COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON COMMUNICATIONS

Reference: Cybercrime

FRIDAY, 9 OCTOBER 2009

SYDNEY

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON COMMUNICATIONS

Friday, 9 October 2009

Members: Ms Neal *(Chair)*, Mrs Hull *(Deputy Chair)*, Mr Billson, Mr Bradbury, Ms Collins, Mr Georganas, Mr Irons, Mr Lindsay, Ms Rea and Ms Rishworth

Members in attendance: Mr Billson, Ms Neal and Ms Rea

Terms of reference for the inquiry:

To inquire into and report on:

The incidence of cyber-crime on consumers.

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information:

- Including the impact of malicious software such as viruses and Trojans.

b) The implications of these risks on the wider economy:

- Including the growing economic and security impact of botnets.

c) Level of understanding and awareness of e-security risks within the Australian community.

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:

- Education initiatives
- Legislative and regulatory initiatives
- Cross-portfolio and inter-jurisdictional coordination
- International co-operation.

e) Future initiatives that will further mitigate the e-security risks to Australian internet users.

f) Emerging technologies to combat these risks.

WITNESSES

Committee met at 9.31 am

BROOKS, Dr Paul Westley, Director, Internet Society of Australia

RAICHE, Ms Holly, Executive Director, Internet Society of Australia

CHAIR (Ms Neal)—Welcome. I declare open the public hearing of the House of Representatives Standing Committee on Communications inquiry into cybercrime. This is the sixth public hearing of the inquiry. Today the committee will take evidence from IT companies and organisations representing seniors, computer and internet users.

Thank you for making yourselves available. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Would you care to make an opening statement?

Ms Raiche—A statement was made yesterday which suggested ICANN does not do a lot of work with the consumer organisations. If you go to the ICANN website and look at the ICANN structure, you will see it is a very open and transparent body. In fact there is so much information that generally you get swamped in acronyms and think it is all too hard. One of the important bodies that advises the board is the At-Large Advisory Committee. ‘At-large’ is a kind of shorthand for all of the internet users worldwide in the five regions that Paul talked about yesterday. That covers a lot of internet users, all of whom are either residential or business consumers. The committee does a lot of work dealing with consumers. The generic name ‘supporting organisation’ is that body of top-level domains over which ICANN has control through its contract with registrars. That is what gives it control over generic names registrars. There is a council there and ICANN, just in the past year, has said it wants a far more active consumer constituency. At the next board meeting in Seoul it will decide on the consumer constituency. We as ISOC-AU have put our hand up and said we would like to join forces with some other consumer bodies and be part of the generic names supporting organisation. I would say that things are happening in terms of ICANN, ensuring that it listens to consumer voices. It is certainly moving in that direction and I would hate anyone to think that it is not.

Mr BILLSON—So the observation may have been right, but this thing is happening?

Ms Raiche—Things are happening. In terms of what registrars do, there is now cooperation between the ‘At-Large’ community and the generic names organisation to develop a registrants charter of rights, which is going to focus on what registrars should do to look after registrants. The registrants are the ones who actually have the domain names—that is, business and residential consumers. I am part of team B, which looks at how you should add to those rights, and a lot of the discussions that will happen in that newly formed group will be about improving the rights of registrants. There are things happening; it is just terribly opaque to everybody that does not work with those acronyms.

CHAIR—Maybe you could tell us, firstly, a little bit about your own organisation—how it works and how you draw ideas—just to set the scene. I am also very interested in the agenda of your association in terms of registrars rights and responsibilities, how you see it going, whether the prevention of cybercrime is a priority and, if so, how? I know that is a very big question.

Dr Brooks—The Internet Society of Australia is a chapter of the global Internet Society and the global Internet Society is a body that was set up by interested users of the internet. Generally, it was set up right from the beginning with the guys who actually built the internet in the first place. The group that was developing the standards, guidelines and protocols back at the very beginning and effectively started the body of internet standards documents called RFCs, requests for comments, comprise the engineers who design and build the internet. That group is effectively running with the Internet Society as the corporate body that provides the legal framework for the funding of that work, and that happens on a global basis. The Internet Society of Australia is one chapter of that global society and frequently we get the global ISOC people to come to Australia to address us and talk about the things that we do. We contribute papers and the Australian experience to the global ISOC, which can then be used to disseminate it worldwide.

As the legal body that effectively looks after and funds that standards development, the Internet Engineering Task Force, IETF, which I think was an acronym that came up yesterday, does not actually exist as a body at all. It is shorthand for all of the interested engineers and people who use the internet and who get together at regular meetings to talk about the development of new standards, guidelines and protocols for the advancement of the internet. One of the odd things about the internet is that there is no central coordinating body; it is effectively a cooperative that works on self-interest. If you do not use the same protocols and standards that everybody else uses then you cannot communicate with everybody else. It is in everybody's best interests to use the same protocols and standards, to adhere to the best practice guidelines that are published by the group that are effectively self-elected to decide on such things so that everybody works together to keep the internet running and to progress the development of internet protocols and standards.

CHAIR—How is the membership of ISOC determined? Do people just join? How does it happen?

Dr Brooks—Yes, people just join. Any interested user can join. The Internet Society of Australia effectively represents the users of the internet, whether they are corporate, home, personal or business users—anybody that uses the internet. Our brief as representatives of those bodies is to help advise. In many cases our members are experts in the use of the internet or, in my case, engineers who build parts of the internet for ISPs. Many of them are just interested users such as grandmothers and grandfathers who communicate with their kids over Skype or videoconferencing at home and are interested in seeing the interests of the users of the internet furthered as opposed to the commercial interests of the people that run the internet.

Mr BILLSON—If it is as organic as you describe, and I think we appreciate it is quite organic in an ARE, an acronym rich environment—

Dr Brooks—There are plenty of TLAs!

Mr BILLSON—Thank you. We like the TLAs in an ARE!

Dr Brooks—I try to stay away from them except when I am addressing a room full of people who I know understand them.

CHAIR—I think we are going to ban them!

Mr BILLSON—That is all okay for me. We are on WiCAM rather than ‘I can’, ‘you can’ and all that stuff! We saw digital DVD technology play out with Blu-ray arm-wrestling HD DVD. The technical platform became highly commercially motivated. It was about who got which group onside—the movie houses and all that sort of stuff. How does that proprietary arm-wrestle over technical specifications play out in such an organic space, or is it a critical mass way of resolving things?

Dr Brooks—It is essentially a critical mass argument. The development of the technical standards for how computers communicate over the internet and the underlying protocols right from the very beginning were based on a fundamental principle of rough consensus and running code. So a group of interested people that want to develop a new capability can get together and do so. Certainly sometimes there are multiple bodies that come up with competing ways of achieving the same result. But at the end of the day the one that wins is the one that gathers the most deployed base.

Mr BILLSON—So it is the modern-day equivalent of ‘possession is four-fifths of the law’. If you get the traffic and the support for your platform, that will give it—

Dr Brooks—In a sense it is a critical mass environment. There is not really ownership, because the protocols are all publicly available and open source. The work that people do in developing new capabilities is published free and open. There is no ownership of a particular protocol or that side of things. There is no reason why multiple capabilities cannot operate simultaneously. For voice over IP applications on the internet we have Skype using something different from someone else, but it all achieves the same result.

