondering if you have any comments to make, Commissioner?

Ms Ryan: We are aware there is a problem that older people think if they put their bank details online they will be hacked or used. I think all Australians worry about that because we do hear about such episodes from time to time. While there are quite a lot of advisory packets of information out there at the moment, a lot of them are actually online. So if you cannot get online anyway you cannot avail yourself of the advice. ASIC has some very good information and advice online but that first step of getting online is the stumbling block. If we can find ways to support more one-on-one tutoring of older people through community organisations, senior school students and so on then it will be essential that the safety and privacy aspects are dealt with. Along with saying 'here is the button' and 'this is where you turn the computer on', from day one they need to know that there will be attempts to rob them—that is what it comes down to—but there are ways they can protect themselves.

Some of the submissions you have before you have pointed out that the less you use the net, the more likely you are to be scammed. I guess that makes sense. In training opportunities, we would advocate and would say from day one bear in mind that older people are going to be anxious about this and older people, even if they are pensioners, do have resources. Some of the information we have had before us has been quite heartbreaking. Older people have been scammed, including by taking an equity loan out on their house, which is, no doubt, their only asset, to invest in a nonexistent investment. So those safety and privacy aspects have to be dealt with from day one. As I said, although there is a lot of information online, until you are competent to go online and until the

sites become more friendly than they are at the moment, the instruction needs to be one-on-one and face-to-face from the very beginning.

CHAIR: You mentioned that on Age Connect and on Silver Surfers in the UK they use young people as tutors. I should imagine that has a double whammy effect in socialisation and the generations understanding each other?

I am aware that there are a few training programs in Australia where senior people help out, but I do think there is also an added benefit there.

Ms Ryan: I agree entirely. While we know that some of the programs under FaHCSIA's NBN aged people's skills involve peers—people in the retirement village helping each other—are great, I strongly advocate programs which bring the senior or even university students in because we know in general in Australian society we have a bit of an age gap which is not helpful to either group. I am pleased to say that such initiatives have started.

I spoke on ABC radio in Sydney the other day about these issues. Chair, I am sure you are aware that there is a lot of media interest in these issues. A caller called in and said that Woollahra Council in Sydney had an arrangement with senior students from secondary schools in the council area and they were offering one-on-one training for seniors in the area. We talked about that and that seemed a terrific initiative. As soon as I got off the phone, someone rang from Randwick City Council—which is just a little to the south-east from where we are sitting—to find out how that worked. A couple of other school principals have rung me to say, 'How does this happen? How will we set up such programs?' So I have great hopes that we will see a lot of relationships between senior school students and seniors in the neighbourhood providing not only the instruction but also the opportunity for more inclusive social values to develop.

CHAIR: I am interested in whether you think there should be a mandatory code of rights or of access and things like that.

Ms Ryan: I think it is worth considering. To me, at this stage, the objective is to get the broader community aware and supportive of the need to include older people in the whole cyberworld we are living in. In terms of whether such a code would improve the protection of people, it may well do so. I would not have a specific proposal for it but, if it is something that the committee is recommending for consideration, I am sure we—as the Australian Human Rights Commission—would respond to it and give some detailed consideration. It is always good to have very strong guidelines so people know where they are and to give the users comfort.

Mr HAWKE: I am interested in your recommendations about research. We have been discussing some of the need for research in this area. One of the concerns about research that has been put to us from internet organisations and users in general is the ability for us to quickly get research as, by the time research is received, in particular in this area of endeavour, it tends to lag quite substantially behind the evolving situation. That has been put to us and I think that is a quite valid contention. Do you have any comments about research? Is it worth while allocating resources to researching this field when there is such a substantial lag in terms of the ever-changing internet?

Ms Ryan: I can understand that in relation to substantial research that goes into a whole lot of factors. What we call academic or scholarly research does take a long time to come to fruition and those of us who are looking for solutions now can be a bit frustrated. But I also think it is possible to do surveys quite quickly over a few months if you know what you are looking for and you engage those who are very skilled at doing this. I think you can get a picture quite soon. For example, I am a member of the government's Consultative Forum on Mature Age Participation in employment. That forum has commissioned the national seniors research unit, which is very capable—and you probably know it, Mr Perrett—

Mr PERRETT: They are often lobbying me.

Ms Ryan: They are very good advocates for the sector they represent and their research is very good. They are doing a very large research project as we speak about a whole lot of attitudes that are preventing older people from participating in the workforce. That research will not be specifically relevant to this inquiry but I think you will find that over a period of months they have formulated the structure and the methodology—so they are out there—and we expect to have a final report from them by May. That will give us a lot of right now up-to-the-minute information on what is stopping people from working, what they would need to change if they could find work, if they are experiencing age discrimination, if they have health issues. They are all the things that form a picture of why it is that, according to this research, two million Australians over 55 want to work and could work but are not in work. I am not here to promote the use of national seniors research, but it is a good example of having a very well experienced set of researchers who are very experienced at looking at older people's issues. So I think you would be able to get a picture from that sort of research of how many older people—say, over 65—are

on the Net or are not, what their attitudes are, what their concerns are. I think you could get that done and dusted within a year and have some really clear directions for the parliament as to what the parliament can do to improve the situation.

Mr HAWKE: Thank you for that and I understand it. I was interested in what you were saying a little bit earlier, Ms Balsamo. Taking the question about training and the recommendation you have had from the research in terms of training, I was very interested in your comment on the feedback on the website. Have you had bodies of feedback about the effectiveness of various government programs that are in place today or about ACMA's available material for seniors in particular? I would be very interested in any comments you might have about that, and if there is a real need to get more that could be useful to know as well.

Ms Balsamo: The study that interested me was the national seniors study about the number of people using the Broadband for Seniors initiative, and I think they got the surveys out quite quickly and they could report that something like 19 per cent or less were aware of the Broadband for Seniors initiative. We had a look at the ACMA research as well, but my sense is that there is not very good reporting or feedback. I think this goes to your question on research. As far as I understand it, there is not a very streamlined approach to reporting. I think there is the ACCC's SCAMwatch. That is the sort of single body to which people can report scams after the fact. Otherwise, people are reporting to their local police or the Federal Police or their banks. But there possibly needs to be a better way by which information is fed back. Some of it could be about proactive research but some might be about the way in which this is reported. I understand there is a national taskforce that connects up lots of these bodies to which people might be reporting. But my understanding is there is not a very good feedback loop.

Mr HAWKE: We have heard that before, actually. So you are talking about this single funnel by which people can make complaints, and obviously that would be valuable to senior Australians in terms of where they could go—and so that is a kind of feedback too. That is valuable.

Ms MARINO: Thank you very much, both of you, for being here. You touched on access to the internet as being a major issue. I represent a regional electorate. As we know, the NBN fibre network will only serve towns of over a thousand people. So they will have to access their services by satellite or wireless. Have you considered whether this would be an additional challenge for mature-age people in accessing the service? A number of these are in areas where they do not even have mobile access, so I wondered whether you had turned your minds to this issue and what you could suggest in that environment.

My second issue is that you have acknowledged that there are people who probably will not sign up to the internet and you touched on the fact that so many services are only available on the internet. I would be interested in hearing how you think we should be better providing information and services for people who will not—and we know there is a proportion who will not—use the internet so that they continue to be offered the services in an equitable fashion, particularly those in regional, remote and rural areas.

Ms Ryan: In relation to your first question, whether the technology of the satellite and wireless will give equal opportunity to those seniors who are able to get themselves some training, I guess that is a bit too technical for me to answer, but I think the intention is that where the NBN will not go—

CHAIR: It is a commitment.

Ms Ryan: It is a commitment; therefore, it will happen, I guess. A lot of this—future commitments and so on—is important and we take it seriously. I suppose, as Age Discrimination Commissioner, I am very concerned for now—for the people who are old now and need better support now. If you say, 'Well, in five years time you will have such a thing,' that is fine for those who are still there, but it could be five years of great hardship. It is a big issue. Services exclusively on the net concern me: first of all, because so many people cannot—or sometimes will not but usually cannot is a better description—access those services either for the geographical reasons you have given or for other reasons. I would hope that government policy at least takes that on board and continues to provide information through what we might call traditional media.

We have advocated that in our submission. We know, for example, that older people listen to radio a lot and I think that radio is a prime medium for information. We know that they like print and, although mainstream newspapers might be declining in their circulation, there are still a lot of local newspapers. I would imagine in your electorate there would be, and certainly around the suburbs of Sydney there are all the free local newspapers. They are a very good platform for information. Because they are free and because they are dropped outside everyone's house, people do read them.

Mr PERRETT: Very trusted.

Ms Ryan: I have found that they actually give more attention to the circumstances of older people in their various areas than the mainstream media. Government should look carefully at those things with its own

advertising and information campaign. Then, of course, there are the seniors magazines and so on for those who are members of National Seniors, and we are told 250,000 seniors are. I hope some of those are in your electorate because the organisation provides a lot of services.

Businesses should be made aware that they cannot assume that they can run their business entirely on the net. There are a lot of people who want and need what they are offering who are not on the net and, although the latest move is that every retail business needs to be on the net, at the same time the old face-to-face service is still important—more important, of course, in our regional areas. I think the twin strategies should be pursued, certainly by government in its programs but also by businesses who are trying to reach these people. Do not assume that everyone is on the net.

Ms MARINO: That is the very point, I think, that is worth keeping in the front of our minds. We probably have a proportion of at least two decades perhaps or more of people who for various reasons will not trust or access, or be able to access, the internet and we have to make sure that those services and that information and all that they require continues to be available. I would be interested in anything further that you have to add on that.

Ms Ryan: It is certainly our position at the Human Rights Commission that human rights are everywhere and for everyone, and they do not diminish because you live in a certain area and they do not diminish because you are getting older. Our basic position is that we advocate for everyone's rights to be met equally. In this particular case it does mean providing information through media that the people can and will receive. So we agree. If you would like us to come back with some further discussion points on how that might be achieved, we would be very happy to do that in the future.

CHAIR: Thank you. That would be really helpful if you could do that. We might move now to Mr Perrett.

Mr PERRETT: Thank you, Chair. Ms Ryan, I was just wondering if you could go back a bit to the program that you talked about on the radio about of the year 12 students being the guides for the older Australians. I did not have the benefit of hearing you on the radio. Could you talk about it a bit more. It seems to be an ideal scheme that would work in a small town or a big town—

Ms Ryan: That is right.

Mr PERRETT: and be a good two-way street.

Ms Ryan: Every town has got its high school and these days I am very happy to say I think every secondary school builds in some sort of community service activity.

Mr PERRETT: Yes, I think it is almost part of the curriculum.

Ms Ryan: As part of their curriculum, definitely. That is extremely important and to be welcomed. I think every town, no matter how small, has got a school, it has got old people and it has senior secondary students. Those senior secondary students, even if they are in the regional areas, will certainly be finding how to get on the net and how to use it all, because it is their generational basic way of communicating. So I think that idea where they can be brought together with older people has to work.

We know that Telstra's Connected Seniors program does provide some funding. The committee perhaps has had a discussion with Telstra. It is not really for me to give you the details, but I have to say that at the commission we were impressed when Telstra came in to see us to tell us what they were doing. There are grants—I think quite small grants—but ones which would certainly assist a school to set up the basics, and I think there grant would cover the actual hardware.

For those people living in areas that have that wonderful institution, the local library—and I hope they are still there in most places—the library is an excellent place.

Mr PERRETT: We just built 3,000 of them over the last few years—school libraries, admittedly.

Ms Ryan: Well, the school library—

Mr PERRETT: A community facility.

CHAIR: There is access to the public.

Ms Ryan: That is right. It is a place that is easy to get to, the students are there, the seniors can come in and would enjoy coming into a school library. I think it would be a very pleasant thing for seniors to come in and see what the students are getting up to and so on. So, look, it is there. On the funding aspect of it, as I said, there is the FaHCSIA program and there is the Telstra program.

I have not explored this but there are probably other commercial organisations that would like to facilitate this—the hardware retailers and so forth. They would probably see it as in their interest and also as a bit of a social service to provide this.

Mr PERRETT: It has been a long time since I taught English but even then there was a local history component—in the curriculum in Queensland; I don't know how it is in other states. Tart of the program required of year 12 students was to engage with local people and tell stories. So it could be a great two-way street.

Ms Ryan: I think that is absolutely right. Another thing that the Human Rights Commission has been involved in recently is making submissions to the national curriculum project—the ACARA project. We have made a number of submissions about ensuring that the new national curriculum reflects basic human rights and equal opportunity and equal access principles. I am hopeful that the new curriculum will even more require community development. So I think there are a lot of strengths in that. It is not a high-cost exercise. If there are costs there seems to be some funding available at least. Also it is the kind of program that, if the school did not have the funds to get the resources, local community organisations I think would find that a very natural project to support.

Mr PERRETT: Thank you.

CHAIR: Commissioner, I wanted to go back to that code of rights and suchlike that I mentioned earlier. The Consumers Health Forum of Australia in their submission expressed concerns about older people being coerced into nominating other people—maybe with caring responsibilities or just being coerced by, for example, family members—into giving access and control of information about their personal electronic health records. We have heard evidence about the benefits of people being able to have their pharmacist and their medical people—their doctor, their physiotherapist, their psychologist, whatever—have access to what treatment people have had and their health records being online. I am just wondering whether you have any comments to make in regard to making sure people are empowered are not disempowered by these processes government is trying to implement.

Ms Ryan: The Privacy Commissioner would have a role in giving you very direct advice. Also, I was actually in this building—the New South Wales parliament—earlier this week addressing a Council for the Ageing, COTA, meeting. There was a lot of discussion then about the codes of practice in residential care and the view put that, although there are codes that sound wonderful when you read them out, they are actually not often properly implemented.

There was also concerned that people going into residential care while they were still mentally healthy should be looking at things like wills, guardian arrangements and the arrangements that give instructions about your health care should you become incapable. Those sorts of things are very relevant to what you are asking about. They are not specifically to do with the internet but they are to do with the older person having control of their own information and having protections. It is also anticipating that they might not always be able to control their own information and then being very clear in their legal arrangements—if they have to give the responsibility to another person, then it is someone they trust and someone who understands what the responsibility is. So that whole cluster of protecting older people's legal rights does require attention from the parliament.

CHAIR: Thank you. Does anyone else have any further questions for the commissioner. There being no further questions, Commissioner, I would like to thank you very much for your attendance today. It has been very interesting hearing from you. The secretariat may well be in contact for further information. We look forward to you sending that other information to us. Thank you for your time.

Ms Ryan: I thank the committee.

BUNKER, Mr David, Head of Architecture, National E-Health Transition Authority

HAIKERWAL, Dr Mukesh Chandra, Head of Clinical Leadership Engagement and Clinical Safety, National E-Health Transition Authority

[10:46]

CHAIR: Welcome. Thank you for your submission, which has been received as No. 4 in the committee's inquiry. Before proceeding, I remind you that this is a public hearing and is being recorded by Hansard and audio broadcast. Do you have any comments to make on the capacity in which you appear?

Dr Haikerwal: I am also a GP in Melbourne's western suburbs.

CHAIR: Thank you. Although the committee does not oblige you to give evidence under oath, this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Mr Bunker, do you wish to make an opening statement?

Mr Bunker: Thank you for the invitation to provide a submission to the Joint Select Committee on Cyber-Safety to assist in its inquiry into cybersafety for senior Australians. The National E-Health Transition Authority was established by the Council of Australian Governments. NEHTA's board includes the directors-general and secretaries for health for Australia as well as two independent board members. NEHTA is the lead organisation supporting the national vision for e-health in Australia, working with consumers, healthcare providers, the ICT industry and governments to enable safer, higher quality and sustainable health care.

The National E-Health Transition Authority is the managing agent for the development of the personally controlled electronic health records system on behalf of the Department of Health and Ageing. The personally controlled electronic health records system enables the secure sharing of health information between an individual's healthcare providers while enabling the individual to control who can access their personally controlled electronic health record.

Our submission to the joint select committee addresses the terms of reference of the committee from the perspective of the National E-Health Transition Authority's role in shaping e-health in Australia and covers our understanding of cyber-threats to older Australians relating to e-health, how the personally controlled electronic health records system will benefit older Australians and how the personally controlled electronic health record and other e-health initiatives incorporate best practice cybersafety safeguards.

Older Australians are one of the key target groups in the community likely to receive the most immediate benefit from having a personally controlled electronic health record and e-health initiatives more broadly. The National E-Health Transition Authority recognises that older Australians are more likely than the average adult population to access health information via the internet and that they are a more vulnerable group in terms of cybersafety. We note that the benefits of participation for this community are centred on improved continuity of care, thereby enabling improved management of chronic disease, improved coordination and follow-up post acute episodes, reduced adverse drug events and improved personal control over health information. In order for Australians to fully benefit from the personally controlled electronic health record system it must be safe and easy to use. Through our extensive consultation on e-health and the personally controlled electronic health record system we note that older Australians may need additional targeted measures and education to reduce risks to identified threats. In the design and development of e-health systems the National E-Health Transition Authority is implementing numerous controls to safeguard both services and those who will be using them.

The National E-Health Transition Authority recognises and seeks to uphold the objectives of the Commonwealth government cybersecurity strategy, in particular that the Australian government ensures its information and communications technologies are secure and resilient. The National E-Health Transition Authority has also developed a national e-health security and access framework, which is a set of tools designed to support both public and private organisations in national e-health. The framework encourages business to adopt a consistent approach to the application of health information security standards and provides better practice guidance in relation to e-health-specific security and access practices.

The personally controlled electronic health records system will also support the receipt, tracking, management and escalation of inquiries and complaints. Individuals who are unhappy with the way their health record information is being handled will have the ability to make a complaint through the personally controlled electronic health record system operator and, if they are not satisfied with the response, they may escalate their complaint to a range of regulators, including the Australian Information Commissioner and state or territory privacy or health service regulators where relevant.

In addition to establishing effective security, access and authorisation mechanisms within the personally controlled electronic health record system, a legislative framework that provides clear, transparent and flexible oversight of the operation of the system as it develops and evolves is required. Committee members will be aware that earlier this week the Senate Community Affairs Legislation Committee completed its examination of the legislation underpinning the personally controlled electronic health record system and recommended passage of the bills.

In closing, I would like to assure the committee that NETA is fully aware of the unique needs of older Australians in using and accessing the internet. The PCEHR will help older Australians take more of a role in managing their own health information, and we are working with the relevant stakeholders to assure it is a system that will meet their needs and provide them with a level of confidence that their personal information is safe and secure. It will in fact provide improved security. The PCEHR will be more safe and more secure than some current recordkeeping practices. I am very happy to take questions.

CHAIR: Thank you, Mr Bunker. Dr Haikerwal, do you have any opening comments you would like to add?

Dr Haikerwal: No, thank you, Chair, but I would request an opportunity to have a summation at the end.

CHAIR: Okay, thank you. I might kick off. You mentioned in your opening statement that complaints will be able to be lodged. I have the concern that if there is a need for a complaint it is probably all a bit too late—that your information has been sold on or misused in some way—but you also mentioned that the site will be safer than some other ones. Without giving away any security secrets, can you expand on how the site will be safer?

Mr Bunker: The PCEHR system is a set of core infrastructure that operates as a system interacting with clinical information systems in what we would describe as endpoint clinical settings: hospitals, general practices et cetera. As a system, the security and access framework has to be able to cater for all of those environments and the technology being deployed. The architecture or the design of the PCEHR system incorporates the mechanisms by which security can be deployed so that as clinical documents are being exchanged through the personally controlled electronic health record system they are encrypted during transit and also digitally signed appropriately to ensure things like non-repudiation and elements around the auditing and controls of that information.

The PCEHR infrastructure system has a range of security controls that are both technology and process oriented in line with best practice standards around ICT and security globally, and making use of Australian government frameworks and requirements around security and access—for example, the use of the national e-authentication framework, which describes the best practice government approach to dealing with e-authentication so that users, consumers and clinicians can interact and get access to the system and the information. In addition, there are a lot of technology options that are available for managing things like intrusion detection, so we can monitor for inappropriate interactions with the system. We will be deploying a range of technologies to assist us in those processes to be able to understand where inappropriate access is occurring, where we can identify that and ensure we have good auditing and evidence trails to support investigations post a breach or where, if someone suspects a breach, we can manage that.

Mr PERRETT: My question is twofold. My office is in Sunnybank, across the road from a private hospital and surrounded by GPs and specialists. The current health system in terms of exchange of information would seem to be quite ad hoc.

Dr Haikerwal: There is none.

Mr PERRETT: I was going to be a bit polite, but thank you, Dr Haikerwal. Any system is as strong as its weakest point. There is no point putting great security gates out the front if you have left the back gate open. At the moment I see it literally being carried around between offices, exchanged between GPs, all for good reasons and with the patient's best interests in mind. But there seem to be a lot of gaps in the current system. If I can have a response to that. And where do we sit compared to the rest of the world in terms of these personally controlled electronic health records? Are we the vanguard or are we catching up?

Dr Haikerwal: May I ask David to carry on after I say what I am about to say. We work the system a bit as copilots. David is the architect, from a technical point of view, and I as a clinician would be the other copilot to ensure that what we are doing works in the clinical space. To me, what we predicate the whole of the agenda on is: I do not want anything today to destroy what I have already got. What I have is a security system that is based on trust within the practice. We do not want to diminish that, so any system that interferes with, in my case, the doctor-patient relationship or the health professional-patient relationship will not be tolerated. That was very much upfront and central in the deliberations we have put into the system to ensure that the rights of the patient to ensure the records remain safe are not diminished. My consultation depends on having absolute trust with a

patient and on the revealing information, which they do not want anybody else to know about. That has been carried forward from the paper world into the electronic world by the safeguards that David has spoken about.

Yesterday I caught a superhighway to nowhere, because 98 per cent of general practitioners use IT for clinical purposes. Within the practice it is really quite secure. The problem arises when you need to send information to the specialist hospital across the road from you or the specialist down the road from the general practice, not so much in Brisbane, by the way, because you are actually the vanguard in many ways—

Mr PERRETT: I am on the south side, not the northside. I know the northside has been at the vanguard of this for years.

Dr Haikerwal: In fact, the south is catching up. You are joining forces to make this more joined up. That is the key thing about joining it up—you have to make sure the information gets to the right person, to the right place and at the right time securely and that it can be trusted. That is the part of the work we have done: to get it to that place. We are seeing that the information being transferred relies on safeguards in the technical world, because it is done in the electronic world. In my practice, someone can come in and take out records, anybody can read them. We have seen cases in Melbourne where footballers' records have ended up in the gutter and been found. That sort of thing happens today in the electronic world. Only people with the right levels of authority can get into the system, look at the system, use the system. To look at the patient's electronic health record, which is the next piece of the work, they need the patient's permission to access that. So where we are going is from a fairly ad hoc world to a much more coordinated world where we get information flow at the right time, not where it happens to turn up, which then informs good clinical practice, better patient care and care coordination. So we actually get a much better joined up system. From the security point of view we are going from a system where nobody knows who is looking at the records sitting in the practice or in hospital, or wherever, to where we know, for somebody who happens to be there and is allowed to be there, that either patient could access a notification that has been done, and they can question that. I agree that the notion is that we do not want anyone to get information without permission if they go to a place where they should not even be. Unfortunately, in the real world, that does happen. We are mitigating that to prevent it from happening and, if it does happen, to repudiate it.

Mr Bunker: To add to Dr Haikerwal's information, the premise of the application or adoption of e-health is one that is underpinned by an improvement in security and an improvement in access control. More importantly, as Dr Haikerwal said, it connects the dots and joins those things up, and understands that there are clinical workflows that happen within organisations and more broad-reaching business processes that span those different organisations to transfer that information in an effective manner. That is one of the benefits of e-health.

From our perspective, in terms of not only the personally controlled electronic health record system but also, more broadly, the work that NEHTA has been doing for a number of years around e-health, we need to define in a standardised fashion what those key strategic clinical payloads—as I described them, things like discharge summaries, referrals, electronic medications, prescriptions et cetera—are. We need to define, conceptually, what information needs to be handled and what is relevant to a clinician. Logically, we need to know how to express that data so it can be interoperable, which means that the systems and the human beings interacting with it can understand it, that it is meaningful and clinical safe. On a technical level, we need to know the appropriate standards and technologies that we can deploy to transmit the information in a manner that can be readable by both computer systems and human beings, as well as those technologies we can apply to make sure it is safe and secure, to validate a digital signature so that we can know whether that clinical payload has been tampered with in transit.

The reality is that there are processes that go on in clinical practices that are beyond the control of simply defining, from an e-health point of view, what is on the wire. We might refer to that as the difference between data in transit and data at rest. In order to support the market, NEHTA has developed a National E-Health Security and Access Framework. It is important to understand that, essentially, what the NESAF does is provide a better practice guideline for healthcare organisations in understanding how they apply good information security policies and practices in their organisation. But in understanding how the market can adopt that framework, it is really important from our perspective that in gaining the support of NEHTA's board to do this work we did not produce something that was what you might call 'shelfware'—we produced something that was relevant, timely and contemporary. We are actively applying that framework by, for example, supporting jurisdictions that are undertaking identity management projects or web based patient administration systems, and working with organisations like the Royal Australian College of General Practitioners to support their security guidelines. We realised that, to be applicable, the framework has to have adoption, and you have to find the right channels into the various parts of the market to get that better practice education there.

That is our approach from an e-Health perspective. From an international perspective, this is something that NEHTA is engaged with. NEHTA is blessed as an organisation with a number of world-class experts in the fields of both security and clinical informatics. We have a number of people in our organisation who are literally world-class experts and who sit on various organisations internationally to do with standards development organisations from both a security point of view and a clinical terminology perspective. I am a board member of the International Health Terminology Standards Development Organisation and the chair of their technical committee. We are driving the clinical terminology and, from a security perspective, we are able to adopt those approaches.

Australia has a unique environment when it comes to e-Health in the way health care is provided, funded and delivered here, but there are a lot of lessons that we can learn, not only from the way that organisations are exchanging information directly between providers, in that traditional e-health sense but also from certain countries. For example, the National Health Service in the United Kingdom has developed its summary care record, which is designed to present summary care information to consumers. We are actively involved in working with those international organisations to learn lessons, and they are also very interested in what we are doing. So we are learning those lessons and applying the good techniques—learning from the mistakes of people who have come before us and working with organisations that are following us as well. It depends; it is not that one country is ahead of the other on a total program. There are elements of the program, and we understand that granularity.

Dr Haikerwal: I have the benefit of travelling widely internationally with my role on the World Medical Association. When I do go to international meetings with that organisation, which I now chair, I do meet the various people working in this space. I have the ability to speak with governments because I come from this sector, from medical community, and I also get the feel locally.

There are many things that we are excelling at in Australia, and the world is actually watching us and the way in which we are doing it. In particular, the element of personal control is something that people are very keen to see how it runs for us. The other part of it is that we have this situation where we have clinicians working very much with the technical teams.

To make this successful we need to make sure that clinicians are involved and working closely with technicians. By doing that, we are learning those lessons that my counterparts and David's counterparts internationally have fallen into a bit of a trap about. In fact, it has not been so much about the technology that has fallen down but the people management and the change management. It has been very badly thought through and so reasonably good systems have actually not come to fruition.

CHAIR: Mr Bunker, there have been calls for the process of PCEHR to be delayed until 2013. I am just wondering if you could quickly—because we are limited for time—tell us about how the process is working and whether it will be okay to be launched in July 2012 as the deadline is. Can you give us a quick report on the process and progress of the system, about the implementation plan and the take-up of targets?

Mr Bunker: I can talk about NEHTA's accountability and responsibilities in the program. Obviously, it is the Department of Health and Ageing's program. I will provide a very brief summary and Dr Haikerwal might like to add to that.

We talked about clinicians and technologists working together and I think that certainly at this stage the really important element that is part of that group is management, and that effective management of the program and the plan is also key. In terms of our understanding, at the moment our project is on plan and we are expecting to have the capabilities that have been declared for the personally controlled electronic health records for day one. I think that the other questions you have about the process and those sorts of things are probably best addressed by the Commonwealth—by the Department of Health and Ageing. Unless you have a specific question about NEHTA's role?

CHAIR: First of all, does NEHTA's contract—I presume that you have a contract—expire in July 2012? Or do you keep working with PCEHR?

Mr Bunker: We might need to take some of the answers on notice, if we could.

CHAIR: That is fine. Anything you want to take notice is great, because you might be able to give us a bit more information than time would permit today. Are you able to tell me anything about the implementation plan and its take-up target, or is that a question I should put to someone else?

Mr Bunker: I think that falls into the same category. If we can provide that on notice then we can give you an accurate picture of what is going on. Obviously, it is a very quick-moving program and there are a lot of things going on. It is probably best for us to provide those on notice.

CHAIR: Okay, we appreciate that and we are happy for you to do it.

Mr HAWKE: I just want to turn to another part of your submission in relation to users. The change management thing is something that I am quite interested in. I have a lot of faith in your technical capability, design and management, but like a lot of internet usage and cybersafety, which the committee is responsible for, it is about behaviour online and the relationship with humans and individuals. I am concerned about people's ability to give carers or family members access—particularly senior members, who may have health impairments or other issues. What kinds of mechanisms are you specifically looking at just to help manage those situations? Obviously, there could be a lot of circumstances arise with a personal record controlled by a senior Australian who has care or a family member or access to them.

Mr Bunker: This is really about the access controls that can be applied around the system. I would state that what I say is in the context that education has to be provided, and all of those sorts of things as well. This is just from a technical perspective, if you like—and this information is available in the concept-of-operations documents, so I am referring to that information. There are essentially four parties, if you like, actors, that can access information in the PCEHR: the consumer, an authorised representative, a nominated representative and health care organisations—health care providers. In terms of what I understand you are referring to, it is those carers of elderly Australians. The access to information is within the control of the consumer, the individual. As the individual who has obviously opted into the system, they can create access controls that allow other individuals to have access to the information, over and above a range of controls that you can apply to your healthcare organisations in terms of a general access list and a more detailed access control to particular documents within the system. But, ultimately, it is the consumer's choice, and there are a range of controls that can be provided.

Mr HAWKE: Controls are one mechanism. What about reporting? Do you have online reporting mechanisms and things like that? You are using all the latest practices?

Mr Bunker: The system incorporates a notification service. The notification service is something that individuals can choose to switch on. That notification system once again comes with a range of controls about what sorts of events that are occurring around their information can be reported on and how that is reported back to them. Obviously, there is a range of channels of how that information could be available, in a very electronic sense—for example, email is an option—as well as being able to actually go into Department of Human Services Medicare offices and shopfronts to get access to that information as well.

Mr HAWKE: That is good.

Mr Bunker: So it has to be a range.

Mr HAWKE: Yes, there is a range. Have you given any specific thought to senior Australians who may have limited skills in this area, in terms of how you deal with that?

Mr Bunker: Certainly, in terms of it being a system which is compliant with the Disability Discrimination Act and accessibility guidelines. Obviously, those sorts of things are there in the system. So the consumer portal, the electronic interface for a consumer to the system, is compliant with all of those standards and requirements. In terms of additional information, I think this now falls into that education domain, where it is important that we have targeted information for particular groups that may be more vulnerable. And not just around their vulnerability but around the aspects of the sorts of services that they are trying to access and their expectations of the system, because I think your point about the human element is very important.

Mr HAWKE: Yes, very much so. I agree with you on that. Just quickly, what is the first layer of reporting? Is it your organisation that handles the first level of complaint or does it get referred to the department?

Mr Bunker: The complaints and inquiries are managed by the personally controlled electronic health records system operator. The operator has a function around being able to handle complaints and inquiries et cetera, and obviously there is a range of ways to do that through a call centre scenario. I understand that there is, within the nature of the operations, the ability to coordinate inquiries that may come through a number of different channels and sources, and also a desire to seek a coordinated approach for individuals who are in different jurisdictions, who are potentially under different regulations and different legislation, around the way their health information should be managed and complaints et cetera handled.

Mr HAWKE: Yes, I understand.

CHAIR: Having taken into account all the privacy and safety issues and things, we do know that seniors in general have not had a huge uptake of online activities. Is the process going to be senior-friendly for them to use?

Mr Bunker: The best way to address that is to say that it will, in terms of developing educational material—supporting information that supports people. For example, if someone is constructing a password: what is the concept of a safe password—is it a string of characters? There is support for those sorts of things. The nature of that material has to be directed to a varying level of computer literacy, if that makes sense. Rather than singling out a group, I think it is probably more accurate to say that there is a range of educational and support material that is presented in line, as you are doing the operations, and also to augment and be beside that in terms of other information that can be accessed. There are a range of channels by which that information can be accessed and there is a range of literacy support for people. We work very closely with our stakeholders because that is the best way for us to understand their needs. I would not single it out as being elderly friendly; I think we need to accept that there are different levels of sophistication, maturity and literacy around the use of technology, and a system, to be safe, secure and easy to use, has to allow for that.

CHAIR: The reason I asked the question was that seniors and the elderly are a bit of a target for the rollout, so it could have implications.

Dr Haikerwal : To add to that, the key here is to work very closely with the sector. The National Aged Care Alliance is a group that brings together many of the peak bodies working with older Australians. Many of the consumer groups we have are chaired by people—including one of the people in our audience here, Mr Peter Brown, my friend from the Consumers e-Health Alliance—who are younger older Australians in their own way and are far more skilled than I and many other people are in the technical space. We rely very heavily on what their needs are and respond to those needs.

The other thing is access. It is not just about the individual's ability to access the material but about having the IT to work the system and the broadband connection. One of the things we are doing is working closely with the broadband system to make sure we have good connectivity so we can get the information in a timely manner that they can read. It is not just about the size of the print, but the speed of the access.