Mr BILLSON—There is a lot of discussion about the National Broadband Network and the symmetrical functionality it offers and the ever hungrier applications and code that will run over it. Prioritisation of packets of certain data is a real commercial possibility. Where consumers leave it essentially to a faceless crowd of very committed individuals with an organic governance and engagement structure to sort out what traffic takes priority within a piece of infrastructure, how do you sort those things out?

Ms Raiche—Can I talk to Comcast’s decision, and then you can tell how you have done it?

Dr Brooks—All right.

Ms Raiche—There is an important FCC decision on Comcast that unfortunately has been wrongly characterised in some discussions. In discussions about net neutrality, what the FCC said was it is okay to manage traffic in a differential way. That is, voice packets can take priority over data packets, which can take priority over peer-to-peer traffic. That is not a competition problem as long as you say, ‘This is the way we will prioritise our handling of packets,’ and you do it in a non-discriminatory way—that is, you do not favour X’s packets over Y’s packets and Y’s packets over Z’s packets.

Mr BILLSON—So packet type is okay but client preferencing is not.

Ms Raiche—Yes. Whoever sends the packet is not a basis for discrimination. Type of packet is okay, as long as you say, 'This is what we're going to do: you pay the price; we handle the traffic accordingly.' That was the FCC's definition of net neutrality.

Mr BILLSON—So it is about transparency, nondiscrimination between clients and commercial prioritisation. Commodification of traffic is being left behind and we are now seeing different—

Dr Brooks—That is right. It is an absolutely essential part of the development of the internet so that applications such as streaming voice, streaming audio and streaming video work properly. It has certainly been an accepted practice to run networks to prioritise some types of traffic over others, generally ISP—

Mr BILLSON—And to price them.

Dr Brooks—They are all priced the same. In the current environment price is not an issue. It is more about the performance of the application and how the network can know which packets need to be queued ahead of others, and generally the way that has happened in a traffic engineering sense is that the level of that amount of traffic is deliberately kept fairly low in the total proportion of traffic so that it does not unduly starve other types.

Mr BILLSON—So where is your voice in all of that?

Dr Brooks—Our view on that is that prioritisation of types of traffic is fine but prioritisation of traffic from a particular provider over another type of provider is effectively covered under anticompetitive conduct.

CHAIR—Do you mean content provider or ISP?

Ms Raiche—If we are talking about where the packet comes from—say it comes from Optus as opposed to Telstra as opposed to AAPT—and you are discriminating on the basis that it is coming from AAPT that is discriminatory conduct. It would be anticompetitive. If you are saying the packets that are coming from Optus are voice and therefore because they are characterised in a particular way they are carried and voice packets get priority over data or over peer-to-peer—

Mr BILLSON—But equally, regardless of where they came from.

Ms Raiche—But equally, regardless of where they came from, that is fine. That is in the FCC's decision.

Mr BILLSON—I was trying to tease out the chair's question about how your organisation interplays its view and input and then bring it back to security.

Ms Raiche—There are lots of ways.

Dr Brooks—We coordinate our members’ views when we are putting together papers such as submissions to areas like this. We coordinate the members that have a desire and the capability to do so to participate in industry working groups

CHAIR—How many members do you have?

Ms Raiche—It is hard to count because we have large corporates like Google and Cisco on the one hand, small organisations that represent a lot of other people and then individuals, so there could be 120 names on my list.

CHAIR—Yes, it is probably more how many organisations than how many individuals.

Dr Brooks—It could be 100 or 200 organisations and how many thousand individuals? You have the membership list.

Ms Raiche—I know. I would be tempted to say something like thousands

CHAIR—Do tiy send out notices by email?

Dr Brooks—Yes.

Ms Raiche—We do not deal in paper.

Mr BILLSON—So you are essentially a clearing house not only for individual views but also for other groupings within your audience.

Dr Brooks—Absolutely. A large part of our function is also to take what is happening on a global basis in other chapters around the world and what is coming through the global internet society, and the bodies that they are coordinating with that participate in ICANN and all those things and distribute that information to members.

Ms Raiche—Because we are seen as one of the outstanding chapters in ISOC. We interact with government, make submissions and interact with other consumer and user bodies. But I want to get back to the chair’s question about the RAAs. RAA stands for registrar accreditation agreement and it is that document which is the contract between ICANN and the registrars.

CHAIR—Which is being revised at the moment.

Ms Raiche—It has been revised and ALAC, the At-Large Advisory Committee, is the consumer body.

Dr Brooks—Which is what we participate in.

Ms Raiche—Yes, in fact our treasurer is chair of the whole thing. It is developing what are called registrar’s rights. A lot of that is simply going to be that registrars ought to be told when their domain name is going to expire and those sorts of things. But I personally and our treasurer hope that we can build into that some requirements on the registrars to behave in a safer way. When I say safer I mean a way that provides more security. A very small example but one that will make a difference is in the Australian domain names administration. If you want to be a .com.au, you have to rock up with an ABN which proves that you are not only an individual but that you are also a company. To get a .com you just have to produce a credit card number and name.

I was advised at an ICANN meeting in Mexico by one of the people in the safety and security advisory committees that if you simply required somebody to put the three-digit number that is on the other side of your credit card into an automatic database you would reduce a lot of fraud. It would mean you could not have stolen the details about a name and a credit card and what is on the face of it. You would have to have the physical card and turn it over to know that number. It would reduce a lot of the fraudulent signing up for a dotcom name, because the dotcom fraud statistics are frightening.

Mr BILLSON—Yesterday we asked the banking industry whether there is some cross-fertilisation of their data about stolen credit cards with the registrars, and the extent to which registrars may be deregistered, and, if there are serial offenders using stolen credit card information, whether that could perhaps be grounds for someone having a look at them. In this additional rights thing that is being worked on—it sounds a bit like a franchise agreement with a few things attached to it—how far can, as you described, Ms Raiche, responsibilities be placed on the registrars?

Ms Raiche—I am about to find out—I am going to try. Until now there has been a lack of focus on the role that registrars can play. Given the amendments to the registrar accreditation agreement, it is a very recent development. It is a beginning to say there are things that registrars can do, both to help the actual individual registrant and to improve security. It is fairly recent and I am trying to push the envelope to say, ‘Let’s get some very interesting things in here.’ We also want to talk about the ISP code. That is very important.

Dr Brooks—With the ISP code in Australia, one of the things that we are very focused on, as representing the individuals and the users of the internet, is that currently there does not seem to be an easy or well-known way of someone reporting a cybercrime in general, whether it is to do with domain names or whatever—and I think we have seen that in some of the other submissions to this inquiry. People know how to report a normal sort of crime. If their handbag has been lost or been stolen, they turn up at the local police station, and the people in the police station know how to process that sort of complaint, but we do not seem to have either of those things in the area of cybercrime or in electronic crime. People who are the victims of some sort of cybercrime do not know how or where to report it. If they do front up to their local police station or ring—presumably, it will not be 000—some authority who they think should be able to take an investigation to the next step, in many cases they have no idea how to handle that either.