Ms MARINO: Thank you for being here. Given that this inquiry is focusing on seniors, I am really encouraging you to make sure that the process is very simple, because they have a great diversity of knowledge and experience in using not only computers but the internet as well. It needs to be user friendly across the various levels of competency and it needs to be very simple and something that they can have confidence in. I know you are probably working very hard on that, but I do know that the skills of the seniors in my electorate vary considerably. I want them, if it is available, to be able to use the internet and feel safe. I think that is important.

The second thing is I am concerned about the complaints process in the way that you have explained it, particularly for seniors. If a senior person does have a complaint—as I understand from the way you have explained it—it goes from one to the other, to the other and then to the other. That would be very difficult for a senior person to pursue—in fact, it would probably prevent them from doing so. A call centre is one thing, but you said it would go from one agency to another, and that does bother me. Dr Haikerwal touched on a very important fact: the most critical thing underpinning our health system in this nation is the trust between doctor and patient. The first time we have a breach here, it will compromise what can be achieved with any form of electronic health, particularly in the seniors group. How they navigate their way through that process of complaint, who is ultimately responsible, what actually happens then, how the seniors know what is going to happen and what redress they have in a simple form are important questions.

The other thing I would be very interested in is the centralised repository of information that will be collated. I would say that will prove to be significantly attractive to a broad range of groups who may well have a reason to want to access that. We have previously seen breaches in those sorts of areas with access to information. Some of those are subject to hacking as well. I would be interested in your comments on the management of that centralised repository of information and what you know about it. I see it as a commercial opportunity for some.

Finally, I want to talk about the systems at a health provider level. I noticed, when you spoke of access and how this would be tracked at a health provider level, there may be more than one person who has access to the information throughout this chain. The tracing of that, the accountability of that, I think will be very important to seniors and to the integrity of the information. So I am happy if there are any comments that you have and if there is anything you want to take on notice.

Dr Haikerwal: I might start from a clinical point of view—how it works from our point of view and why it is important to us as clinicians as it would be for the people we look after, our older Australians. David will talk a bit about how this is handled from a technical point of view.

You are absolutely right. This is not simple. Anybody is going to have difficulty navigating it and we have to make sure that we are doing this in a transparent way and in a way that we can navigate. If they are going to put

safeguards or other limitations on who can access and read the record they can do that in a way that is user-friendly—for want of a better word.

In fact, only this week we did some testing on how that could look and decided that it is too difficult. We want to come back and take your words to heart. The important thing to do is to make sure that it is kept simple. The way in which this works in a practice means that the way practices and health facilities and any facility using a PC or a computer system work, is to remember the basics. In other words, if you are using a password, use it yourself and do not leave it open for somebody else to use. That applies as much to a consumer going to an internet cafe and looking at their information as it does to a health professional in their practice leaving it for somebody else to look at. In a hospital ward if you have one log on and one user name and anybody can look and write things we do not know who it is.

In a real situation, where we need to log on and log off we need to have what we call the 'provenance of information' defined. Every health practitioner has an individual health identifier, from a health point of view. Using that number each time you log on and log off you know exactly who has looked at that information. In a practice it is a similar situation, where the practice manager or whoever is looking after the record can determine who is looking at the record.

In fact, at a practice level, once you have got into the practice there are log-ons, anyway. It is about good practice around what the clinician will do as well as the actual technical basis behind that. Those are sorts of comments that I would make on your points. Complexity is really very important, I agree.

Mr Bunker: Just to provide some additional information, firstly I will clarify. My apologies if I was not clear in terms of the nature of how complaints are handled. It is our understanding and expectation that the Commonwealth, in collaboration with states and territories, is developing proposals for a single entry point for PCEHR privacy complaints. So the PCEHR operator will provide the inquiries and complaints mechanism. There is certainly an expectation that the way those things are handled there is a mechanism by which that single entry point can be developed. Hopefully, that provides clarity around the statement I made.

Ms MARINO: It does. That is the process but what happens then? For instance, I have some wonderful, very prominent seniors in my electorate. One of them could have their information and their health—something that is particularly critical in their background—splashed on the front pages of a local newspaper. This is what is likely. So what happens then? This process will be particularly important.

Mr Bunker: Absolutely. We agree.

Mr PERRETT: To calibrate, what is the current situation if that occurred right now?

Dr Haikerwal: Thank you for both questions. We have a set of privacy principles in every state bar WA, and the privacy legislation, which is quite strict about how health information is recorded, managed and shared, and which people have access to it. And there are disincentives for doing that in an incorrect manner.

They would continue and we have another layer of security around this, because this is now done in a much more rigid way that can be locked down better, can be recorded better and traced better because there is an electronic trail that we do not currently have. Nonetheless, it must be kept absolutely simple, and people should know where to go to with a complaint. The local complaints will be made at a practice level, initially. Today in my state of Victoria the Health Services Commissioner has a role to play. The privacy commissioners are working towards some of the stuff at a state level. Certainly the Office of the Federal Privacy Commissioner has a significant role to play in this, as well.

Ms MARINO: You touched on the practices; you have a start-up date of—June?

Dr Haikerwal: 1 July.

Ms MARINO: Do you have accurate data on how many practices throughout Australia are ready to rock-and-roll with this because they have the technology and the systems and are ready to go?

Dr Haikerwal: I will need to take that on notice.

Ms MARINO: Thank you, I would appreciate that.

Mr PERRETT: Further to Ms Marino's question, in the current process to become a GP, establish a practice, obtain a provider number and all those things, there is an element of needing to show awareness of confidentiality and the keeping of records and the like. I understand that it is quite a burden for GPs, which is why they often have other people step in and do some of this, because they wanted to spend the time treating patients rather than dealing with files. Would you explain the current training and requirements? We are not starting from scratch here are we?

Dr Haikerwal: Some people may not want to have a Medicare provider number, but most people do have one and most people do write it. There was a time when people would not write their Medicare provider number, but now they do, because it makes the patient's journey more straightforward. There are the usual qualifications that are signed off, for Medicare purposes, by the Department of Human Services Medicare. The level of recognition of your specialty qualifications, whether it is general practice or a different specialty, needs to be noted because that gives different levels of Medicare access. When we come into the health professional role, it is actually the medical registration authority—AHPRA, the Australian Health Professional Registration Authority—that registers all the nearly 500,000 health professionals at the moment and will register those in the future. That registration process is quite rigorous. The feed for the health identifiers, which were passed by the Senate on 24 June 2010, depend on the health professional agency for the feed of health professionals who can then access the system.

The security and access framework, which has been worked through with professional organisations, with consumer groups, obviously with the governments of Australia, and indeed with the software providers, has been to say: 'This is what is required to make the system function safely'. It allows you to know who the person is, the level of access they have and what organisation they work for, so you can then determine the providence of the information. This is not necessarily for an audit trail or for being punitive, but actually to know that if I am going to use this information that we are spending a lot of effort to collect and share it is of a quality and there is a surety that it can be used for clinical practice and to escalate problems from one professional to another—for example, if there are problems or if people have not got better from whatever treatment there has been. So it is a very integrated way of delivering health care. It is much more joined up between providers and the patients they look after and also the systems—public, private, hospital, out-of-hospital, aged care, home care. A variety of agencies are involved. We have a great system internationally and it works well, but we can do it better. We need to do it better, because we will have a much better, more sustainable healthcare system if we do it in this way.

Mr PERRETT: Under the current punitive arrangements for people who breach privacy, such as the records that were found in the street in Victoria, you can go through the civil courts or through the privacy commission. What is the stick that the privacy commission has?

Dr Haikerwal: For a medical practitioner or health professional registered with AHPRA it is very savage: you could be struck off and not be able to work and provide food for your family. You do not take a risk with the actions of the registration authorities lightly. There are also criminal punitive arrangements.

CHAIR: Thank you, Mr Bunker and Dr Haikerwal, for giving evidence today. We have run out of time, but the secretariat will be in contact with you should we require further information.

BOSLER, Mrs Nancy Deloi, President, Australian Seniors Computer Clubs Association

[11:29]

CHAIR: I welcome the representative of the Australian Seniors Computer Clubs Association to the table. Thank you for your submission, which has been received as No. 7, to the committee's inquiry. Before proceeding, I should remind you that this is a public hearing and is being recorded by Hansard and audio broadcast. It is a formal requirement that I notify you that, although the committee does not oblige you to give evidence under oath, this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. you wish to make an opening statement?

Mrs Bosler: I would like to, thank you. The Australian Seniors Computer Clubs Association, ASCCA, welcome the opportunity to make a submission to the Joint Select Committee on CyberSafety's inquiry into cyber safety for senior Australians. I thank you for the opportunity to represent ASCCA at this public hearing—how good that it is during New South Wales Seniors Week 2012.

CHAIR: We have timed it well.

Mrs Bosler: You did indeed. If older people are going to be able to reap the values of using technology and the internet for communication, e-health and e-commerce, we must address problems of access, including cost and training. We must protect them from issues that compromise cybersafety as they try to achieve access and equity in this age of technology. Seniors may be one of the fastest growing age groups taking up the use of the internet, but they still represent far too low a percentage of that community low. Projected figures show a rapid increase in the number of older Australians, making education and skills training essential if the increasing use of websites to disseminate information is going to work. The NBN has the potential to bring great opportunities to all Australians, but seniors need to be educated and informed so that they can use a computer and access the internet safely. They must be helped to understand how to protect and secure their computers by being able to identify online security threats, make transactions securely online and help their families to be safe online. Education is badly needed.

The work being done by the national cybersecurity awareness committee is providing valuable, plain English and well designed material to help inform older people. It needs to be widely distributed. There is a considerable role for governments, particularly the federal government, to provide direct funding to community groups, outside the vocational area, for computer literacy for daily living skills. With all business and community sectors relying more heavily than ever on ICT for disseminating and seeking information, the daily living skills, business transactions and even socialisation of those who are not computer literate will be severely affected. Older people will therefore be discriminated against. Funding for community groups such as ASCCA is a serious challenge. Our objectives clearly define our aims are to help seniors to become computer literate and safe and competent users of the internet. ASCCA is the national peak body for seniors and technology. Our expertise is often sought and we welcome opportunities to participate on committees, councils and boards when we seek to advocate for the needs of seniors. We have managed for 14 years without any core funding, but are finding it harder and harder to access even project funding.

Identifying that older Australians need to be educated about cybersafety and that their behaviour as internet users opens a wide range of opportunities would help overcome the challenges that a lack of awareness so often brings. Broadband for Seniors kiosks and ASCCA's national network of seniors computer clubs are working with their members to help them embrace the use of the internet, but there is much more to do. The demography of our nation demands that the needs of older Australians for education to enable them to be safe and confident users of the internet be addressed. I commend the Joint Select Committee on Cyber-Safety on holding this inquiry and look forward to outcomes which will empower older Australians by making them aware not only of the advantages of cyber-safety but also of what they can do to become safe and confident users of the internet.

CHAIR: Thank you. I wrote a note to myself while you were giving your introductory remarks. I was going to ask if you had links with the Broadband for Seniors kiosks, and then you mentioned them. Would you very quickly expand on what those links are.

Mrs Bosler: The Broadband for Seniors kiosks is really an excellent program—2,000 kiosks rolled out across Australia. It is funded by the federal government. NEC is the lead agency and ASCCA, my organisation, is part of the consortium. We have actually written the face-to-face training material that seniors are using within those kiosks. They are a wonderful stepping stone for seniors to become used to the basic concept of using the internet. It is that fear factor of not quite knowing where to start and whether they can manage that often is the stumbling block for older people. Those kiosks are doing a good job.

CHAIR: In your submission you talk about the advantage of having older trainers as IT trainers for seniors, and we heard this morning from the Human Rights Commission about the UK and Ireland, where they have younger people going into help seniors to become more confident online. Do you support programs that might involve younger people as well? Do you see any special advantage in the skills that retirees or older Australians might have in helping other older Australians become more confident?

Mrs Bosler: Older Australians usually find being helped by their peers to understand how to use a computer is a really good way to go, but they also love the interaction with the younger people. Younger people, of course, must understand how to work with older people. Too often you may ask a grandchild, 'How do you fix this, Jamie?' only to be told, 'It's easy, Nanna; look, it's done.' You think, 'What did you do? How do I do that?' It is better if a younger person understands that they have to be a little more gentle and take time to work with older people, because older people do like—they need—to work at their own pace.

But I have seen some lovely programs with the interaction. I have seen also some TAFE programs with a component where they have to work with a special target group, and sometimes they might select to work with older people. There have been some lovely outcomes. I have also seen many high schools endeavour to find work placements during work experience at clubs. That has not worked as well because they are actually looking for a block of help. They may want a student to come in five days a week for five hours a day, and that does not fit in with the way the computer clubs usually work. So that does not work as well—but, oh, yes, older people love to sometimes work with younger people.

CHAIR: You mention the clubs. I think there are 156 clubs—is that correct?

Mrs Bosler: Across Australia, yes.

CHAIR: I am interested in how those clubs have been set up. Are they set up in local areas by interested people or is there some other process they go through?

Mrs Bosler: There are a number of ways that a club can be set up. It could be that there is an existing computer club somewhere and they hear about ASCCA and think that it would be to their advantage to become part of a larger organisation where their voice is more likely to be heard. But a good percentage of the clubs we actually set up ourselves. We may get a phone call from someone in a country area that says, 'There are a group of us up here who would love to be able to learn how to use a computer. We understand that you can help us set up a club; what do we have to do?' We have actually written a development kit, which is available free on our website, that anybody can use to help set up a computer club. In fact, they could actually use it to set up any sort of a community club. It would take them through the process of how they could have a public meeting and talk to other people in their area to find out if there is a need for such a club; how to form a steering committee; what that steering committee would need to do; what would happen once they have met their brief; and how they extend beyond that point. We would help them in any way we possibly could. If it was within close enough distance, we would go and talk to that public meeting for them. We are on the other side of an email or a phone call and they can say: 'We've got that group. We've had that first meeting. We are keen to start that club, but we don't know what to do next.' I am very likely to say: 'Why don't you check with community services at your local council and find out if they can suggest places where you may be able to hire a room in a community centre, a church hall or something like that.' Every aspect they need for setting up that club is available.

CHAIR: It is really pleasing to hear that it is not just city-centric.

Mrs Bosler: Absolutely not.

CHAIR: One of the issues around this inquiry is access for rural and regional seniors—and immigrants, maybe people whose first language is not English. That is all really important for us to know about.

Mr PERRETT: I was going to ask you a question in your private capacity, if that is all right, Mrs Bosler.

Mrs Bosler: That is fine.

Mr PERRETT: I imagine some of your friends might be more mature Australians. They know your passion—you are organised, you are committed, you are a national leader in this area. How are your friends on the internet? Are they friendly? Are they wary? Are they reassured by you? Are they savvy? You would have a range of friends in a range of settings, I would imagine.

Mrs Bosler: Absolutely, and each of those things applies. But, for the most part, if they can build up a personal rapport with someone, even if it is by personal emails or suchlike, they are more confident to ask questions. If they can have face to face, that is even better. But I find people use the internet in all sorts of ways. One of those is to gain information so they can work out if this internet is going to be something that is going to help them and suit them, so they can get to the stage where they are happy to say: 'I've got a problem with this.

I'm worried about such and such. What do you think I should do about that?' We have had workshops where people have said to us: 'I'd like to use the internet, but I don't quite know what to do first. What is an ISP? What ISP can I trust? What is going to happen? How am I going to manage paying for it? I have a limited fixed income. I am scared that, if I start using the internet, I might run up bills that I can't cope with.' So they need to be reassured and they need to be given good, sound information.

Mr PERRETT: Getting them through their L plates and their P plates is an important part of the process obviously. Once they are off and driving, they get all the benefits of the internet.

Mrs Bosler: They do. Once a person can really start using the internet and feel confident in using it, the world opens up for them. It is really amazing.

Mr PERRETT: There are economic benefits. You do not have to catch a bus to go and pay the bill—all of those things that come with the ease of internet use.

Mrs Bosler: Yes, particularly for people in rural areas and such, where so many agencies have closed—they need to be able to access the internet to do those payments. Public access points are very useful, but they really would like to be able to use the computer at home.

CHAIR: You mentioned the issue of access in areas where services have closed. Have you got any comments for the committee in regard to the e-health proposals? I know you were in the room listening to the previous submitters.

Mrs Bosler: I think e-health is going to be absolutely marvellous. The NBN rolling out is going to make such a difference. Look at the planning that is being done in Ballarat at the moment, where they are looking at using e-health for oncology, for psychiatry, for dental, for wound management. That is a marvellous program, and that is just the tip of the iceberg of what e-health is going to mean for older people and all people right across Australia. So I am very, very supportive of that. I think the concept of the card, which we were talking about last time, is wonderful, but there are a lot of answers still to be found. I do not know that much attention has yet been paid to the roles of carers. I mean the real carers: the home carers. So many older people are perhaps not capable of being able to be the authority that says, 'Yes, you can have my information.' They may have dementia; they may have had strokes and are not able to speak very well. For all of those reasons we need to make sure that carers are well covered and well informed about that proposal.