Interestingly, when reading through some of the other submissions to this inquiry from individual users outlining their experiences, when they tried to report something and tried to get on to a hotline to the Federal Police and the high tech crime commission, they were only answering the phone between nine and five. These sorts of experiences, certainly in Australia, are something that are national in scope rather than being international in scope. They are things that we in this country can fix. So working on improving both the methods for reporting cybercrime by general members of the population and improving the ability of the authorities that actually can do something about it—

Mr BILLSON—This is this front-of-house discussion.

Dr Brooks—Some sort of front house—

Mr BILLSON—Holly read yesterday where the solution might be 13EHARM or something that at least gets you somewhere, where people can be directed to responsible agencies.

Dr Brooks—Absolutely. It seems a little bit contradictory but a method that does not necessarily rely on the internet for reporting. It is all very fine to report cybercrime by email but if the cybercrime that has happened is that your ISP account has been stolen then you do not have email to do that, so you would have to fall back on conventional telephone numbers.

CHAIR—You can do it through an online complaints system though.

Dr Brooks—For spam, you can.

CHAIR—No, I do not mean that there is a capacity to do it now. I mean that, rather than send an email, a lot of organisations, particularly government, is online—

Dr Brooks—A webpage, yes.

CHAIR—where you actually fill in particular criteria.

Dr Brooks—One of the issues we focus on very heavily is accessibility for people with disabilities—we help people who are blind or deaf use the internet. Many users of the internet have no idea how the internet works—and neither should they. Many do not know what a web browser is. Some people think the internet is MSN, because that is what they use for communicating with their kids. I have met people who use the internet on a daily basis but do not have email. They use a particular application and call that the 'internet' because that is what they use.

It would not be right to rely on just one method of reporting. There would need to be several because different members of the community understand different things when you say 'internet' and they use different programs and different applications. Some may be comfortable with email and some do not know what email is—they use instant messaging and think that that is the internet. Some use a web browser and think that is the internet and they get their email through the web browser and that is how they access the internet. One of the beauties of the internet is that it enables so many different forms of communication. A clearinghouse for reporting issues needs to accept input using many different forms of communication to allow for the preferences and the comfort levels of different members of the population in using different communication methods.

Ms Raiche—I have one more thing. It was mentioned yesterday—and it helps to add to what we do—that the Internet Industry Association has developed a code, which Alana was very supportive of. The aim of that is for the ISPs to, if they do not already, monitor the traffic to determine if a computer has been compromised. Remember that she basically said you do not need depacket inspection to do that. If there is a whole lot of bot farming, you can start to cut off a range of bots just because you have spotted them. This would be a very significant thing. It is a voluntary code. Comments are due by 30 October, so write in and say, ‘Do it.’

CHAIR—There seems to be fairly general agreement that, if an ISP is monitoring traffic and sees suspicious traffic that may indicate that a computer has become a botnet, it should communicate with the consumer first and assist them at least by giving them information to fix it and that cutting off the server should only be the last resort if there is either no response or inaction. Is that a proposition that ISOC-AU support?

Ms Raiche—Yes, that is exactly what is in the code.

CHAIR—The code?

Ms Raiche—The draft code that has been released for public comment that is on the IIA website. The first thing you do is tell the customer and tell them what to do about it. You should assist the customer by saying that they should do certain things. In the case where there seems to be a huge attack—denial of service or something—then there is a recommendation that it be reported to AusCERT or the federal High Tech Crime Centre. The emphasis is on first going to the customer and trying to fix it.

An interesting case came up in the discussions and the development of that. An unnamed provider did that with a customer, who was very cooperative and said, ‘I will take the steps,’ and took those steps. But there was still a traffic pattern that suggested it was a bot. They took further steps and it still was not corrected. They went back to ACMA’s new Australian internet assurance initiative—and I hope you have been told about that. ACMA has set up a way to monitor traffic and let ISPs know when there is suspicious traffic. The suggestion was made that it might be that that person is on a wireless connection and somebody else’s computer is compromised. I had not even thought of that, but that is an issue that may arise.

Dr Brooks—There is a trade-off in this because most ISPs in this industry are fairly cash strapped. It is a very low-margin business. A very small number of ISP staff are supporting thousands, tens of thousands or hundreds of thousands of customers. There is a limit in practice to the resources that an ISP can put into helping an individual user through the complex steps of virus checking all of the PCs and machines in their house. We now have a situation where there is not just one computer connected to a broadband connection; there is a computer, a laptop, the kids’ computer, the TV and a DVD player—and all these things could potentially be an issue. There are ways that an ISP can address some aspects of their computer being taken over.

Certainly best practice guidelines that have been around for a long time suggest an ISP limit the rate at which a customer can send out emails. Most normal customers will not send out more than 10 emails in 20 seconds. Anything that is trying to send out more than 10 emails in 20 seconds is probably sending spam. There are ways that an ISP can automatically set up rate limits in a computer that do not require human intervention that allow—

CHAIR—It triggers an alert.

Dr Brooks—In either triggers an alert or just does not allow that 11th email in 20 seconds. It acts as a rate limit, and most people are completely unaware of it if they are doing normal traffic patterns, but someone who exceeds a fairly ridiculous threshold is effectively blocked automatically and then that encourages someone who is sending spam to go to another provider. If you can get everybody doing that then they will move offshore. But that only addresses email sending and spam; it does not address hacking attempts, phishing attempts and people who are inadvertently members of a botnet because their computer has been compromised.

CHAIR—We received evidence in earlier hearings that the largest threats these days are not so much spam, though spam is still a constant problem—

Dr Brooks—It is annoying.

CHAIR—People are quite alert to the problem. The biggest threat is spoofing, which is fake domain names and sites where people go and inadvertently compromise themselves by accessing it—

Dr Brooks—Effectively, yes, that is right.

CHAIR—Or real sites that have embedded malware. You are on a real site but a section of it—

Dr Brooks—Yes, but it turns out that the administrator of that site somehow allowed it to be insecure and so people injected malware onto the main site, unbeknownst to the operators of the banking site et cetera. I think the Sydney Opera House website was one a year or so back. So normal people accessing what they think is a legitimate domain—and most of the content on that does come from a legitimate source—inadvertently download something that the owners of the site did not even know was there.

Ms Raiche—If you remember when the black list was released and should not have been and there was all that kerfuffle, there was a dentist on the list. The dentist asked why his site was on the list. It was because his domain name had been hijacked and all the traffic was going offshore to a Russian pornographic site, and he said, ‘Excuse me.’

CHAIR—Do you support the code?

Ms Raiche—Yes, having helped draft it.

CHAIR—But you do not always—

Ms Raiche—Yes, I know.

CHAIR—Are there bits in it that you do not agree with? Are there bits that you think should be in it but are not?

Ms Raiche—I will probably get killed for saying this—

CHAIR—It is okay; we will not kill you. It is fine.

Dr Brooks—Not in this room!

Mr BILLSON—Mind you, the hearing is being broadcast.

Dr Brooks—That is right.

Ms Raiche—I would hope that eventually the code is not voluntary. It is so important that we do everything we can to protect our citizens. I understand that this is a cost impost and I understand that there are ISPs that are operating on the smell of an oily rag, but it seems to me that there ought to be some entry level requirements. I would hope that an entry level requirement is that you take steps—and not necessarily specific steps—within a reasonable framework with some reasonable options. You must monitor traffic in some way and you must do something about traffic that looks as if it is coming from a compromised computer.