Ms MARINO: Mrs Bosler, thank you for being here. I just want to touch on what is probably a very sensitive matter. It is something that is coming to me from seniors and their families in my electorate. It is the issue of passwords. Most internet users are encouraged to change their passwords every three months. I know that this can be a challenge not only for seniors but for many—what password goes with what? The thing that comes through currently is that there are families, perhaps when someone passes—whether it is a young person, a mature-age person or a senior person—who need to get access to a person's information to manage an estate or something else, and accessing a password is critical to accessing the information. What would you suggest as being a way to manage that particular issue?

Mrs Bosler: We are talking about someone who is no longer able to manage their affairs or they pass away?

Ms MARINO: They pass away. Currently I have people saying, 'My mum'—or my dad, my grandma, my brother or my sister; whoever it is—'has passed away' or they have lost their life in some circumstance. There is the issue of the passwords, and being able to access what they need is quite difficult. Could you offer some suggestions on managing that issue?

Mrs Bosler: I understand exactly what you are saying. It is an enormous problem. Very often, if an older person dies or they become totally incapable of dealing with their own things, their papers or their information is very scattered. It is an enormous problem. Personally, I have recorded my bank accounts and my passwords and such things, but not on my computer. I have lodged them in a safe deposit box at the bank and there is also a copy with my solicitor.

Ms MARINO: If you were changing your passwords, you would need to update that information.

Mrs Bosler: Yes, with great difficulty.

Ms MARINO: Yes. That is a very practical suggestion on how to manage it, but would you see the need to communicate that more broadly to others? When we talk about cyber safety, we say 'Don't tell your password. The only person who should know your password is you.' That is so critical to security, but, in this instance, they need to have a trusted method that is also communicated—whether it is a will or some other way to say: 'This is where you access this information.'

Mrs Bosler: Even though I have done something for myself, it is not a question I had addressed in my mind as something we had to look at. It is a very valid and important issue. We need to encourage seniors to change their passwords frequently. It may be that we need to consider them organising in their mind a word that is going to be very good for them to be able to remember, but not one that is a pet's name or a birth date, and they need to change it regularly by changing the letters at the beginning of it or at the end of it, or something like that.

Ms MARINO: Or even inserting a number at some point. That is the frequent thing that is said when I talk to people about this. There is a more pressing issue. More people access e-health and a range of websites. The number of seniors using the internet will grow, and this issue is going to become even more relevant with the increase in the number of personal records, such as bank accounts, online. They will be able to do almost everything online, so there may not be the papers sitting somewhere that, historically, relations rely on to access the critical information. If you talk with your broader group and consider you have something else practical that you can provide to this committee, I would really appreciate that.

Mrs Bosler: I thank you for the suggestion because I think it is a vital is issue that I, frankly, had not thought of.

Ms MARINO: Thank you for that.

Mr HAWKE: Is Computer Pals for Seniors one of the groups that is involved in your national organisation?

Mrs Bosler: Yes, it is one of the names.

Mr HAWKE: There are various names, aren't there?

Mrs Bosler: They use the name that suits their particular group of members.

Mr HAWKE: Are you aware of any outreach groups for seniors? Do they go and visit nursing homes, other institutions or any of that sort of proactive engagement? Because many of them tend to be independent seniors who have gathered together, which is a good thing as well. Are you aware of any outreach programs?

Mrs Bosler: In 1998 we recognised that very often people in a retirement complex were disadvantaged because of either lack of transport or lack of mobility. We have set up quite a few seniors' computer clubs within retirement complexes. Broadband for Seniors are setting up kiosks in some retirement villages.

Many of the earlier clubs that we opened were created from outreach of an initial club. One of the earliest clubs on the northern beaches was at Forestville, the Forest Computer Pals for Seniors. They grew a little bit too big and they could see there was a group of people based at Narrabeen or further up the peninsula, so they suggested to those members that they become the nucleus for forming a new club, and that happened. When that new club was set up they could see they had quite a few people from Manly, so they went and started a Manly club. It has spread out like that.

We also know that sometimes there is a more professional group that might set up to take lessons to a person's home on a one-to-one basis, which is more expensive. There are going to be seniors always that are interested in that as well. We have been providing some training for the people who go into homes by having them at one of the clubs where they do some one-on-one training to get used to that style. Yes, there is outreach and there needs to be.

Mr HAWKE: That is good. Do you have any general comments or reflections on how we are going with internet access in retirement villages, nursing homes and things like that? Is it being taken seriously? Is it being provided in a better fashion now?

Mrs Bosler: It depends entirely upon the management of that particular aged care facility. You would find the larger groups such as the Anglican retirement villages have been very supportive in helping to get internet access and computer training into their facilities. There is always going to be room for more. We must make sure that we do not eliminate any section of the aged community—and that means those in aged care facilities and even those in nursing homes.

I have had computer groups in nursing homes that have been very valuable. I remember there was one particular gentleman who had to come into care. He had lived on a boat and he was no longer well enough to stay on the boat. He hated the idea of coming on land and going into an aged care facility. When he arrived, the recreation officer asked if he would like to learn how to use a computer. He said no. She knew of his love of boats and she also knew he was not settling in very well. So she was careful to often lead him past the computers and have on the monitors a lovely sailing boat or something and eventually he asked, 'Why have you got a boat on that computer?' and she said, 'Oh, there's stacks of information about boats on the computer.' He became a different man. It was just a little bit of clever motivation. If a senior is motivated to use technology and can you learn at their own pace, they are likely to succeed.

Ms MARINO: It is also a wonderful way of keeping in touch with their family and friends, no matter where they are physically located. So many seniors I meet have a wonderful time in that sense.

Mrs Bosler: Absolutely.

CHAIR: On that note I am reminded that, in your submission, you mention a different social networking page for seniors.

Mrs Bosler: Yes, it is finerday.com.

CHAIR: I had not heard of that before. Are you able to quickly tell us about that?

Mrs Bosler: It was set up by somebody who had been involved in aged care facilities. She could see the need for a social networking site that was quite safe for residents and their grandchildren to keep in touch. It is free. When I was overseas in Ireland looking at various aged care thingos, I used that as my internet connection because it was web based. That meant no-one was seeing my emails other than those that I invited to see them.

CHAIR: Is it successful in Australia?

Mrs Bosler: It has not been used terribly widely; it is far more successful in the UK. But it is well worth following through with because it is safe and it is easy to use. They can send and receive emails. They can put up photos and share them with their grandchildren, and their grandchildren can put up photos to share with their grandparents. That is even more important. It is a nice interaction.

CHAIR: Your submission had quite a lot of information about the BRAID report. Is that a UK based report?

Mrs Bosler: It is European based.

CHAIR: Is there any information from that report you would like to share with us? I think you mentioned that, although some of it is outside the scope of the terms of reference for this inquiry, it does give an overall picture that we need to know in regard to cybersafety for senior Australians. If you would like to take a few minutes to tell us what you can about that report, that would be great.

Mrs Bosler: The whole idea was to develop a roadway where ICT could be introduced to seniors in Europe. They have been working very hard; it is on a fairly academic level at this stage, but it is very interesting. One report read that they felt seniors were not going to be sophisticated users of technology; they were going to be more mundane and ordinary. Well, I tell you what: mundane and ordinary might be enough! But we have seniors right across the whole range. We have those who are very sophisticated. We have members in our clubs who were involved in the creation of the early computers in the 1940s right through to others who do not know how to turn a computer on properly—and turning it off is a little harder! This research is looking very seriously at how seniors can be helped to get benefits from using technology. They recognise that we have got to do it that way because everywhere, the world over, governments and agencies are using the internet to disseminate information, and if people cannot access it they have little hope. I am sorry that I cannot—

CHAIR: Is that report publicly available?

Mrs Bosler: It is publicly available. I have a copy of it with me. I will share that with you afterwards. I would be very happy to do that.

CHAIR: That would be great.

Mrs Bosler: It is quite exciting. I will have the opportunity of presenting a paper in May at their final conference in Prague, and I will be talking very, very strongly about how Australian governments and Australian community groups are working together to ensure that Australian seniors are not left behind as we need to start using the internet more and more.

CHAIR: That is wonderful. We will officially move a motion to accept that document just so that we are covered for our purposes. Do you want that copy back?

Mrs Bosler: No, you can have that. It is got my scribbles on it but you can certainly have it. It is available publicly.

CHAIR: I have a couple of other questions that I want to ask. In your submission you talk about the attitudes and views of your members about cybersafety and internet use. Has your organisation done any formal surveys or studies in regard to that information that we might be able to access that might be of use to us?

Mrs Bolser: I have done some research and surveyed. It is about six years old now but it was very interesting and there are not very many changes from what was said then to what is said now. The one big change is that in 2006 39 per cent of those who answered the survey—and there were 508 of them so it was a cross-section—said they only could access dial-up and they were desperately frustrated. We know that there have been significant improvements since then and dial-up is being gradually faded out, but that is what I am looking to the NBN for,

so that we can actually access everybody. They were concerned about safety issues and about their grandchildren and their use of social networking sites. They were worried that they were putting things up that really were not discreet. If you look carefully at what a child is putting on the internet you may find somewhere in there there is the school's name—

Ms MARINO: There are photos.

Mrs Bolser: Yes, and all of those things. And if you take a little bit here and a little bit there you have actually built up a whole profile. The idea of saying, 'We are going to Melbourne for three weeks next month and we're looking forward to that.' Wow. We know the child's address. The grandparents are worried about that. They are worried about their grandchildren accessing pornographic sites. I do not quite know if we are ever going to be able to prevent that because a lot of those youngsters are very clever.

CHAIR: But once again that is an education process to young people and there is certainly a lot is happening through ACMA and the Youth Advisory Group and things like that.

Mrs Bolser: There are wonderful things being done there and it is improving very much indeed. I can let you have a copy of that research if you would like.

CHAIR: That would be wonderful.

Mrs Bolser: That project also called for us to address the issues we found, so you will find the way we address them as well in there.

CHAIR: One of the things this committee is doing in regard to this inquiry is having an online survey itself. You might like to encourage your members to access that once it comes online and fill it out for us, and that way we can get more information from more people.

The other thing I wanted to quickly ask is this. My personal view is that cybersafety is not just the domain of the user but it is the ISP and even government in some respects. Do you have any views with regard to that?

Mrs Bolser: I think it is a situation we all have to look at. I would like to see that information about cybersafety is provided at point of sale for every computer. That will not cover second-hand ones but there needs to be that information. I would like to see that if the operating system on that computer has inbuilt security, that it be the default that it is all activated. I think are so many things we could do. Even when our seniors go overseas, and a lot of seniors do travel overseas, DFAT really needs to be providing information about being cyber safe when they are overseas as well. I do not think that is an issue that has been addressed.

Mr HAWKE: And members of parliament.

CHAIR: No, and I think that is the first time the committee has said that put to us. It is a very important issue. As politicians who may travel overseas that is quite important to us as well, as Mr Hawke just said.

Mrs Bolser: I would like to see information about cybersecurity written in a way that is going to inform and, that will not terrify them. We want them to be confident on the internet.

CHAIR: Aware, alert but safe.

Mrs Bolser: That is right. I have had seniors say to me, 'I'm not going on the internet. My husband says that there are always people stealing our identity and so he does not want to touch the internet.' There are all sorts of worries like that, but education can help with those. That is why it is so important that we get through to all people of all ages, but my particular interest is seniors. We must help them to understand the value of cybersafety. I was quite alarmed when I realised that quite a few people were well aware that they should have anti-virus programs on their computers but did know how to access them. Then the idea that they had to be regularly updated, they were not aware of that either. Even the need to keep their software updated, they think, 'Well, okay, that program is working well. I do not need anything extra.' But very often the update is not to give them more use of that program, it is because a threat has emerged and it has been updated so it can put in a patch or solve that problem. That was something that we also need to make sure people know.

Ms MARINO: Mrs Bosler, the other thing that some of the seniors have said to me is that they are not even really sure when that patch and that message turns up, whether it is genuine.

Mrs Bosler: Whether it is legit.

Ms MARINO: And whether they should click on it or whether it effectively is another form of accessing information out of people's computers. I think that issue is another thing for all computer users and internet users, but equally that is something that the seniors have said to me they are very worried about. Is it a genuine Microsoft or other message or whatever their virus protection is? Can they be confident that it is genuine? That is something that they are wary of.

Mrs Bosler: Yes, you are right. These phishing emails that come in, they can quite easily sort of understand that they do not touch them unless it appears to be from their own bank. Then they are inclined to actually have a look.

CHAIR: That is right. Some of those phishing scams are very elaborate. We heard evidence earlier in the week about the background setups for internet pages and things that some of the organisations will go to to make sure that it looks legit. There have been investment advisers even being caught out. Some of them spend a lot of time and effort on the background stuff to make them look legit. Once again, if you go online to research something, again you could easily be caught too. As we say, we do not want to put people off. The aim of this committee is to actually encourage people, but to also find out what those areas are of concern so that we can deal with them.

Mrs Bosler: Yes. And some people think they are being very proactive if they get something that is obvious spam, but they click on the disconnect, unsubscribe.

CHAIR: Yes. Mrs Bosler, I would like to thank you for your evidence today and for your submission. It has been wonderful to hear from you. We will adjourn for lunch until 12:45. Thank you.

Proceedings suspended from 12:07 to 12:45

SHAW, Mr James, Director of Government Relations, Telstra Corporation Ltd

KANE, Mr Darren, Director, Corporate Security and Investigation and Internet Trust and Safety, Telstra Corporation Ltd

CHAIR: I now welcome representative from Telstra Corporation. Thank you for your submission, which has been received as No. 22 in the committee's inquiry. Before proceeding I should remind you that this is a public hearing and is being recorded by Hansard and audio broadcast. I need to notify you that, although the committee does not oblige you to give evidence under oath, this hearing is a legal proceeding of that parliament and warrants the same respect as proceeding of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Do either or both of you gentlemen wish to make an opening statement before we proceed with questions?

Mr Shaw: We do have a brief opening, Chair. Telstra welcomes the opportunity to appear before the committee's inquiry into cybersafety for senior Australians and expand on those key themes and recommendations that we set out in our submission to you. As you probably know, Telstra is Australia's largest internet service provider and the issues raised in the terms of reference for this inquiry are extremely important to us and to our customers, and we are keen to assist the committee to provide input to efforts to improve cybersafety awareness amongst senior users of the internet. In recent years engaging online has become an important tool for everyday living, with many people using the internet for a wide range of purposes, including communicating with friends and family, sourcing information and transacting online.

More specifically, the internet facilitates enhanced communications amongst older Australians, especially those who face barriers such as mobility or other impediments that would otherwise make communication and other activity difficult. However, while the internet offers a broad range of positive benefits to be enjoyed and experienced by older Australians, there remain a number of risks and threats associated with engaging online. While senior Australians are progressively adopting new technologies, there are concerns about cybersafety amongst this cohort that are having a direct impact on attitudes and confidence to use technology and is an inhibitor to greater digital inclusion.

Our company has a longstanding commitment to making the online experience safer for our customers and we are working hard to address some of these issues. An example of this is our Telstra Connected Seniors program, which helps older Australians learn more about technology and how to engage more safely and securely online. The program offers individual self-teach guides and interactive workshops and also offers eligible community groups with the opportunity of funding to run successful training courses around technology.

Telstra also advocates that addressing cybersafety amongst senior Australians should be a shared responsibility involving a variety of different groups, including government, not-for-profit organisations, industry and, importantly, end users. It is therefore important that all groups work together to achieve a safer digital future for senior Australians. Furthermore, we believe further research on the nature and prevalence of cybersafety concerns amongst senior Australians would assist in an evidence based approach to the issue.

Finally, we encourage more consideration on the merits of promoting internet safety through public awareness campaigns intended to promote safer online experiences for all Australians including seniors. That is our opening statement and we are more than happy to take questions.

CHAIR: Mr Kane, do you have anything to add?

Mr Kane: I am happy with the joint statement.

CHAIR: Okay. I will kick off. You mentioned responsibilities. What does Telstra actually do to let the end users know their responsibilities? Obviously as an ISP I am presuming what you just said was that you think you have got some responsibility in regard to safety as well. I am happy for you to expand on that. But what do you actually do to help the consumer make sure that they are safe online?

Mr Kane: Telstra has had a longstanding commitment to cybersafety and one of these is to our senior user group, targeting our customers, the Telstra Connected Seniors program. In 2010 the program provided 53 Telstra Connected Senior grants totalling $448,302, which is 46 local grants of $5,000 up to the value of $182,765, and seven state grants of $50,000 to the value of $265,537. This resulted in a demonstrated change in seniors' behaviour with a measurable 7.2 per cent increase in competence and usage.

We have trained more than 62,000 older Australians: 28,000 through face-to-face training and 34,000 through self-teach DVDs loaned through libraries across Australia. That was in the 2010-11 program. We felt that it was a successful program and we have continued with the Telstra Connected Seniors program in 2011-12. We delivered face-to-face seniors' training to more than 22,000 seniors nationally, featuring cybersafety as a key topic. We

continue to drive more than 30 large-scale training events nationally, aligned to coincide with each state's seniors week. We have developed cybersafety educational material, self-teach videos and other collateral for the Telstra Connected Seniors website which is hosted on the telstra.com site. I have actually brought along a number of those props today. One is the Connected Seniors DVD workshop one, *Mobile phones made easy* and the other is *Life's more fun when you are connected.* I am quite happy to leave them with the committee.