Dr Brooks—It is one of those things that market forces probably do not help. In an environment where an ISP is acting in a responsible way, users get better performance for something through that ISP than somewhere else. You end up with a natural commercial market force. That ISP will gather more customers and ISPs that do not take those steps will wither away and die. This is a situation where the general user base will not see any difference at all whether or not the ISP is acting according to the code, so there normal market force concepts just will not apply. But we would certainly like to see ISPs able to assist their users. Users in general are not technically knowledgeable and may not have any idea that they have been compromised. They certainly are not doing it deliberately and should not be punished, in a way, for doing it, but the ISPs are the ones with the technical knowledge to identify that something is going awry and to help the customers work through it and eliminate it in some form or other.

That behaviour by the ISPs is really what the code is trying to encourage. They are accepting a fee for providing a commercial service so, in a sense, if they have the capability and the technical understanding to help their users when their users are in trouble—and the users may have no idea that they are in trouble—they could let them know that they should run a virus scan over their machines and disconnect it because something has gone horribly wrong. Maybe their kids have downloaded something; who knows? That would be a big help in cleaning up the internet and the effect that those infected users have on the rest of the internet population.

Mr BILLSON—You see the ISPs having a greater role to play. There is work going on with the registrars to make sure they are not just doling out domain names but have some responsibility attached to that that is not just administrative but is about the way the system operates. We heard yesterday, essentially, a ‘regulation doesn’t solve everything’ pitch, which I am very sympathetic to. The engineering fraternity is well placed—and unnaturally handsome, as is evidenced here!—

Dr Brooks—You are too kind!

Mr BILLSON—There are two prongs left. One is community education and awareness. We are seeing over and over again that there is a level of awareness but some indifference to do something about the awareness. Then there is the issue of what a legitimate and reasonable thing the government can do is. Can you talk about those last two prongs? I am particularly interested in whether you think there are gaps in the law that could support the work of those other stakeholders.

CHAIR—Think of the Australian Spam Act. There is a lively debate about whether it should be amended or not.

Ms Raiche—I first support what Paul Twomey said yesterday, which is, ‘Don’t think about security; think about resilience, because you are never going to build a wall that is high enough.’ It is always going to be a series of measures that will make things safer but never safe. I trust you have heard from ACMA, because some of the stuff they are doing in consumer education is actually quite interesting. For instance, they have a program where kids can talk online to detectives who can then say, ‘That behaviour is wrong; let’s work through what you should do.’ That is not a huge program, but it is an effective one. They are also working on programs to educate the parents, because most often parents do not know what is going on. They have programs for various age groups. So I would not say they are doing nothing. I think it is a matter of the reach of that. We participate in the e-security week that is run by the department, and that is just a range of strategies. That involved Harvey Norman and Dick Smith. It is getting out to the industry to say, ‘You want to put brochures there and start people thinking that when they are buying a computer they need to think about things.’

Mr BILLSON—There was an argument yesterday that if you are going to load an operating system you load some antivirus capability as part of it.

Ms Raiche—Talk to Microsoft about it.

Dr Brooks—The issue is that antivirus software can only protect against certain types of threats.

Mr BILLSON—It has a shelf life.

Dr Brooks—It can protect users against inadvertent downloading, but it is not going to protect the internet population from someone who is going out deliberately trying to attack and cause threats. It is part of the jigsaw but it is certainly not something that is going to create the whole thing. The reality is that in many cases these are social issues, not technological issues. Technology can only go so far in terms of helping to slow down inadvertent access and threats.

Mr BILLSON—The awareness stuff is important. It is spotty and in your explanation I think that you mentioned three different programs. There is ThinkUKnow and—

Ms Raiche—There is something else, and you have just jogged my memory. We run little meetings with groups of people. We were out in the Western Australian talking to the Senior Computers Association—and you are going to have Senior Computers Association this afternoon—

CHAIR—Yes.

Ms Raiche—There was a very interesting statement by some senior computer people. They are living on a pension and have a download limit that they can afford, and along comes a security patch and it takes their month’s download limit. Are they going to download it? No, because they want to download pictures of their kids. So you would have to say that it is rational behaviour on their part. It is also rational behaviour on the ISP’s part to say, ‘We need to put in download limits because costs are involved,’ but it winds up being one of those little holes that security goes through.

Mr BILLSON—You reckon that the security should be excluded from downloading—

Ms Raiche—We have not figured out what to do about it.

Dr Brooks—The software industry has come a long way in the last few years in terms of being able to almost rely on there being a real time communications channel. In the last five years or so we have seen a vast increase in the number of these software packages that automatically update themselves.

Mr BILLSON—I get stalked by Adodi—

Dr Brooks—Exactly. But it is a much better situation than in the old days when, if there were a problem with software, that got fixed by relying on the user identifying that maybe there had been an update, going and getting the update and having the resources to apply the update. We are in a vastly better situation than we were four or five years ago. But now we are in a situation where not everybody has a full-time connection to the internet, and arguably they are the ones that we are trying to protect. And while it is certainly not true that all software automatically updates itself, many do get automatic software updates these days.

Mr BILLSON—Yes, I am nervous. Some of it is spam.

Dr Brooks—That is right. But the issue that we have at the moment is that all of those automatic updates occupy space and there are people with download limits, and while it is a very good thing to have very cheap plans with very low download limits for those people that cannot afford anything more, you end up with this chicken-and-egg problem where people who are afraid that those security patches that fix the problems in the software might exceed their download limit end up more insecure than people that can afford a bigger limit.

Mr BILLSON—We have only got a couple of minutes and I was keen for you to come back to whether there is any legislative or regulatory effort that the Commonwealth needs to turn its mind to that would better support and give strength to a lot of the activity that we have had described to us that is going on outside government but where government action could be helpful and supportive.

Dr Brooks—We need to recognise that the internet is a commercial operation. ISPs are commercial organisations and users have, if you like, the responsibility for the safety of their own systems. The main area that we can see is certainly increased funding of programs for education so that people are aware of how to prevent attack or, if they have a problem, ways of reporting it so that it can be investigated. There also needs to be funding for authorities to be educated on how to handle problems like this. Things are going to happen regardless of what you put in place. You cannot prevent everything from happening. But ensuring that we have better mechanisms in place for reporting and investigating issues, and for resolving them, would be a huge step forward.

Mr BILLSON—And the cyber intelligence hub concept like the US National Cyber Forensics and Training Alliance—

Dr Brooks—That is certainly important. Because cyber crime is generally cross-border, institutes in some countries, that are well funded, have their research disseminated on a worldwide basis so you do not necessarily need every country duplicating that type of research. It also tends to be long term in nature. Organisations like that are interested in doing research on identifying long-term trends and things like that, which is all very fine and well but does not have the ability to respond within minutes to an actual attack happening at a particular point in time. When somebody notices that their equipment, their ISP or their home PC has been hacked, it requires different tools, a different level of investigative ability and a different organisational structure for them to be able to pick up the phone and get on a hotline to somebody who can within minutes identify what is going on and try to track that back in real time to where it is coming from so you can actually catch the guys that are doing it. That institute is not going to do that.

CHAIR—Where does that operate?