CHAIR: Are you tabling those, Mr Kane?

Mr Kane: Yes.

CHAIR: Is it the wish of the committee that the submission be accepted as evidence? There being no objection, it is so ordered.

Mr Kane: We also have educational material in print form, which is the *How to use your mobile phone* seniors' guide—I will table that—and the *How to explore the World Wide Web* seniors' guide. Again, I will table three copies of each.

CHAIR: I will include those in the previous agreement, if that is okay.

Mr Kane: Finally, another initiative is the Telstra EasyTouch Discovery 3 phone. I spent some time at the Telstra T-shop again this morning to confirm what I understood to be our promotion of this. These target our senior customers. They have a larger number pad, are more easily explained and, when seniors attend our Telstra shops to purchase a phone for their purposes, this phone is one we keenly recommend because of ease of use. We have a touch screen that our assistants in our T-shop retailers will walk through so that seniors understand, if it is their first phone, what the merits of this product are and the services that are available. I draw your attention to the $20 service that we put them on—the plan. I think it is a $15 service with a $5 data plan. That is not much usage for the amount of money, but at the same time it is generally what the seniors are after, which is a phone for emergencies initially. As they become more confident, we will provide them with other services and products which suit their competence on the net. So we attempt to understand and then manage their online risks.

Finally, we continue to deliver internet and cybersafety face-to-face training sessions in all NBN enabled release sites nationally. I understand we have a training pod that supports that. The Telstra Connected Seniors program is tailored to help older Australians learn how to make the most of new technology. The program offers individual self-teach guides, fun interactive workshops and also offers eligible community groups and non-profit organisations the opportunity to apply for funding up to $50,000 to run training courses around technology. They are some of the initiatives we provide this demographic.

CHAIR: As one of the largest ISPs, what is your view on whether ISP safety is enough and whether ISP organisations have the capacity to monitor scamming activities more than they might do at the moment?

Mr Shaw: On the first part, we think that the industry generally—the ISPs—do have a role and a responsibility to inform end users and educate end users so that we get a safer environment. Darren has given some evidence there about our commitment to that. We would have to let our commercial opponents speak to what they do, but I do not think you would find anyone who, as a general proposition, would say that we should be doing less in this space. I think there is general agreement we could all be doing more. How that might be done and how it might be coordinated—the extent to which government, NGOs and the industry alike can come together and make that work—is probably fruitful ground for discussion. We certainly see a considerable value in our corporate social responsibility activities but also from a commercial perspective to interact with our customers and inform them about how to do more in this space and how to protect themselves more.

In terms of the second part of your question, I am sorry, I do not quite understand. Who are you asking whether they are capable of—

CHAIR: I was asking if you thought that ISPs have a capacity to monitor scamming activities more effectively than they do at the moment and to act against them .

Mr Shaw: Again, we can really only speak on our own behalf—I am not really in a position to talk about our competitors. We keep a very watchful eye on what is happening on our network in a number of ways. On the operations side, our security people are constantly looking at the traffic coming on the network and whether there are any vectors of attack, as they call them, where people are trying to do malicious things on the network. We remove a considerable amount of spam that comes onto the network before it even gets to the users, and when we do become aware of scams that have actually got through to users we do attempt to educate them and inform them about that. Quite often Darren will be quoted in a media release as the director of internet trust and safety warning consumers of the latest scam that has come to our attention. We are not backward in trying to alert people to what

is happening out there. We do an awful lot behind the scenes to try to ensure that those scams do not actually hit people's screens.

CHAIR: Do you think the current regulatory controls are adequate, or that they could be improved upon?

Mr Kane: I recognise that the globalisation and jurisdictional issues with the digital world as we know it today would make further regulatory controls very difficult in ensuring compliance. I think the best method of ensuring customers are aware of online risks is greater education and awareness. I also highlight the fact that Telstra is the principal partner with the Australian Competition and Consumer Commission with their Australasian Consumer Fraud Task Force National Consumer Fraud Week, which started last Monday and finishes today. I was at the launch of that here in Sydney on Monday. We continue, as James put it, to work with our customers across all demographics—as I like to say, from cradle to grave. We take a very committed approach to cybersafety. I have been in this role as the director of internet trust and safety for four years now and working in this area for approximately eight years. There is the provision of tools and tips and educational information to all of our customers through our Connected Seniors program—the one I mentioned—and a dedicated Trading Post Trust and Safety Team, where we have e-commerce commitments. We have help pages, forums and alerts; we offer information to educate our customers; we have the BigPond security product—a comprehensive computer security solution made available especially for BigPond members. Not only do we support the Australasian Consumer Fraud Task Force week, but we are also heavily involved in Safer Internet Day, Privacy Week and National Cyber Security Awareness Week. They are just some of the measures that we are committed to employing and supporting. I think there is room for further coordination to lessen duplication between all participants to try to ensure customers are aware of online risks, and there is an opportunity for government to coordinate that approach. At the same time, I do think sufficient is being done to ensure that all users of the digital world understand the risks. It is probably how we are reaching our target market, but it needs to be more coordinated.

CHAIR: Do you think that information on cybersafety should be mandatory at the point of sale for internet connected products?

Mr Kane: I firmly believe that Telstra wants to ensure that all our customers have the very best online experience. We sell access—that is how we make a profit. We sell services and products that connect people and individuals. If we were to sell a service or product or network access that did not deliver a good online experience, people would not connect with us. Therefore, it is absolutely in our interests to ensure that all of our customers understand the potential online risks. It is also important to understand the positives around the digital world. I think there needs to be a balanced approach. I do think that there is sufficient information available at point of sale for all users to better understand the online risks. I do think that ISPs and telecommunications providers do provide sufficient information based on my evidence here at Telstra. I also think more can be done to ensure our customers understand why they need to educate themselves to these online risks. I use the old adage about taking a horse to water. Making it mandatory for us to provide the information would not solve the problem. I think we do that anyway, because we want to ensure they have a greater online experience and keep coming back for more.

CHAIR: Did you want to add anything to that, Mr Shaw?

Mr Shaw: I concur with what Mr Kane has been saying. When you buy a new motor vehicle it comes with certain literature about road safety and other things like that, but not every consumer reads that; they just cast it to one side. Simply regulating to provide something when we think that it is already being provided is, we believe, counterproductive. What we really want is to increase people's appetite for consuming that information, understanding the importance of that information. So we think that focus on getting people to take that material and providing material that is suitable to the various demographics that we sell, tailoring it to those groups and them understanding that it is in their interest to read it and understand what is being said, is a more important focus for activity, rather than regulating to provide it.

CHAIR: Through the week I was doing a bit of research. I actually went online and had a look at—for want of a better way to describe it—your clock, and the nine o'clock to 12 o'clock part for seniors. I thought that was really useful. It had some good basic hints and tips and things in there. Do you want to make any comment about that?

Mr Kane: Thanks for the compliment, Senator—

Mr Shaw: Mr Kane was the leader in developing that clock, so he is quite proud of it. You have struck the right note.

CHAIR: I was not aware of that, I might say. But I did find it useful.

Mr Kane: I came up with the idea because of Mr Shaw's comments about tailoring messaging. What I found when this issue started to develop, that is cyber safety and education awareness, was that they went out with a one-size-fits-all. It was targeting children. So if you look at the clock face, the 12-to-three is for up to 14 years. There are animated videos, and multi colours. It was quite obvious that that was not resonating with the three other areas, particularly the forever youngs, the over-55 market. I had to come up with an understanding of how we could tailor messaging to all demographics, so all customers got the opportunity to understand their online risk. What we have done is broken it into the four quadrants. We have tried to keep it simple so that all new users of technology can understand our positioning. Also important is that we needed to keep it current as things changed and developed. I can make mention of the fact that before 2006 Facebook was not known. Now, here in 2012, it appears to be the only medium for communication in some aspects, particularly the demographic under 21. It is really important to have a method to tailor messaging, which is something that this committee could take away. If you are going to tailor messaging, get feedback from the actual target market as to how the messaging resonates. We have had feedback from our Connected Seniors program that has indicated, exactly as you have, that they have found value in the nine-to-12 segment.

CHAIR: You advocate for a taskforce approach to engage stakeholders, following on from what you were just saying. How do you see that being set up or organised? What sort of campaigning? What do you think the taskforce would do?

Mr Kane: It is my belief that at the moment cyber safety is a little fragmented from a coordination approach. I think our company has got it right. I think we have a centralised point for the emission of cybersafety information and we recognise that we are servicing a different market and different segments. We target our messaging and tailoring at those segments. I do not see that same approach in some government departments or in other agencies. If we are to work effectively in a taskforce approach, I think there has to be an acceptance of one firm approach. Another key initiative would be an agreement not to duplicate but rather to link. I have made the point several times in other committee inquiries that resources for this program—that is, cybersafety—in agencies, other commercial entities and certainly at Telstra are not abundant. We are committed to it but we would like to do it innovatively and creatively and to use what is available without duplication, because it is all the same message. A taskforce approach would definitely need to ensure less duplication and replication and more creativity and innovation. Therefore we would need participants in the taskforce that had that approach. I sometimes see a taskforce approach lose its effectiveness because not everyone is heading in the same direction.

I think there are relevant agencies and departments within government. I have worked hand-in-glove with applications such as Google, Facebook and others; I have worked with senior NGOs such as Alannah and Madeline; and I have prior experience of working in taskforces or working groups that have been incredibly effective. That effectiveness comes from all agreeing at the very start on what the outcomes are to be and how to achieve them.

CHAIR: The taskforce you are talking about there is the one that the government set up in regard to young people?

Mr Kane: That is an effective taskforce. That is the consultative working group on cybersafety, which has been together now since 2008. Yes, there have been some really successful initiatives and I am quite proud of our participation in that. But I have often said that that taskforce is targeting cybersafety for children, whereas I do not see anything similar for the different demographics, and I have often argued the point that perhaps cybersafety should be bundled together so that it is one committed approach.

Ms MARINO: Thank you for being here today. It is not the first time I have met you gentlemen in the course of these types of inquiries. With your Connected Seniors program, have you had a measurable increase in seniors as customers as a result of that process? Could you also tell me what the most frequently articulated issues that you had from the seniors group during those sessions was and, if you are willing or able, tell me what proportion of your senior clients access your cybersafety resources that you talked about so that we know it is actually seniors who are accessing the information that you are providing?

Mr Shaw: In respect of the first question about sales, we do not have direct statistics to show that the Connected Seniors workshops themselves lead to increased sales. We can only point to the fact that the business's numbers have been looking reasonably good over the last couple of years. We must be doing a number of things right and we like to think that Connected Seniors is part of it, but there is no survey at point of sale of anyone who appears to be, for instance, over 55 as to whether there has been attendance at a Connected Seniors workshop. I am afraid we cannot provide you with any hard data on that.

As to the issues around what comes out of the various sessions, if we could take that one on notice we will go back to the people that run the program and see if we have any information that we can bring back to the committee on that particular matter.

Ms MARINO: That would be great. It might inform this committee of additional issues that we may not have been aware of.

Mr Shaw: It is a very fair question and we will endeavour to get an answer to that. In terms of the proportion of the seniors who are accessing the material, there is no real measurable way of collecting that either. Whether a senior goes in to get the collateral from the shop or they pull it down from online, we do not identify them as that particular segment of our client base just because they are accessing information. Equally, they could be accessing information for other people or their grandkids could come in and get it for them as well, so it is not really a straightforward process of identifying how the customers line up against the various segments and the material they are accessing.

Ms MARINO: Okay. In the period that you have had this capacity online, what has been the growth in how it is being accessed? Irrespective of what the demographic is, what has been the growth because the service is available?

Mr Shaw: We will get you some information on that.

Mr Kane: There are actually two unique sets of visitor stats that we can provide. The first is the Connected Seniors website, where a lot of the seniors that do attend the Peter Blasina sessions and other training we provide get the information from. There are also the seniors that we direct to our cybersafety site in that 9-to-12 quadrant that Madam Chair spoke of. We will get the stats for both, but what I can say, leading up to an award that that site won at the 2011 Australian and New Zealand Internet Awards for security and safety in September-October of last year, is that we had an increase of upwards of 600 or 700 per cent in unique visitors to the site, and that is to all four quadrants, from cradle to the grave, 12 to 12. But we will get you the most up-to-date stats that we possibly can. We are quite proud of the fact that the industry has acknowledged the success of the site.

Ms MARINO: Which is a really important thing and a great initiative. It probably just underlines the importance of having that service available, how important safety is and the need for it. It underlines and reinforces it.

Mr Shaw: Absolutely.

Mr Kane: We would agree.

Mr HAWKE: I have a question on research. You have noted the need for research on the prevalence and nature of cybersafety threats. I am interested: is there any research being funded or collectively undertaken by the task group, or by any entity you are aware of?

Mr Kane: I am not aware of what research or commitment to cybersafety is being undertaken by any other body or task force other than the ones we do with Telstra. I understand that connected seniors would have some sort of an effectiveness survey to see whether we were providing a valuable product. It has been one of my points of order on the consultative working group that are particularly targeting cybersafety for children. A very fast growing segment of the marketplace in the digital world is, of course, the over-55s market. I know from anecdotal evidence from my mother and others that there is a real thirst and appetite for more information on how to stay safe online. That was the advocacy of a task force approach on that point. Was the second part of the question on what I would feel to be valuable information to that segment?

Mr HAWKE: We have had the point made by other organisations about the lack of available research, and some organisations have made points about the lag time between getting the research and whether it is effective or not.

Mr Kane: I would support that last comment absolutely. Technology evolves almost daily. We have found that a longwinded survey, and any analysis of and the dissemination of the research, may take anywhere between 18 months and two years, which is a long time.

Ms MARINO: God.

Mr Kane: Exactly right. So we have to look at emerging trends and how they may impact on that segment of the market, and then take our best guesstimate and move on that.

Mr HAWKE: So you are doing that commercially, obviously, but is that being done for the purposes of cybersafety?

Mr Shaw: The ACMA has a research program which has touched on this area of seniors. The focus of society in this area has predominantly been, as Mr Kane said, on children up to this point, but there is now a greater

recognition that we need to make this a whole-of-society issue. To that extent, we have a number of established bodies out there which have put a lot of work into the issue of cybersafety for children, as part of this whole awareness. A task force approach would be to get them to look at spending their research efforts across the whole of society rather than just focusing on the kids. I think the case has been made that we need to do more for children, and to get things right there, but this has been to the peril of other parts of society and we should recalibrate our efforts in that respect.

Mr HAWKE: I understand. Moving back a little bit to what the chair was getting at before, in terms of your corporate social responsibility in this area—and I understand you have a business imperative and a commercial imperative—are you really saying to the committee that you find the legal framework is adequate for cybersafety in Australia for dealing with threats, whether it be through litigation or through following up challenges in cybersafety? Or do you think there needs to be improvement in the laws generally?

Mr Kane: I have a responsibility, wearing my other hat of Director of Corporate Security and Investigation for the company, to manage our law enforcement liaison and our provision of information for telephone intercept and for lawfully requested information. I am very much aware of how much is done under legislation regulation in our licence. I am also aware of some of the regulations that we work under in relation to corporate social responsibility. I feel that it is in the interests of our company to ensure that we comply with all of those requirements and to ensure that our customer has the very best online experience. That really does require us to make sure that they are educated to potential online risks. We are a company that makes good profits—and by that I mean people have a good experience—not bad profits.

Mr HAWKE: I understand and accept the contention that you are behaving responsibly towards your customers. What I am getting at is: when your customers come to you with cases, whether it be fraud or all the cybersafety risks and things that happen, is the legal framework in our society today adequate and sufficient to deal with those serious allegations of fraud and other matters? Do you find it responsive? Does it need improvement or adaptation?

Mr Shaw: No-one in our business has come to me during our work preparing for this or just in our general work. We have an organisation within the business, our internet trust and safety working group, which Mr Kane chairs and which I am a member of. It brings together people from the products area, the networks area, the legal area and the public affairs area. I can say with hand on heart that one issue that does not come up at every meeting is whether we need more regulation or changes to the law in this space. It is not the first order issue that comes to mind when we talk about how we address the issue of cybersafety. I am more than happy to go and ask the question of our regulatory people and our legal people in particular as to whether they think there might be improvements that could be made to existing laws to address any deficiencies they might see in dealing with these sorts of processes, but I am not confident of getting a very large response.

Mr HAWKE: From lawyers?

Mr Shaw: Not all the regulatory team are lawyers, and certainly the public affairs people are not, but I am quite happy to ask the question—

Mr HAWKE: I would be interested if they did have any suggestions or thoughts as there has been some discussion about this in previous hearings.

CHAIR: Could you take that on notice, Mr Shaw, and get back to us.

Mr Shaw: Yes. Are there any particular current pieces of legislation that you might have—

Mr HAWKE: Even the operation of criminal law in relation to the internet as to whether your customers are able to access that in terms of the new technologies; I understand that jurisdictional issues all have different things with the internet but, in terms of the Australian law, whether there could be improvements.

CHAIR: Mr Shaw, you mentioned that it was not the first point of interest in regard to cybersafety at those meetings. Can you tell us what might be?

Mr Shaw: It is very much a sort of holistic approach. It is almost a taskforce within Telstra, which is why we think it would work well as the whole-of-government, whole-of-industry and whole-of-community approach. It brings together everyone within the business who has a particular interest in the online environment. There are people who are developing new products and want to put them out there, so we run the ruler over it in terms of whether we think it is up to scratch in terms of ensuring that consumers can use it easily, ensuring that it is not going to lend itself to fraud or to misuse, ensuring that there are other opportunities to work with other parts of the business and finding what leverage they might have done in their product development or public affairs activities in that space. We get feedback from the public affairs people on the sorts of issues that they are finding coming from the media and what the concern of the day is from there. The government relations team, which I head, is a

part of it, and we are looking at our interaction with the political stakeholders, what issues are top-of-mind, what we are doing in the business that we can bring to people's attention and what people are bringing to us as a concern that we should make sure the business is aware of so it is dealt with in our product development and our education and consumer information activities. It really covers all sorts of areas. The agenda can be 10 items long. It can cover 10 different parts of the business on any one day, but we have found it a very productive way to bring everything together. The material that Darren has used to populate that clock face has been drawn from that process.

Mr Kane: I would also add that it is a great way to ensure the messages from the company on cybersafety are consistent. What we do find sometimes is that out in the internet there are so many messages and it is ambiguous and does confuse, so it is a great way to ensure that all points of the company know that we have a cybersafety committee and we put out a consistent message which has credible information which we can rely on. The last thing we want to do is give information out to our customers that they are able to come back to us with and say, 'You told us to do this and this happened'. So it is a test.

Mr PERRETT: I want to talk a little bit about the Telstra Connected Seniors program. How many organisations have you given money to so far? What are the funding arrangements? Are you on budget in terms of giving that money out? Are people taking it up? How successful has it been, and what sort of feedback are you getting? I realise that is a big question.

Mr Kane: I did read through some of the answers to those questions at the start of our submission. The 2010-11 program provided 53 Connected Seniors grants totalling about $448,000, 46 local grants of $5,000 and up to the value of $82,000. Then we had seven state grants of up to $50,000 and under the value of $265,537. That was in 2010-11. We are continuing to offer grants up to $50,000 to run training courses around technology. I know you have heard from Mrs Nancy Bosler from Australian Seniors Computer Clubs. They are a big recipient of our grants. We continue to deliver face-to-face seniors training to more than 22,000 nationally in 2011-12, featuring cybersafety topics. We have an ongoing contract with Peter Blasina, the Gadget Guy, who runs a lot of the regional and metropolitan Connected Seniors programs. We develop educational material—self-teach videos and so forth. I have tabled some of those for the committee to review after this. We also have products and services specifically targeting our Connected Seniors. So we say that is a very, very successful program.

Mr PERRETT: Without opening up your balance books, is that successful economically in terms of some seed investment? That might be a question for Mr Shaw.

Mr Shaw: We have not done a direct correlation of people who have attended these courses and subsequently gone on to purchase equipment. The fact that Telstra is seen to be doing the right thing, and the brand and the reputation that goes with that, in itself is a significant payback let alone any direct economic value drawn from sales and the like. The whole notion of corporate social responsibility—or sustainability as it is called these days by many firms—is something that is very important to our business because we are a large Australian firm and we do sell so many different products and services to so many Australians. We want to be seen to be doing the right thing for society and our customers, but it is in our commercial interest to do the right thing in areas which have some payback for us. If every company was to do something similar then the whole of Australia would be a little better off. It might help the committee if we gave you a quick walkthrough of a Connected Seniors program.

CHAIR: It would. Where do people get access to something like this video?

Mr Kane: Through the Connected Seniors page on telstra.com and maybe make a request by email. I can check on that.

CHAIR: Is it available in libraries and places like that?

Mr Kane: Our submission says that we have a:

... Telstra Website and available for loan through more than 1,000 libraries nationally ...

CHAIR: You mentioned that Telstra does training to coincide with each state's Seniors Week. This is National Seniors Week in New South Wales. Can you tell us what you might be doing here in New South Wales this week?

Mr Shaw: Peter Blasina, the Gadget Guy, has been active around New South Wales for the past week. I think he is in Kiama with the folks on the NBN being deployed there.

CHAIR: Kiama seems to be a very popular place for people doing work for seniors.

Mr Shaw: Yes, it is one of the first release sites for the NBN. Their travelling truck went through there. We have what we call the 'shipper'. It is a shipping container that drops down and opens up into a demonstration centre where we have all of our fibre products and services that we going to deploy on the NBN. That has been

around Kiama as well and I think its last day might be there today. It is moving on up to Armidale shortly. With all those resources around the area and the media focus around the NBN, it has been an ideal way to actually put people like Peter Blasina in there and leverage off like that and say, 'By the way, while all this stuff is happening in a technology sense, here is a bit of the human touch in how you can access it and use it to your benefit.'

Ms MARINO: In your submission you touched on the need for a coordinated approach to research on cybersafety and cyberthreats. You have previously given evidence at other committees in relation to the nature of cyberthreats. I would be very interested in hearing more about what you think that research capacity would look like, who would be part of it, how it would be funded and how it would operate. Given your experience in the field, I would be very interested in your comments on that.

Mr Shaw: We would see a research program being run through this taskforce approach that we have talked about before. It is that notion, as Mr Kane said before, of everyone having a sense of where we are going and what we are trying to achieve so that we can coordinate a research program, which will change over time. I would not want to get into the specifics of what it might be, but the fact is it should be there and be capable of addressing the issues of the day as they arise and in a timely way so that you have an evidence based approach to your decisions around cybersafety. Also, that your education material and other things are based on current knowledge of the deficiencies in people's understandings of the technology and the like.

Ms MARINO: Given the fluid nature of this issue and the advances in technology and the fact that it is such a moving feast, who would you see as physically sitting on a research body of that nature? Who would sit around the table?

Mr Shaw: You would clearly want the education sector, because a lot of research is driven by the education institutions. That is where a lot of the knowledge about how to conduct a research program sits. Certainly industry should be there because we are the ones which are dealing with customers who have problems and issues. Quite often we are the canary in the coalmine for when things start to happen and run off the rails. I think there is a role there for government to sit there and assist in bringing this together, and it is not an uncommon model where you have industry, the tertiary sector and government sitting there. I think there is a role for the community, particularly groups that are out there at the moment delivering some of this training to connected seniors and others. We are looking at, at least, four different groups sitting around the table—industry, consumers, educators-researchers—and there is also a role for government.

Ms MARINO: Given that it is constantly evolving and usually ahead of the game, I suspect that this would be an ongoing capacity?

Mr Shaw: I think so. We have touched on road safety issues before. There is ongoing research into road safety that looks at a whole range of things—changing technology in vehicles, changing road conditions, changing consumer behaviour or driver behaviour and that sort of thing. Alcohol used to be the issue; now it is drugs. Things change and that needs to be reflected in the way you construct your research program. But it happens elsewhere in the economy and we think it is a reasonable model that could be adopted here.

Mr Kane: It may be as simple as a road black spot. If you have a piece of highway where you have had multiple accidents, you have a look at the root cause of the accidents and you put in remediation measures. That would be one way research could be effective in this space. Where you have four or five issues bubble up around something with the same root cause, you do some quick research which you can base on evidence. You go back to the taskforce approach and look for quick action steps and then a longer term strategy to ensure you have mitigated that risk.

CHAIR: Mr Shaw, do you want to add anything else?

Mr Shaw: Not on that particular issue, but just quickly—

CHAIR: You can always send the committee any other information you have that might be relevant.

Mr Shaw: Indeed. Just quickly, the Connected Seniors is an instructor-led training session, so a person—for instance, Peter Blasina, who we are using at the moment—is at the front of the room with members of the community present. The idea is to provide training in a number of different areas relevant to the online economy. We try to have a buddy situation in these Connected Seniors groups. More often than not, we try to get high school students from the local area in there because they are often quite savvy. Equally, schools these days have community outreach plans and the like, so getting students and seniors together is good and technology is a good way of utilising that resource. We take participants through how to use mobile phones and smartphones and basic things like texting, video-calling and how to do basic online transactions like shopping on your smartphone. We give them an introduction into the internet: what is the World Wide Web, what are the benefits, what are the issues associated with using the web? It is all about setting up an email account, browsing on the web, how to

chat, how to shop online, how to send photographs and the like on the web. There is discussion around social networking sites—Facebook, Twitter, YouTube and those sorts of sites. There are tips and advice on how to use social networking sites in a way that is as safe as possible for the user. Participants then get taken through a session on digital photography and digital video, how to use your phones and other things to generate that sort of content and how to use your computer to send it and get it online.

There is also a session on computing and computing equipment. We say to them: 'If you are of a mind to go buy a computer at the end of the session, this is what might be the most appropriate for you.' We give them a bit of information about that and provide further resources so they can investigate. Then we conclude by summing up: what are the positive uses of the internet, how do you find things on the internet, but what are the dangers associated with some of that? We discuss things like music, videos, online shopping and those sorts of things which we sort of take for granted but which new users may find entirely foreign. We wrap that up. It is a session lasting a couple of hours for the people involved. We think that covers the basic elements of getting online.

CHAIR: Mr Kane, just quickly because we have run out of time.

Mr Kane: I just want to add that one thing we are very keen on is managing the actual fear factor of transacting or socialising online. With the Connected Seniors program we recognise that one of the key drivers of issues around cybersafety is that people are very concerned and they lack confidence in this space. One aim is to try to reduce that fear factor.

CHAIR: Gentlemen, can I thank you both for your time today. Once again, we have received a lot of information in a fairly short time. If you have any other information you would like to give to the committee, the secretariat would be happy to organise that. We did give you a little task, Mr Shaw.

Mr Shaw: There are a couple of questions on notice there that we will get back to the committee on as quickly as possible.

Fraser, Professor Michael Henry, Director, Communications Law Centre, Sydney University of Technology

[13:32]

CHAIR: Welcome. Professor, the committee has received your submission as No. 31 in the committee's inquiry. Before proceeding I should remind you that this is a public hearing. It is being recorded by Hansard and audio broadcast. I need to notify you that, although the committee does not require you to give evidence under oath, this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament.

Professor, do you wish to make an opening statement before we proceed to questions?

Prof. Fraser: When I walk back to my office at UTS I expect to do so in safety, without encountering threats. It has been 100 years and more since we carried firearms or swords on our sides when we walked through the streets of Sydney. When I go into my office and I open my computer, even though it is part of a secured system of the university, as a matter of course I will encounter threats every day. It is the same, and more so, for individual Australians around the country who do not have the benefit of the secured and filtered systems that I do. They will encounter all manner of threats online. I do not think that this is an acceptable situation for a civil society when we are now using the internet as a mainstream form of communication and commerce, that it should be such a dangerous environment for citizens in general to deal with.

As you know, cybercrime is an international organised criminal activity. It is no longer conducted by teenagers in their bedrooms; it is a multinational, highly corporatised and highly sophisticated commercial undertaking—so much so now that if I were to want some malware for a nefarious purpose I can simply rent it or lease it as easily as I can do any commercial transaction online. These are fully corporatised structures with command and control, specialisation of tasks and their own internal economies. They are operating on an international scale with effective impunity. There is very little reliable research about the effect of this internationally. The figure that is quoted for the revenue to cybercriminals is $1 trillion per annum.

It is my contention that if cybercrime continues to grow at the rate that it has been growing, and continues to pose such a threat, that within a relatively short period—five to 10 years—the public internet will be abandoned by the public for any serious communications or transactions, and it will be left for games, gambling, pornography and other such uses. Any serious-minded use of the internet will retreat behind corporate, privatised nets.

CHAIR: Separate?

Prof. Fraser: Separate—highly secure, where there will be large teams of hundreds for each one working 24/7 to maintain the security of those separate networks. Then there will be the rubbish web for the rest of us, full of threats, insecurity and vulnerabilities.

This comes, in part, through the history of the way the web was developed, which I will pass over here. But basically it had built into its DNA that it was open and free, and that you could act anonymously. That worked very well when it became a network for academics to exchange information, as it was once it went past its early military phase, and when it was an area for enthusiasts and for those with a particular interest—that kind of cooperative approach to management of the environment of the web worked very well. But it will not do for a network that has become a mainstream form of communication and which is essential to the development of an information society and a knowledge economy, where Australia's competitive advantage lies in the future.

The point that I would like to make about that is that I applaud the necessary and important educational and training programs that are being offered by a variety of actors in the online economy, including government, law enforcement agencies, the ACMA, Telstra, industry and others. I support them, but the educational efforts are in themselves not sufficient to ensure security online. And, as we see, nor are the law enforcement efforts where we are trying to trace cybercriminals after the fact to investigate their alleged crimes and then bring them to justice. We are having limited success with that.

What is required is a prophylactic, or preventive, approach to building security—trying to reduce the opportunity for cybercrime. What that takes is a coordinated approach to build in technical standards and industry codes which will strengthen the internet—strengthen its security—and harden it from this open network approach into an internet where security is built in. What that takes is a lead agency to coordinate it. There is a lack of coordination. Say, for argument's sake, the lead agency were to be a law enforcement agency or some new cyber tsar. I think that is what is called for at this stage. That agency needs to bring all the players around the table: all the law enforcement agencies, the hardware companies, the software companies, the ISPs, the consumer groups,

and the representatives of vulnerable groups such as seniors or the young. It needs to bring these actors together to develop interoperable standards and industry codes that will reduce the opportunity for cybercriminals in what is now a very open network which is very vulnerable.

In addition to that, education is very important but no matter how much education there is it will not solve the problem. People's personal vulnerabilities are exploited very cleverly by these cybercriminals. We say that people have to have a password and they have to have antivirus software, but they forget to update it because it is a technical thing that they have to do, or they use the same password for everything, or someone rings them on the phone and says: 'I am from Microsoft. I am here to help. Just give me your code so that I can—

CHAIR: It happened to me last weekend!

Prof. Fraser: It is happening all the time. People, especially the most vulnerable and susceptible people in the community, should not be expected to have to deal with that on an individual basis. These kinds of threats need to be addressed by preventing the open slather opportunity that now exists. According to the statistics about where money is being laundered to, these people are operating largely from Russia and from Russian-speaking areas of eastern Europe, and from other places, and they are enjoying tremendous success. A two-pronged approach of education and prevention is required. We are not doing well enough on either.

The need for that kind of round-the-table cooperation is, with great respect, absolutely called for because it is not possible, even with the best will in the world, and the best efficiency and effect in the world, for legislative reform to keep pace with the mutations of these kinds of threats. It is a cat and mouse game. It is no criticism whatsoever of the parliament that it will necessarily lag behind in addressing this threat. Legislative reform of course is called for to bolster and strengthen security online, but a coordinated approach—a modern customer management approach where you bring all the players around the table to design the new product or service together, to design security into the way the web actually operates in Australia—is called for to keep pace with this threat, I would submit.

I think that more could be done to put responsibility on key choke points or hubs in the web. Naturally industry does not like the cost of that regulation, but, for example, the income of ISPs comes from their throughput and it ought to be incumbent on them by mandatory regulation or legislation that they look after the security and monitor and manage threats far more actively than they now do. It is fine to say that individuals should look after themselves and have their own antivirus software and take their own precautions, but not everyone is equally competent to do that, and there are hubs in the web where that responsibility can properly be placed, where the profit is made by the throughput, to ensure that those threats are reduced. I do not agree with arguments that these people are like public carriers and that, like the post office, they should not be looking into the mail. Of course there are privacy issues that need to be managed, but I think much more could be done by the ISPs, for example, in managing and creating a secure environment for their customers. That is part of an ideological discussion about regulation or no regulation, but I think it is necessary in this instance.

CHAIR: One of the questions we have been asking other people is: do you think there should be mandatory regulations for ISPs in regard to how they work and cybersafety issues?

Prof. Fraser: I would say, yes, there should be, because it has sort of become normalised now that all kinds of criminal activity happens online. People seem to accept that, and business is growing, so they naturally will not want to meet any of those costs. They are making considerable efforts, but I think the bar needs to be raised. I think it would be justified to mandate that.

CHAIR: Are you happy for us to move on to questions, or is there anything else you want to mention to us before we do that?

Prof. Fraser: I will very quickly mention three things, if I may. I think that it would be helpful for senior Australians themselves to play a more active role in volunteering to assist their fellow senior Australians. That could be facilitated through government.

At the Communications Law Centre, I receive a lot of complaints from people who make complaints to the state police. They go to the police station or they ring the local police station, and it seems to me, anecdotally, that police are not able to receive those complaints. If they are able to receive them, there are not the forms, the processes and the systems for them to manage them. A constable might refer a complainant to the Federal Police or the High Tech Crime Centre. They refer them back to the state police. I do not think we even have any measure of how much cybercrime there is, because I do not think the police are able to receive the complaints and to respond to them adequately.