Dr Brooks—We do not have anything like that at the moment.

CHAIR—But does it operate anywhere?

Mr BILLSON—Is there a model that you could guide us to?

Ms Raiche—Part of that was starting to be talked about in the last e-awareness week. There was a focus not so much on cybercrime but on a place people can go.

CHAIR—We have discussed such a central point quite a lot.

Dr Brooks—The internet community can track things down fairly quickly once it is aware of it. Currently we have a situation where things like not so much take-down notices but police warrants for interception and those sorts of things do get action very quickly through the ISP community. If an ISP notices that it is being attacked in some way through a denial of service attack, it can get in contact with the next network up the chain very quickly, who can quickly look at the traffic, identify where it is coming from and track that through. What is missing is that step to get the problem report from a general member of the population into that action chain of the ISPs and the networks that the traffic is flowing through so that the source can be tracked back and something can be done about it rapidly. That is a part of the puzzle that seems to be missing. Once an ISP has a problem report that it can look into in its part of the network and see what is going on and identify where it is coming from then that part of the tracking down process can happen and does happen very quickly.

CHAIR—We very much appreciate your time. It was very informative.

[10.18 am]

GALLIGAN, Mr John William, Director, Corporate Affairs, Microsoft Pty Ltd

STRATHDEE, Mr Stuart, Manager, Security Program, Microsoft Pty Ltd

WATSON, Mr Peter, Manager, Platform Strategy, Microsoft Pty Ltd

CHAIR—Welcome. 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. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Would any or all of you like to make an opening statement?

Mr Galligan—I will put a couple of more formal points on the record and then opening up for discussion, if that pleases the committee. We represent three very different parts of Microsoft here today but we do share a fairly common objective, and that is to make sure that we provide for our consumers, our customers and the general community a safe and secure digital environment around which to work, play, live and do whatever they want in this connected world. This is part of Microsoft's global commitment to what we call 'trustworthy computing'; a long-term strategy about building our software with security in design, by default and then also in deployment.

I suppose I do not need to remind the committee of the massive advances over the last 30 years in terms of computing. Microsoft has probably been at the heart of many of those, so our experience is rich, and at times we have probably also been at the brutal end of that as well. This is all the more reason why our commitment to make sure we provide digital confidence in the community is so important. As rapid advances in software, IT services and communication have really enabled so many traditionally separated and disparate systems to come together, they not only provide a great connectivity but also the vector for malfeasance and criminality.

While everything from our leisure and commerce to the way we are going to educate our children has become so much more sophisticated and used to connectivity, we really see that the internet now is a great place to create crime. There are four key principles around which we think the internet becomes that incredibly attractive place for criminality: firstly, it is globally connected, and getting even more so; secondly, it is relatively anonymous, as the witnesses before testified; thirdly, there is a relative lack of traceability and, finally, there are rich targets, be they financial information, personally identifiable information for consumers, military information or business information.

What makes this scenario even more daunting is that global connectivity is going to grow. The advent of the National Broadband Network here in Australia is not only going to spark a new array of communication and access, it will usher in the digital economy that we have been talking about for so long, where government, business and citizens across the country will have access anywhere and be connected to an ever-increasing array of sophisticated connected devices. Indeed, we submit that the NBN is not so much an infrastructure and communication investment but a major social and economic shift for the nation. And as important as the physical rollout and deployment will be, the NBN requires a whole-of-community change management focus to ensure that we empower citizens to be digital ready for the changes to come. With broadband to become the dominant platform on which we transact our lives, the role for government policy, industry collaboration and community education could not be more important in building security, safety and trust into the design of the network. The NBN will change the way we live, work and play, and if Microsoft's vision for cloud computing is any guide there will be more rich targets online as more and more people do more and more things in the cloud.

So if local, national and global connectivity is going to continue to grow along with more rich targets, what are we going to do about cybercrime? It is in that spirit that we present ourselves to the committee today. We have four areas that we would like the committee to focus on. They are in our submission, but we will repeat those for the purposes of today. We believe that there needs to be a comprehensive national strategy around cybercrime as well as greater government-to-government collaboration on cross-jurisdictional issues. So, too, we need to better understand the threat landscape and to evolve and focus the public-private partnership model, as well as international collaboration. Further, we should consider a legislative model designed to ensure that greater regulation, if enacted, does not necessarily occlude providing the oversight for innovation and other cybersecurity issues. Finally, we need to ensure that the internet provides an appropriately deployed identity metasystem to ensure not only confidence in the network but also to provide the opportunity for free speech and expression.

We are pleased to assist the committee today in its inquiry into cybercrime and its impact on consumers. If I can help direct the flow of questions and discussions across the three of us; Stuart Strathdee, our Security Program Manager, is really the expert in the threat landscape and the technical issues regarding cybersecurity. Peter Watson is the Manager of Platform Strategy, and probably best placed to talk about the future security trends with cloud computing and the impact on the National Broadband Network. If you care to ask a question around me, I look more at our end-to-end broad policy initiatives—our issues around privacy—and our community investments around education and how we become better corporate citizens with respect to our investments in subsecurity. I thank the committee for allowing us to present today and we are pleased to hear any questions or comments that you have for Microsoft.

CHAIR—To start off, I just want to say that I am very pleased that you are here. I would hazard a guess that Microsoft has more contact with more internet users than any other corporation in the world. So I would be very surprised if Microsoft is not identifying new trends. We are very hopeful that by having you here today as representatives of Microsoft we can pick your brains. You can give us an indication of not only what things government can do but things that we can put into our recommendations to suggest that third parties do, which obviously is not binding on them but can be helpful. We see this very much as an opportunity to change the structure of the security of the internet. With the NBN coming, we as a government—and I am not speaking on behalf of Mr Billson here—think it is really important that we have our security infrastructure right. As a committee we see these hearings as a great opportunity to try and add to that debate and move it along a bit further than it has gone so far. I would really appreciate a bit more elucidation on the internet metasystem.

Mr Galligan—Absolutely. I would like to table at some stage a paper by our global chief security adviser, Scott Charney, on establishing end-to-end trust. That provides a very readable and comprehensive understanding of some of the issues, if time does not allow us to get into it in detail now.

CHAIR—I would not mind just a rough outline of what it means. We are happy to receive that as well.

Mr Watson—I might respond in two parts. Firstly, you mentioned Microsoft having a good understanding of trends and activities that we are seeing across the internet. We definitely think that we do. One of the things that we have done, both globally and in Australia, is to put a number of programs in place where we share a lot of our insight and our information with government agencies.

CHAIR—Who do you interface with?

Mr Watson—We have a number of programs. One of the programs is the SCP, which is our Security Cooperation Program. That is an agreement that we executed with the federal Attorney-General's Department and the Department of Defence. The Defence Signals Directorate is the actual executor of that. That allows us to provide a lot of the information we have on threats and trends around security vulnerabilities. We provide that information to DSD. Then, through their portal, they share that information with all federal, state and territory organisations. We put in place the agreement with the federal Attorney-General's Department to do that.

We also have another program, called GSP, which is our Global Security Program. Again, we execute that with the Department of Defence, through the Defence Signals Directorate. It allows them to access our source code to do analysis, when they are looking at security from a critical infrastructure and national infrastructure protection point of view, to understand to what some of the capabilities in Microsoft products are and how they can leverage that.