The other suggestion that I had—and this is my last point before opening for questions—is that, at least for the next 30 years, there will be people of my age and older some of whom will not use the internet or are very fearful

of using the internet. I would make the analogy to the days when there was a great deal of illiteracy in a small town or a village. People have to deal more and more online with government agencies and other important providers. I would suggest instituting cybernotaries—say, in shopping centres—where people could go to log on to Centrelink and know that it really was Centrelink and do their business with confidence, just as people used to, in olden days in the village, go to a notary or justice of the peace when they had to transact with government or official papers in some way when they could not read. I think that situation will last for about 30 years, where there will be people of my generation and older that could be helped by such a proposal.

CHAIR: I am aware that all my colleagues have got questions to ask you. I wanted to quickly ask you, though, about the research partnership the Communications Law Centre has recently announced with LeadBolt to develop a mobile commerce standard. I wonder if you can very quickly talk to us about that.

Prof. Fraser: LeadBolt were criticised in the press for claimed breaches of privacy. They send ads to mobile phones on behalf of advertisers. In order to do that, I understand that they draw information from the mobile phone to create a profile so that they can target ads for advertisers. A similar issue has been raised recently with Google and the way it harvests information from all its services to get a profile. LeadBolt were concerned to work with us to ensure that they were meeting privacy obligations and their own privacy policy and, if not, then to develop industry best-practice standards. To their credit, we are discussing the possibility of establishing an industry-wide standard for m-commerce and perhaps industry bodies to oversee those standards. They are also persuaded that perhaps legislation will not be able to keep up with these fast-developing services. We have not yet begun the actual research. We are in the process of recruiting the researchers to begin it.

CHAIR: Professor, are you able to quickly tell us how they harvest that information?

Mr PERRETT: From the phone.

Prof. Fraser: I cannot tell you properly yet. As we say, we have not done that research, but I understand that when they send ads and you get these ad banners appearing, they are technically able to reach into the phone and draw out personal information from that phone using cookies and other such things. I am not certain that is correct, because we have not begun the research at all. We have just formed this partnership and, as I say, we are recruiting the researchers. But that is my second-hand understanding.

CHAIR: Based on your knowledge, do you think that the standards currently imposed for ISP providers are tight enough to allow that to happen?

Prof. Fraser: No, I do not think so. I think that the breach of privacy is one of the most worrying developments in our society and the way that private information is used for purposes that are unknown to the individual whose private and sensitive information has been gathered, sometimes for direct purposes but also then leveraged for secondary and tertiary purposes unknown. I think it is a threat to democracy. Our forebears fought against set-ups where there were institutions that knew who you spoke to, what you were reading, what your political affiliations were, what kinds of things you drank. There were organisations such as—without trying to overblow this—the Stasi, the KGB and the SS, whose job was to find those things out and to use them for their own purposes. There are now multibillion dollar corporations who are gathering that very same information, and it may be that their management today are very nice people—I do not know—but they are corporations and they may use that information for any other purpose. I see it as a tremendous threat.

CHAIR: You mentioned the research—what is the time line on that?

Prof. Fraser: We are going to do the first phase of the research over the next two to three months, which will be a scoping exercise and part of that will be to draw out the time line of the further research. I cannot answer that question yet.

Mr PERRETT: Further to the research query, I assume by the time you have found the people—these are specialised skills in terms of being both criminal and investigating the criminal—one of the problems would be that they have moved onto a new scam or opportunity by then.

Prof. Fraser: Yes. I think there are two ways of trying to deal with that. One is to legislate to reduce the opportunity for anonymity online. There are many civil libertarians who value the opportunity for anonymous communication online, but it is being exploited by a whole range of criminals. One of the standards—and I understand it will be controversial—that should be introduced is to reduce the opportunity for anonymity because otherwise they just transmogrify and you are back to square one. They have moved on. They have changed their IP address. I think that is one of the important standards.

The other is the need for much greater international cooperation. There is the European Convention on Cybercrime. We have not signed up to that yet but—

CHAIR: We have certainly been trying to. We did an inquiry on it, and it has gone through. There have been delays in the Senate.

Prof. Fraser: In the bill, yes.

CHAIR: It has gone through the House.

Mr HAWKE: It sailed through the House.

Prof. Fraser: I think there were legitimate concerns there and there is no criticism of that. In due course, we will sign up to that. It is still the case that, if a law enforcement agency wants to investigate what has happened in a foreign jurisdiction, there is a process that might take six months in some cases. Some law enforcement agencies have been building better arrangements, but it is ludicrous to try and follow that trail with a 19th century process for getting evidence from a foreign jurisdiction. That is also an essential element.

Mr PERRETT: That is the end of the process. You started by talking about interoperable codes and getting all the players together. One theory is that the horse has bolted on this; it is already over. How could we get all these people together—law enforcement, the ISP providers and the international community? Is it a simple process or is Pandora's box well and truly opened?

Prof. Fraser: It has been, but I do not agree with those people that say you have to give up. It seems to me that it is puerile to say that somehow this area is outside our law or above it or it has gone too far and too fast. That is an adolescent point of view. It is an important part of our society. It will be regulated according to the norms that we apply in the rest of society. To say that somehow it is different and special—

Mr PERRETT: I am interested in it, not quite as a Luddite, but in terms of law and order—say, John Wayne comes into town to say to the people with the guns, 'You've got to settle down and put your guns down.' How do we do it? Should it be done by people like Telstra? Are there some big sticks that can be easily manipulated?

Prof. Fraser: I think it will take government—as it usually does—to bring everybody around the table, first on a national basis, to do what they can to make the web more reliable and less susceptible to cybercrime and cyberespionage nationally and to develop standards and codes across the whole supply chain to make that happen bit by bit. That will be an ongoing task and a complicated task.

Mr PERRETT: Should we be attacking their wallets, the businesses' wallets? They make money through volume and we would be putting some bottlenecks in that process, surely.

Prof. Fraser: Yes, you would, because you would be thinking more than the end of the quarter, as government, with respect, should. It would be like saying, 'We are going to put up some traffic lights at the intersections now and it will slow things up for a few nanoseconds, and we will have some laws about where pedestrians can and cannot cross, even online.' But unless we do that, I think that over a relatively short period of time, confidence will erode in the whole capacity of this technology to deliver what we are counting on—that is, an information society. I want to just add one more point. It cannot just be national. While they are doing that, they have to reach out.

Mr HAWKE: I am interested in what you are saying here. It is a little different from other constructs that we have heard and I am not sure I agree in some ways—but that is not material, we are not going to have a debate today. It is kind of a dark construct on the internet at the moment. I am interested in your comment that we would go back to these private networks, essentially. Are private networks not one way of solving this problem in which people are doing bad things out there? In fact, private networks that are verified by a commercial provider or other providers are one answer. That is probably the most effective way because it is in their interests to do so. Telstra was here just before—I think you may have heard some of their evidence—and it is in their commercial interest to ensure that their user has a good experience. I accept that contention because otherwise they would be out of business.

Prof. Fraser: I think players like Telstra could do a lot more about providing information at the point of sale and on their bills and in informing consumers more than they do about the existence of the TIO and other agencies. They are naturally commercially focused. On the wider question, I do not in any way object to the idea of these private networks being established, and we see them being established. The large banks and others will have their private networks and they have 250 techs sitting in a bunker 24/7 fighting the constant attacks—they are probably getting hundreds of attacks every day. But what I do not want to see is a digital divide open up so that if you are dealing in a commercial space you can operate inside these walled-fortress webs, but you are otherwise left to protect yourself. So if you are in John Wayne's town you are all right, but past that is the badlands. That will lead to a digital divide where underprivileged members of the community do not have the same security, unless they are doing certain kinds of commercial transactions which are within these fortresses. The possibility, which we cannot yet properly imagine, is that an information society will develop, including the

kinds of communications, services and creative industries that will spring up, which will be fettered in its development.

Mr HAWKE: This is a very interesting topic. It makes me think a lot, but I do not necessarily agree with a lot of your comments. I disagree profoundly with your comments about the operation of the internet, similarly to the Industrial Revolution, not being a different thing in human history. I think that the Industrial Revolution was different—it changed, shaped and set society on a different course—and the internet appears to be doing the same thing. It is another revolutionary turning point.

So my question to you out of your evidence is: are we not still talking about human beings and human society, now just in a digital format? There are the same risks, the same problems and the same behavioural issues that you have in the real world, with some different pronouncements, emphases and other things on there. But are we not then talking about solutions that operate the same way? Criminals online are the same as criminals offline, and our responsibility as a government is best used in establishing criminal law, making sure it is enforceable and that it can be enforced, as you say, quicker, easier and faster—all of those things. Surely, don't you think that our energy is more productive in that space rather than regulating or trying to stifle a current of energy which is overwhelmingly a force for good? I would rather target those people who are online doing the things that are wrong.

Prof. Fraser: As far as I can see, I am agreeing with you.

Mr HAWKE: Sorry!

Prof. Fraser: Except perhaps that I do not think you can solve the problem by targeting only those who are doing things wrong. I think you have to build the security into the network.

Mr PERRETT: Education and prevention agencies?

Prof. Fraser: And prevention—

Mr HAWKE: Yes, I separate all of your education and everything—I think these are responsible things. But I am talking about the people who do bad things on the internet. They are going to exist, whether they be, like you say, corporate now or not. I think you are right; they are larger, they are corporatised, they have better resources and all those things. But we face things like jurisdictional issues whenever we ask questions about why we cannot do something about this. There is inadequacy of law, like you said—the state police and the Australian Federal Police. Is this not where we could really spend some time in new thinking in how to frame law and how to frame agency responses that would actually help us to target these people appropriately? The people who are doing the bad things on the internet.

Prof. Fraser: Yes, with respect, I agree with that. The only thing that I am saying is that we have to address it with equal vigour at both ends of the problem by also reducing the opportunity. The reality is now that these villains are working with absolute impunity, especially where there are kinds of malware and scams that are skimming a few cents or dollars off millions of people's accounts, nobody is able to track them down and prosecute them.

The law enforcement where John Wayne comes into town after the crime has been committed and chases down the bad guy is one approach. But we want to make the town safe to begin with as well. They are both necessary, and I think that we are not putting enough in. Law enforcement naturally wants to chase the bad guy; that is what they are good at, and thank heavens that they protect us in that way. But it is the actual building of the social infrastructure of security into the online environment, so that when I go to my computer at my desk there will not be all these strange offers and malware and trojans and scams that I have to confront—to prevent that from happening needs more attention.

Mr HAWKE: It is very interesting what you say. My final point is that I just want to draw an analogy for you to see what I am getting at—let us say the things that governments are interested in doing and involved in everyday. For example, the analogy I draw would be tax legislation. We have a lot of tax legislation, and every year we pass TLAB—tax law amendment bills—which amend the tax laws in so many different ways. Even the brightest tax lawyers in the country really do not understand them. But we do not put that emphases on this kind of criminal behaviour on the internet. We do not have a series of legislation that is constantly amended and updated, which, as you say, you cannot. I do not think that John Wayne should be riding a horse today, fighting these people, but we can equip them with almost the latest, up-to-date responses in terms of legislation and the ability to chase. We are not doing that as a government—I do not think that we are really addressing that problem.

Prof. Fraser: Yes, I agree, and I would add that along with legislative preventative measures that code is code. So if you build technical standards in as well then they can keep pace. Where legislation would have a more overarching shield, technical standards would chase the morphing threats.

Mr HAWKE: Absolutely! I just do not find any government effectively addressing this question.

Prof. Fraser: I believe that is the case.

Ms MARINO: One of the things that I wanted to ask you about is whether you have had a look at the personally controlled electronic health records process and what has been suggested for managing the risks associated with that. As I have said earlier here, I think the relationship between doctor and patient and the trust that exists there is paramount, underpinning confidence in our health system. So in managing the cyber threat, if you like, to the personally controlled electronic health records, I have a couple of issues of concern.

Do you think the central repository of information that will exist to the government level in relation to this information is at risk and, if so, is there a significant risk in your view given the nature of the Eastern European cyber criminals that you have discussed and those who would have a lot to gain out of that information, as you have alluded to previously? Secondly, in the way this system physically operates, have you any concerns about privacy, about the laws surrounding penalties and the rights of the consumer and the customer, so to speak? Can you provide any points that you believe would be of use in looking at the issue of personally controlled electronic health records and the system that it uses to do so?

Prof. Fraser: Thank you for that question. The more that information is networked and databases can be brought together and connected to make enriched information available, the more useful the information is but the more susceptible it becomes to damaging breaches and cybercrime. These threats are asymmetric threats so it is the hallmark of this environment that the more we develop these services and link the most sophisticated technical expressions of our culture, the more vulnerable they become to interception and misuse.

In a way, our society nowadays is defined by that. We saw in 9-11 commercial passenger aircraft, one of the most sophisticated expressions of our technical and social culture, being turned against us as missiles by a few blokes with box cutters. So the more sophisticated we make these systems and the more connected they become and the more useful they become as social and technical services, the more vulnerable they become to attack and the greater the risk of damage from an attack. I think that it is a very valuable thing that these personal health records can be stored and can be made accessible, but I want to know that if I go down in Darwin someone will be able to look at my record from Bondi Junction and from St Vinnies here and know that I am allergic to this or that. I think that that is an incredibly valuable thing but it is very vulnerable to serious misuse.

There is no ultimate security except to disconnect it from the internet. The most sensitive databases are disconnected from the internet and are put in glass rooms in the middle of the floor. So the issue of security is paramount in individuals having confidence that their information will only be used in circumstances for which they have given prior informed consent. I am not an expert on the technology in that system so I cannot answer the second part of your question as to where the vulnerabilities may lie and how they may be ameliorated.

Ms MARINO: Professor, in the next period, if you do have any cause to research that further or you have any comments that you would like to make on that, I think that would be useful for the committee.

Prof. Fraser: Thank you.

CHAIR: Thank you, Professor, for your time today. We are on a bit of a time limit, as you know. If you have any further information that you wish to supply to the committee then we are very happy to accept it.

Prof. Fraser: Thank you very much for inviting me. It has been a pleasure.

OSBORNE, Ms Lesley Ann, Manager, Digital Society Policy and Research Section, Australian Communications and Media Authority

TROTTER, Ms Sharon, Manager, Cybersmart Programs, Australian Communications and Media Authority

WRIGHT, Ms Andree, General Manager, Digital Economy Division, Australian Communications and Media Authority

[14:15]

CHAIR: I welcome representatives from the Australian Communications and Media Authority. Thank you for your submission, which has been received as No. 24 in the committee's inquiry. Before proceeding, I should remind you that this is a public hearing and is being recorded by Hansard and audio broadcast.

Mr PERRETT: Chair, could I say just for the record that I know Ms Trotter from another life.

CHAIR: I am glad you have put that on the record, Mr Perrett.

Mr PERRETT: For the second time, I think.

CHAIR: I notify you that, although the committee does not oblige you to give evidence under oath, this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House and the Senate. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Ms Wright, do you wish to make an opening statement before we proceed to questions? I do have to warn you that we have only three-quarters of an hour, but of course we are more than happy to call you back another time. I know that you probably have lots of information to give us, so if you want to take about 10 minutes or so then that is fine.

Ms Wright: Thank you, Senator. Yes, we would like to avail ourselves of the opportunity. We feel it is timely that we are here today because we note that it is Seniors Week in New South Wales, and New South Wales is currently celebrating the many diverse contributions that seniors make to the broad community.

I think your committee is aware that I and my colleagues are passionate about cybersafety, and we welcome the leadership role that the committee is playing, we feel, both in Australia and internationally with its focus on the cybersafety needs of seniors. We are aware that the emphasis internationally has been on young people to date and there has been much less on seniors. We think that made sense early on when young people started to live a lot of their lives online, but seniors are following there as well. We are increasingly focusing on the notion of cybersafety education as something you need to equip you from the cradle to the grave in this day and age.

I know you are aware of the work we do with our Cybersmart program, but perhaps the committee is less familiar with the wider role generally that the ACMA has in delivering effective consumer protection measures and ensuring that the community is well informed about communications measures generally. For example, that includes initiatives such as the Do Not Call Register and avoiding and reporting spam and also addressing the problem of compromised computers and the spread of malware. In all the work that we do in providing programs and services to the community on these communications measures, we see that it is vital that they are underpinned by three key program delivery principles.

First of all, we think it is important that you never presume that you know what the problem or the answer is and that you do research into what Australians are doing and find out what they need. Secondly, you then do not presume that one size is going to fit all and you deliver through a variety of delivery channels and tools. We have found in our work, in administering our programs, that there is a wide range of needs and ways in which people like to access information. The third principle that underpins our work is working in partnerships in order to maximise the reach of what we provide. We think these are very important matters.

Also, from our experience, we know that people do not want a wealth of theoretical information. They want some helpful tools that ensure positive behaviour and good results. One of the things that I might leave with the committee, if I could, would be a publication put out by one of our service providers late last year which looks at education. I want to particularly flag the fact that it has a how-to section, so, for example, on how to set up Facebook privacy controls and how to set up Google SafeSearch. There is another how-to in relation to Microsoft Windows.

CHAIR: Ms Wright, just before you go on I will move that that be tabled. As there is no objection it will be so. I thank the committee members. Please proceed.

Ms Wright: What is important here is that it does not say 'set your privacy settings' but gives you five steps that you can follow and then it is done. We think that is very important. So we think the move from saying 'we're

giving you some tips for setting your privacy settings' to guiding people through is the way that we need to approach education programs. We think this is particularly so with seniors.

If I could sneak in a fourth principle, it would be that you do not automatically think that we need to reinvent the wheel. I was talking to a colleague and friend the other day about the fact that we were going to appear here today before you and they said, 'I received some spam recently. Wouldn't it be great if we had a reporting device for spam.' So I went back to my office, I went to Google and I deliberately did not click on 'Australia' so I went on the Web so it would be broad. I entered 'reporting spam'. Of the top seven things internationally that came up for 'reporting spam', the first three related directly to the ACMA: 'How can I report spam?', 'Reporting spam' and 'ACMA: spam'. The fifth was an international tool but the sixth and the seventh took me to the ACCC's website on how to report spam, to the ACMA—so partnerships are good—and how to report scams, and that goes to the ACCC. Often people will say in conversation that we need a such-and-such but it is important to actually check what is there.

But the questions it raised for me are these. As I keyed in 'reporting spam', I would be saying to Lesley, when we next did research, 'Can we check in a focus group of seniors whether that is the term, if a senior were spammed online, they would actually use? Would they go to Google? Is there some other expression that they might use?' Then that is what we would be wanting to link to our services so they could find them easily.

Coming back to the program principles and applying them to seniors, as you know our experience at the ACMA with seniors in the cyber area to date has been mainly with grandparents. We are very aware of their role as carers, and they do like to come along to our face-to-face parent presentations and they display an interest there. This year for Safer Internet Day we did particularly target grandparents. From the knowledge we have from our research to date, they like face-to-face presentations. Even after the Safer Internet Day campaign we have found a number of seniors clubs have approached us to come and do those face-to-face presentations and be interactive so that seniors can be guided through the steps from turning the computer on. We also endeavour to, if you like, knit across the generations, and we provided a list of questions to seniors that they might ask their grandchildren so that they could get online, search, and learn how to use social networking sites. We think young people love to help their grandparents in this way, but we think grandparents can be embarrassed because they actually do not know the questions to even ask in the first instance.

The third resource that we are aware they want is when they have got some expertise, they are appreciative of online tools to guide them further. So, with the research we want to go back to two threshold questions: first, what are the barriers to their participation to date, so that we can understand the kinds of strategies that will motivate and support older Australians to go online? Then we also want to explore how we can ensure that their participation is safe, so then we can then drill down to the types of messages and information that would make a difference to seniors, recognising that it is a very diverse cohort, and how we can then ensure that when they do go online their experiences are positive.

I emphasise the importance of delivery channels, and we already know from the work we do with younger people, where we utilise schools, libraries and other such forums so that we can also reach the parents, that again it is important to find out what will fit into the broader life of the senior so that they can access information: do they go to computer clubs, senior citizens clubs, libraries or other outlets associated with activities of interest?

We are aware that young people, for example, if they are in a service or a site, if they want help they like to get it from within that site. Again, it is not just enough to have our shopfront: we want to be working with other partners so if there is a problem when they are online with the service, they can get information there. We believe—but think it should be tested—that it may be the same for seniors.

CHAIR: Ms Wright, we might need to move on. I am sure there are lots of questions.

Ms Wright: I was going to end simply by saying thank you for inviting us to speak today. We would welcome questions.

CHAIR: You have done some research and it indicates that seniors tend to use the internet for email and research but not so much for online shopping, networking, blogging and other things. Are you able to tell us a bit more about the methodology of your research and if there were any different trends, for example across states and regions?

Ms Wright: I will ask Leslie Osborne, as our head of research, to answer that question.

Ms Osborne: This piece of research—

CHAIR: Can I just ask, is that research publicly available or available to the committee?

Ms Osborne: Yes, it is, and it is probably best if I provide it.

CHAIR: Just give me a quick precis.

Ms Osborne: This piece of research was part of our Communications Report 2009-10 series and we asked all of those people, which was the general population online, about the activities that they undertook. The point that you made in terms of communications activities, research and information is an illustration of the way that the use of the internet is now becoming mainstream amongst older people, but they are not using yet the services and participating in the kinds of activities—particularly transactional activities where they might be some anxiety about e-security and safety issues—as young people, who are more confident because they are online more. That was my takeaway from that particular finding.

CHAIR: Have you got that report to table today or will you just forward it to the committee?

Ms Wright: No, I just have the chart.

CHAIR: That is fine. If you could forward it to the committee, that would be wonderful. In your submission you mention the barriers to participation in the digital economy and the CCI research. Is that different from the research we were just talking about, and is that publicly available as well?

Ms Osborne: Yes—that is one of the major pieces of work that has been done on seniors and their participation online. I think that was possibly an ARC supported study, and we can provide you with the link to that research.

CHAIR: That would be wonderful. This may not be an appropriate question for ACMA, but do you see cybersafety as a responsibility of ISPs and if so to what degree?

Ms Wright: With our work to date we have proceeded on the principles that underpin the legislation we work on—that this is in a sense, in our language, a co-regulatory area—it involves input from the government, industry and users or citizens. Another way of characterising it is that there are things you can do when you are supplying a service from the supply side, and that can be from industry and government, but there are also things on the demand side that people need. One of the initiatives that we have is the Australian Internet Security Initiative, where we are able to pass on reports of compromised computers to particular industry participants who then check them out and they contact their users to inform them that their computers are compromised, and they work with them to address that. We have initiated that in Australia and it is regarded as an international first and best practice, and it has been emulated by other countries. We would be happy, since we are undertaking to provide you with a number of pieces of material, to follow up with the number of compromised services that are reported to us daily—and it is a large number—and the number we then pass on to service providers and the type of buying in that we get from service providers.

CHAIR: Do we know if there is any obligation on service providers to then report back to the people whose computers have been compromised?

Ms Wright: It started as a voluntary initiative. If we look at the icode, the icode which is currently under review, in its first iteration one of the ways that providers could meet some of the subject areas of the icode was by taking the AISI initiative from the ACMA. There are increasing incentives to do so.

CHAIR: What would the outcomes be if someone did not let the consumer know that the computer had been compromised? Would they maybe never necessarily find out?

Ms Wright: Apart from saying that it would not be good, I probably do not have much detail on that to provide you with, because our emphasis has been on encouraging providers to do that. We know that the trend is trending upwards. We notice in other areas around the world where that type of service is not necessarily on offer that there is an increasing interest in what we are doing here in that regard.

Mr PERRETT: I am interested in your comments on the government's webpages, in terms of how user-friendly are they and are they cybersafe, and whether we should be rewarding people generally for having effective and safe webpages.

Ms Wright: Our research in the whole cybereducation area has shown us that when we are dealing with adults they regard government as a trusted brand. They tell us that, when they go online and they google and they get hundreds and hundreds of resources, they look for something that they feel is authoritative and that they can trust, and government rates well there. I think it is then up to government to honour that trust and apply the types of principles that I spoke about earlier to test the service you are providing—as you are developing it, test it with users to make sure it meets their needs—and to also know that services do not stand still, so a tool that may serve people today needs to be regularly kept under review so it remains current. Certainly the idea of positively rewarding those initiatives would build on the interest I have in people being aware of what is out there and not

having to reinvent the wheel—because a vast range of choices without knowing which ones you can trust can be quite confusing for users.

Mr PERRETT: You have not given anything qualitative there in terms of how the government operates at the moment. You have not passed comment. You have talked about a framework but you have not given a judgment.

Ms Wright: I am resisting the temptation to say our own resources are very good, Senator!

Mr PERRETT: I am in the House of Reps, not in the Senate.

CHAIR: Yes. There is only one important senator here!

Ms Wright: In that case, I address my answer to the chair! Lesley, I think we had statistics on the confidence and the trust. I have also noticed statistics recently in more general publications about the take-up online of government services and the way users like to get their information in that regard.

Mr PERRETT: So there are positive signs.

Ms Wright: Yes. I do not know if you have any of those statistics at hand, Lesley, but I was surprised by the very high percentage of people who are now regularly accessing online services. But again we would need to be testing what age groups and what cohorts are using those services.

Ms Osborne: I understood that you were getting at a couple of things there. Research that we have done as part of our digital media literacy program has included concerns by users about consumer protections and education they might need when they are using new mobile services like mobile wallet or are involved in sharing personal information online. We have pursued—this is more in a qualitative sense—expectations for information, and that is where particularly we have identified that people are comfortable with and can look towards government to provide information about consumer protections in those areas. We have not evaluated particular resources. Most of the work that we have done specifically in this area has been research to support the development of educational resources for cybersafety, for Sharon's people, for instance—and she could tell you a bit more about that. Where we do have some statistics was a study that we did with parents about how they would like to receive information and what was the most trusted source. That was where we have information that, if it came from the government, parents would take more note, and they would be particularly comfortable with material that was from government but delivered through schools. I know there are independent assessments of websites that are available, done more by academics, for instance.

Mr PERRETT: Certainly we, as an interface with our voters—and, being in the House of Reps, we have a clearly defined group that we interface with—

CHAIR: Yes. Senators just have to deal with their whole states!

Mr PERRETT: Touché. My office is often the interface between someone who has called up and asked what is happening and the government agencies, so we use the government websites a lot, and there are a range of qualities there. Some take it very seriously and I think it expedites the process; others are a little bit labyrinthine.

Ms Wright: Taking your point, we are moving into a time where it is not necessarily enough just to have a range of separate initiatives. I think it is beholden on government to coordinate more generally what is offered, to ensure that there are not gaps or duplications and also to ensure quality. There is no point offering a service if people are not using it. So it is very important to show that you have evaluated your service and that it is having a positive impact and is driving changes in behaviour; otherwise, there would be no point in using that vehicle.

Mr PERRETT: Academics might be the stick in terms of analysing, and some awards might be good in terms of recognising good behaviour. Is that something ACMA would see the benefit of perhaps?

Ms Wright: Yes. I think it would raise the awareness of what already is on offer, and that is important. There are probably some areas where more resources are needed but there are also ones where there are resources but people are not necessarily aware of them until they actually need them, and then they want easy to access, just in time information. If they can then remember that they have read or seen something on television about a service that was particularly good, that tends to come back into their minds.

Ms MARINO: Thank you very much for being here today. One of the things I wanted to ask you about is whether you have looked at the proposed e-health system in the personally controlled electronic health records. Given that we have heard today that through this process the consumer, an authorised representative, a nominated representative and healthcare providers will all have access to a personally controlled electronic health record, I wonder if you have looked at this and identified any gaps or risks associated with that process and how that works in a physical sense as well as an electronic sense.

Once this is up and running, I suspect that one of the next round of scams we are likely to see out there are targeted health scams and seniors may well find themselves as a specified target of those. We know that seniors

can be quite vulnerable given the statistics that we see in relation to scams. Given their concern about their health and perhaps the trust that they have in health professionals, some may actually believe that some of these scams could be quite genuine. So in the early stages, until that becomes apparent, I wondered whether you were designing products to manage this type of scam, particularly for seniors.

Ms Wright: That is currently beyond and outside our remit. You may or may not be aware that the ACCC has carriage of Scam Watch Awareness Week. While we participate in that awareness week, we also tend to pass on to them reports about scams should we receive them. They may be in a position to assist you, because it is more focused on their remit than it is on ours today.

The role that we have to date when it comes to the online area has been principally focused on young people and their carers, but we felt that we could contribute today because that has picked up grandparents, and we have done research which makes us increasingly aware of the needs of seniors. But our remit is not that extensive. I would expect that the ACCC may be able to talk more about their scam watch activities and what they are aware of in that regard.

CHAIR: I would also make a point there. The ACCC are currently undertaking some work in relation to dating and romance scams. So they are getting a bit more inclusive and current about it.

Ms MARINO: Maybe one thing would be for young people to alert their grandparents to the issues facing personally controlled electronic health records and to look at how they can help prompt their grandparent to be aware that this type of scam could be out and about. I think all forms of encouragement in this field would be appreciated. So if you are not directly involved, perhaps an indirect way of encouraging grandparents would not be bad either.

Ms Wright: Yes—noting, as I said, that on Safer Internet Day we provided grandparents with questions they could ask other members of the family when they went online together to explore. It is relatively easy to build in questions that they can ask. As I said, they were often embarrassed to ask a grandchild to help them on the internet because they did not even know how to phrase the question. As somebody who quite a long time ago now benefited from the 'teach your mother to text' campaign, I think these are wonderful initiatives.

CHAIR: Earlier in the day we heard from Telstra. One of the suggestions was a task force developed specifically for seniors and cybersafety. I am wondering if ACMA have any view on the potential of such a task force. Do they think it would be worthwhile?

Ms Wright: We have not had discussions in that regard, but we work on a number of matters with Telstra. It is one of the areas where we endeavour, in the education area, to make sure that we do not duplicate but rather promote the good things that each might be doing and are conscious of them. We are aware that their representatives are increasingly concerned that it is not enough to provide information and education only to young people and we have to look beyond that. That is a view that we share. Any such task force would be an extension, if you like, of the relations we already have with them. We think it is a fertile area to be also looking at adults in their own right, not just as carers.

CHAIR: Ms Wright, I am just reading once again and refreshing my memory of your submission. I have highlighted here the recent study you commissioned—I think you have alluded to it already—that surveyed international cybersecurity awareness-raising and educational initiatives in 11 jurisdictions. Are you able to give us a brief outline of the results of that?

Ms Wright: I will ask Sharon to assist me. A couple of years ago we were very much focused on supplementing the programs that we already offered. Most of the Cybersmart programs we offer have security information because we believe that people do not go online and say, 'I want to be safe today and I'll worry about security tomorrow.' For users it is part and parcel of the same thing and they need both at once. In coming up with some specific programs on security, we wanted to see what had been done internationally and how successful those programs were. We would be very happy to provide you with a copy of that research. The memory I have of it is that, of the 68 that were looked at internationally, about 14 per cent specifically targeted seniors and hardly any of those programs actually evaluated what they had done or the impact of what they had done. We thought that, in anything we did, evaluation would be very important. Sharon, do you have anything to add on that study or that general area?

Ms Trotter: I think that you are right. You have made the two points. One was around the lack of programs targeting seniors, and the other key point coming out of it for us was around the lack of evaluation. We are using the identified need for evaluation to build into our program development going forward. The research is published and it is online, but again we would be happy to send you that. It identified a range of cybersafety and

cybersecurity programs from the general awareness type programs right through to the educative programs, so it is a good resource. I am happy to send you that.

CHAIR: Thank you. There are obviously a large number of seniors who do not go online so would never have seen any sort of program of education on security and how not to get scammed. Do you have any suggestions to the committee about what sorts of broad approaches we could take?

Ms Wright: Again I will start off and then turn to my colleagues. As I mentioned, once we had focused on grandparents on Safer Internet Day, we found that a number of seniors organisations approached us for outreach presentations. I have just mentioned two in passing that we have done this month, one with the Gosford City Council and another with Bega Valley shire.

Our trainer said to us that it was very interesting to him because, on one hand, the seniors there very much wanted to be guided through going online and what they needed to do and they wanted it to be interactive; they did not want just to listen. I believe he was able to accommodate that. Then, once they had a feeling for the mechanics of what you needed to do, what you could do and what was on offer, they moved to focus on various security concerns: how safe was their credit card, and what do you do about maintaining your privacy?

This underlined that for some people who do not even know how to go online you have to start almost face to face or have a program where they can work with a family member without embarrassment, to start off, and then you can build on that with online resources. But if they do not know how to turn on the computer they cannot get to the resources. We have found even more generally with our programs that our online tools are well received, but what people, schools and young people like best often is the face to face, and then they see the others as adjunct. Sharon, do you want to amplify?

Ms Trotter: When we did our Cybersmart parents research, we identified that parents themselves often had a need for a telephone number as well. I think that with seniors we can probably surmise that some of those traditional media forms—television, radio, obviously, and the print media—might be a good way of reaching them as well. I think this is something that would be very worthy of further exploration in terms of what is really going to resonate. That is probably what we can infer so far.

CHAIR: In the last five minutes or so, is there anything else you would like to add—any other information you would like to give the committee?

Ms Wright: I think you have been very kind with the time you have made available to us. I would just like to reiterate that, if there is anything further we can do to help or provide, please contact us at any time.

CHAIR: Thank you. I thank you for your evidence today. I bring to a close what has been a very rewarding and very fruitful day of evidence gathering. We have heard from a large range of submitters and have been given quite a lot of food for thought in regard to the inquiry. I thank everyone who has attended the hearing and given evidence. Should the committee have any further questions, the secretariat will seek further comment from those people at a later date. Thank you to Hansard—very patient and very nicely behaved today! Thank you, committee, and thank you, secretariat.

Resolved (on motion by **Ms Marino**):

That this committee authorises publication of the transcript of the evidence given before it at public hearing this day.

Committee adjourned at 14:53