From the education point of view, we have also established a program with the Australian Federal Police and ACMA called ThinkUKnow. We have volunteers from Microsoft staff working with law enforcement officers who go out and talk to parents and teachers about how they can stay safe online and how their kids can have a safe experience. One of the key components that Microsoft saw that we could bring to the table there was our knowledge of what parents need to do to have a safe online experience and what they need to be looking for with their kids.

CHAIR—Can I take you back to the internet metasystem. I think it is something no-one else has mentioned before, which is why I am particularly picking on that.

Mr Watson—Microsoft thinks that for the internet to move forward there needs to be end-to-end trust. How do you create this trusted ecosystem? If you look at the physical world, most people have multiple personas or different identities in terms of how they relate to somebody. When I buy a train ticket I really have an anonymous identity. I am just doing a financial transaction. If I am buying an airline ticket, I might be presenting credentials in relation to the frequent flyer program that I am dealing with. But when I go to see my doctor or see my tax accountant I am using a higher level of identity and giving more specific details about who I am.

In terms of the direction that the internet needs to move to, our view is that it needs to create this identity metasystem. We do not view that the solution will be to create one mega database where all identity characteristics for individuals are actually held. It is really a case of using a fitness-for-purpose model, that you create a metasystem where, as a user, I use and present the right level of credentials at the right point in time. As the previous representatives talked about, presenting an ABN number to get a domain name is the right piece of information to be presenting. If I want to get information in terms of providing my tax files online I should provide my tax file number. If I am talking to my doctor online, obviously I will provide my Medicare number. So the question is: how do you create that metasystem where you are presenting the right pieces of information and the right credentials at the right point in time? We believe that that presents advantages. It delivers two things.

Firstly, it still maintains a level of privacy for the individuals because I am not providing unnecessary information. If I am signing up to buy music, why should I be providing information as to where I live or what my home phone number is? The person whom I am buying music from online does not need to know that information. We believe the identity metasystem can provide that level of privacy protection.

Secondly, we believe it will still allow for anonymity of the internet. There are certain situations where people still want to be anonymous. If I am going to browse for products online, again, I do not want to be giving my personal details. It is really a case of ‘fitness for purpose’ by looking at what identity and what level of credentials should you be presenting at the right point in time.

CHAIR—How do you implement that? Is it just a protocol? How does it work?

Mr Watson—This is where the government’s policy around the NBN provides a lot of opportunity in this space to move Australia towards this. It is a case of working with the right players in the right ecosystems or industry sectors. If you take health, education, transport, sustainability or the environment there are various organisations, even in the financial services sector, which have a role to play. If we take health, for example, NEHTA has a role to play in that they are a trusted source for issuing identifiers for medical practitioners. There is a role for government to play there not only in working with those entities but also working with the industry associations to ask: ‘Who should be playing the right role in terms of doing that in-person proofing and the issuing of that identity?’ Also, they also need to create that broader model and to ask: ‘Who are the other players that can leverage that information and use it?’ That creates a lot of flow-on benefits in terms of the regulations that you can put in place and the agencies can then come into play in doing the validation of the activity that is actually occurring.

Mr Galligan—I think Peter’s comment on the word ‘ecosystem’ is a good one, because it will require both the community to be aware of how to use this new credential and this new identity network—someone to be the trusted model to provide it and then of course the pipes or the network around which it will be provided to ensure there is a security layer there to ensure it is not abused or compromised in any way.

Mr BILLSON—So you would broadband categories of engagement with the technology, engage the stakeholders and say, ‘In this health space, this is a legitimate authentication level?’

Mr Watson—Absolutely. When most people draw the internet, it gets drawn as a cloud—pipes going in and then there is this big, ubiquitous cloud which is a place where everything happens. What we really see is an opportunity to actually segment and create miniclouds, to say, ‘You can look at an ecosystem and you can take health, financial sector, transport, education and say that we know who all the key players are, so let us create a model and ask what are the roles of those players?’ Who is actually issuing the identity? Yesterday I noted that a person made a representation to the committee about whether or not they would use Windows for their internet banking.

One of the issues is regardless of what technology you use you are always going to be exposed to risk. The more important issue is how I trust the parties I am dealing with. If you want to know which are trusted organisations and which have been issued a validated identity in Australia that you can do financial transactions with, there is a role for APRA to play. As a citizen, I can go to a trusted body and then make a decision because I am getting information that is telling me the right thing.

In the area of education, as a parent, could I go to an education department or a federal government agency which focuses on education and which says, ‘Here are known trusted sites we know of that have good information and quality resources for kids and students to be using’? How do you define those ecosystems? How do you subset what, at the moment, is the Wild West of the internet? How do you start breaking them down into trusted ecosystems? What is the context and what is the function being performed?

CHAIR—I am very interested in the issue of cloud storage. My husband bought a computer this week and along with it came two gigabytes of cloud storage. We have not set it up yet, but it has occurred to me that, normally, if you have got storage on your computer or on your network, you can check it and make sure it is secure. If it is out there somewhere, how do you know it is secure? How do you check it?

Mr Watson—I think this comes back to the ecosystem model. One of the advantages of cloud is that it does provide this ability to access it anywhere. The reason why people are looking to leverage cloud storage is a lot of people nowadays have multiple devices. I have my computer at work, I have my computer at home and I might have my mobile device. I might have pictures of my holidays that I want to show my work colleagues, I want to be able to manage them when I am sitting on my home PC or I might want to show the person who is sitting next to me on the train. Having cloud storage provides a lot of benefit to me.

Again, if you have no level of insurance or understanding from that provider or also, potentially, from another party in terms of where that information is going or how it is going to be handled, you really come back to what was probably the right model in the physical world: buyer beware. In the online world that is not a good model to have. Do I have the ability to make those trust decisions around how to take this information from someone who is saying, ‘I have this cloud storage offering,’ and how to make some informed decision from a reputation point of view? Do I look at the hundred other people who have all put notices there to say, ‘Yeah, I had a really good experience with this’? Is that telling me it is safe or is that just telling me that another hundred people used it? Is there somebody I could go to? Is there an internet body or a government agency that I could go to who will say, ‘Here is something we know; we have looked at this. If you have requirements around storing your medical records or storing your personal details, we believe these organisations have met the right criteria so they are the right ones'?

Again, it is not saying we want to restrict what can go on but it is giving people that level of choice to make an informed decision. I can say, 'These ones, I know there has been some validation and a level of checking that has been done.' I am then making that choice for a reason, whether it is financial or otherwise.

Mr Galligan—It is going to be about user choice and user design. Take health, for instance: the concern a lot of people have about every health record being up there and accessible for all and sundry is probably a valid concern if that is the way the network is set up. If you have a permission based opt-in system that allows for only this particular doctor to see this particular medical record then if they are an obstetrician they might not need to know everything about your other health issues but they may need to know a particular set of medical information and can access that information. If the user is given control of that then the trust is not where it is stored but who can get access to it, because security will become more and more sophisticated to ensure there will not be rogue access to that information. The convenience of someone having that data being fluid through their life choices—be it what doctor they use, what hospital they use or any other issue they might need—is a trade-off. Hopefully, the security of the network is strong enough and becomes permission based in terms of who I want to give access to that information.

Ms REA—I am curious to pursue this a little bit more. It sounds like an interesting idea, but I am just trying to work out in my head how it would actually operate. You are talking about different levels of security according to the nature of the transaction, so I am interested to know first of all who makes that decision. Who makes the decision that buying a train ticket is less of a security problem than accessing your medical records? Who determines the level of security? It sounds to me like you are talking about some sort of central body or agency. Can you outline it a little bit more?

Mr Watson—Absolutely. Firstly, we do not see that you would have one central body or agency, because I suppose our view is that it is really about fitness for purpose. Different ecosystems will have different bodies and different players in them. To give you an example, one of the things that is occurring in education at the moment is that we have done a lot of work around how we promote child safety and how we make kids have a safer online experience. If we look at it, one of the things we see is that schools already do in-person proofing of students. When a student rocks up to school, the schools actually validate whether they are little Johnny or little Mary and whether they are eight or ten years old. With the rollout of the netbooks that is occurring across all the education departments and also with email accounts, most schools are giving students an online identity. They are actually giving them an ID when they say, 'Here is your email account' or 'Here is your device.' That provides the ability for online operators such as Microsoft, through our live platform, to distinguish between who is a child and who is not a child. We are not saying we want our 10-year-old daughters to come to the Microsoft site and say: 'This is who I am. Here are all my personal details—my age, my actual name and my address.' They should be able to say, 'I am a ten-year-old child,' because that is all we want to know.

Ms REA—And then you can validate that through the education system that says, ‘Yes, this child is actually part of this.’

Mr Watson—This electronic identity is coming to our site and purporting to be a ten-year-old child. Can the education department confirm or deny that they are? We do not need to know anything more. We do not need to know what their name is, what their address details are, or what school they actually go to. If we can validate that it is a 10-year-old child, that allows us to then create a safe environment. We can set up an environment where, unless we can validate that you are a 10-year-old child, you cannot come into this area. Adults can still then go to other online properties that we own, but we can create a secure area. It could be a secure area for Hotmail where only 10-year-olds can talk to each other. Straight away, you have removed a whole section of the population.

You can apply that model to the health scenario. If I want to go and start looking at health information because I am not feeling well—I might have a pain in my stomach and I want to gather more information—I can present my credentials to say I want to talk to a doctor. To get some initial information, I may just want to know if that person is actually a doctor. Have they been issued with the appropriate credentials from a government body to say, ‘Yes, this is a doctor and we have issued them an online certificate that says they are a doctor’? I can start engaging with them because all of a sudden my level of trust has just increased. I have gone from public information when I was searching through the web about colds and flus, and now I have actually made contact with somebody who is purporting to be a doctor, but I have the ability to validate that. If I then want to take it to the next step, the doctor may say, ‘Before I can engage with you and prescribe anything, I need to validate that you are really Peter Watson.’ Therefore, I need to present a credential. It may be my Medicare identifier that proves who I am. Then you have created that trusted relationship and we can start interacting. So it is built up in layers.

Ms REA—To pursue that a little bit further, there are two questions in my mind, and in fact I was going to ask you this question anyway. We have heard in previous hearings that there seems to be an accepted view that the ability to hack is almost overcoming every security system and that as soon as we create a security system of some kind the hackers or those who are out there engaged in criminal activity find a way around it. With reference to the three-number security code on the back of your credit card, that is fine for showing the card, but many things that you purchase online now ask for that security code. Once you put any form of ID into the system to validate your legitimacy, is there not an ability if your computer is compromised for that identity to be stolen or for that security to be hacked into?

Mr Strathdee—There are two things. In the identity metasystem that Peter was just discussing there is also the capability to revoke certain credentials. Unlike the physical world, where if you provide someone with your driver’s licence or your passport you cannot take that back—once they have that information they can redistribute it—with this identity metasystem, if that were hacked or distributed to a body that was misusing it there is capability to revoke that credential so it cannot be used any further.

Ms REA—And that can be identified? You can know that?

Mr Strathdee—Yes.

Ms REA—The biggest problem at the moment is that you do not know that your identity has been stolen.

CHAIR—How do you prevent that?

Mr Strathdee—There is auditing that is part of the system, so you will be able to see where it has been used, how it has been used and that sort of thing. The best way I can describe it is: think in terms of a revocable identity or a revocable credential in that particular instance.

Mr Watson—If we look at how technology has evolved and how security threats have evolved, Microsoft has done a lot of work in terms of building security capabilities into our operating system. Once we started doing that we found that people who were perpetrating these activities started moving on to spam, so one of the things we did is develop a technology called sender ID, which we built into our messaging platform, which was email and communication. Then we found things started moving to web based activities, so we started building phishing-filter capabilities into the browsers. I think it is an ever-evolving thing—how do you build them into the stack?

It is also about the identity piece and why we see that as key. We do not just see it as identity for the individual; it is also identity for the software. Currently, when I do my internet banking or when I engage with a government department I am presented with a website but there is no mechanism for me to validate if that is really the tax office website, if that is really the Centrelink website or if that is the federal government’s website, so what we are also saying is that this identity metasystem is not only for individuals but for the software as well. It is to say, ‘Do I get a digital certificate that comes from the federal government when I connect to their website and that says, “Here’s a certificate”?’ I can go validate that and say, ‘Yep; I know that’s a certificate from the Australian government.’

The third thing is, as Stuart touched on, that auditing process. If we go back to the scenario about creating safe online playgrounds for children, are there going to be instances where people are going to be able to get hold of those identities through suspicious means? Yes, that will still occur, but the reality is it is going to give you that ability. If I am a person who is a student using that site and I am being approached inappropriately, at least I now have the ability to say, ‘I know who was doing it: it was that identity over there.’ That allows the regulatory authorities to very quickly narrow their scope to say: ‘We can go to the schools and ask who issued that identity. Then we can go talk to the parties who are the owners of that identity to ask who had access to that identity.’ At the moment, you do not have that luxury. Law enforcement agencies are dealing with an identity on the internet but have no mechanism to validate who issued that identity or a mechanism to follow that up. That puts challenges in place that law enforcement agencies are having to develop technologies and mechanisms to deal with. That is still going to occur, but at least if you can take out what is known and trusted from the equation you are focusing on the unknown and untrusted. It does not make the threat go away but at least reduces the threat.

In terms of where I believe the government wants Australia to head with the NBN, it allows you to evolve the economy and those systems because you can create those trusted ecosystems, those clouds that are going to allow people to do increased activity because they will have a level of confidence and trust to do it. You are still going to have that area which is untrusted and unsecured, but that exists in cities today. There are parts of any major city where you have a higher level of trust or confidence, either because you live there or you work there, and if there is an area you have not gone into you know from other information you have gathered that after dark or at different times of the day it will be a less safe experience. If I am building an ecosystem of trust, it allows the consumer to make that choice.

Mr BILLSON—This idea is really about relationship risk management. The way you have characterised it as an identity metasystem, I can see how a user might think that is placing added responsibilities on the user, when really what you are saying is that it is the relationship—it is the other end of the relationship where you are calibrating the risk and therefore the disclosure of who you are. There is this 'be a friend to have a friend' kind of rapport being built, and then you can move on from there.

Mr Galligan—That is right. There are five layers plus the audit. We say there should be trusted devices to make sure you know you have got hardware and devices that are robust and have security built in. A trusted operating system is a very important part, obviously with a company like us. Trusted applications because, as we heard before, as you close one part of the balloon the air moves to the other side, so where there are applications it is about making sure they are trustworthy. Trusted people, which is about the relationship: do I know this person; do I trust this person? Lastly, there is the data: is the information trusted as well? Then all through that there is an audit trail to be able to see where there is a break in those trust models.

Mr BILLSON—So you are extending the current financial model where you can visit any website and check out what their interest rates may be on a mortgage, and you do not need to do much more than that; then you might want to check out whether you might get some preliminary green light to go further into debt and so on; but if you want to actually move money around there is a whole additional layer of verification and authentication of who you are and what you want to do and all that.

Mr Galligan—A level of anxiety, too, and as a consequence you might take a level of trust above printing out your boarding pass for Qantas. If you are moving funds between bank accounts, you build up the layer of trust: 'I am now at a different level of nervousness or I am going to require a little more trust in the network or the application or the data I am sending.' So there is always going to be a graduation: 'If I lose this data does it matter? If somebody gets this information does it matter?'

Mr BILLSON—The banks, with BPay and things like that, effectively do what you are describing for their site—that is, they will not have a bill-paying service on their site unless they can check out that the level of security they expect for their site is continued to the sites that they have set up some sort of relationship with.

Mr Watson—It is very much that relationship thing. It is building that electronic relationship model, but it is really applying context to it. One of the challenges with the internet at the moment is that it does not have context. Everything is: you are unknown, you are untrusted. I do not have the ability as a user to make an informed decision because I am not getting contextual information. Our recommendation to the committee is that the government moving forward is presented with a great opportunity with the NBN to not just roll out faster pipes on the ground but to actually build those ecosystem models; to say, ‘How do you create those contextual environments and do it based on an ecosystem model?’

Australia, being a continent, has a lot of advantages. There are requirements from a monetary point of view and the financial transactions I am going to do are likely to be an Australian dollars, so that means I know there is a group of bodies that can come into play in the financial sector. If I am dealing with health transactions there is a group of bodies physically located in Australia that I am going to deal with. If it is education, again, there is a bunch of physical bodies here; in transport, there are physical entities here. So all those organisations exist in Australia at the moment and they are performing those roles in most cases from a physical point of view.

I think the opportunity for the government is to work with those organisations and industry from an IT point of view in terms of how you now move that into the online world. How do you create those trust relationships, those contextual relationships, in an online world so that as a user I can then have that experience? I can say, ‘When I am doing my financial transactions, I now have a minicloud that I am dealing with and I know who are the trusted parties that I should be clicking on to get that contextual information: is this a valid website, is this a valid transaction?’ It would be the same for health, education, transport, the environment and the utility sector.

Ms REA—I want to get an understanding of how realistic this idea is. I think it is really interesting and I think there is a lot of merit in what you are saying, but I wonder how it would work in reality. For example, my husband and I and the kids have gone on an overseas trip twice now and we have booked all our accommodation online from Australia. Would the metasystem actually deal with that? It does not really worry me that I might lose the €100 deposit I paid, but if I land in Reykjavik and the house I have booked does not actually exist that is probably a bigger issue! So, realistically, how far can this system go?

The flip side of that, which has been going through my head, is: what sort of regulation would be required to stop monopolies? We have never had a bad experience, not once, and we have often dealt directly with owners, which is the cost advantage that you get from the internet. But what is to stop people setting up a quasimonopoly and saying, ‘We’ll validate you; you come with us and you’ll get more traffic,’ and actually excluding some legitimate people? I can understand that the financial, health, and education sectors—those key, well-regulated industries—can probably be managed, and I think it is a good idea, but is it realistic to extend it to all of the things that people now use the internet for? They do have high risks. As I said, $1,000 out of your bank account is bad; but you, your husband and three kids standing in the middle of a street in a country where you cannot even speak the language and do not know where to go is probably worse. Do you know what I mean?

Mr Watson—Yes, I do. I will answer the various parts of that. Firstly, in terms of how realistic it is, the technology actually exists today. Digital certificates—basically, encryption keys—have been around for quite a while, and the IT industry has been working out how you leverage them from an identity point of view. In terms of the identity metasystem, Microsoft has built into its platform a solution called CardSpace which allows people to select contextual identities, to get more of a graphic user experience rather than having a big encryption key with ‘do you trust the—

CHAIR—How do you do that?

Mr Watson—It is a two-way authentication process. We could go into it—

CHAIR—I will read the book!

Mr Watson—It is also worth noting that, while Microsoft has CardSpace, the open source community has developed OpenID, which is the same platform. So it is not unique to Microsoft; there is an industry solution.

In terms of how you roll that out, our view is that you do need to start with ecosystems that are probably better defined and more suited to it. That is the reason we have been mentioning health, education, transport and energy; they are areas that we see as fairly easy to pick off at the moment. How you then expand that in terms of international boundaries is going to be about how you get agreements across entities. It is again looking at how you build those trust relationships so that, if there is an organisation in Australia that is a trusted authority that people go to to ask 'is this a legitimate financial services institution' or 'is this a legitimate health institution', if I click on an overseas site there is somebody else I could look at to ask if they link back to the Australian one.

The reality is, though, that we are not saying that this solution will make the internet 100 per cent safe and you will break everything up. Our expectation is that you will still have parts of the internet where you are never going to be able to put that sort of model, and that would be an untrusted environment. But at least from a user's point of view I can then adjust my behaviour to that. With the example around booking a holiday, in my household we have a dedicated credit card that we use to buy internet services. The reason we have set that up is that it is not linked to our mortgage or to any of our financial bank accounts.

CHAIR—It is risk reduction.

Ms REA—That is a very good idea.

Mr Watson—Yes. It is basically a debit card and we put the money in. So, whenever I convince my wife—

Ms REA—It is an excuse to get another credit card. What a great idea!

Mr Watson—A lot of the financial institutions in Australia now offer that. They offer prepaid credit cards. The advantage of using those prepaid credit cards is that I reduce my risk. If I am going to a website that has this really good piece of technology that I have convinced my wife that I am allowed to buy, I can also then convince her that I am making the appropriate trust decision because I am using a prepaid credit card that might only have $500 in it. Again, from my point of view, whilst I have not removed the risk I have reduced it. I have said, 'Okay, if something goes wrong—if I spend that $500 and the goods and services do not turn up—yes, I've lost that $500, but I haven't then exposed all my financial situations.' Then as an individual I can go to the law enforcement agencies and say: 'That was the site that I went to. Here are the details of the transactions. It is very easy to identify because all my other transactions are separate; I can clearly give you the information so that you can then engage in how you deal with that issue.'

Mr Galligan—This plays back to that change management expression we raised in the preamble. Is the country going to get, I suppose, more incentivised to move online faster and with a richer array of services, be they government, economic, education, leisure or whatever? Simple things such as Peter has outlined are exactly that—they are pretty simple—but they require a level of understanding of the trade-offs for that. It is quite simple stuff. This is the change management we are talking about. I was talking to the folks this morning; we were just having coffee and listening to the new train timetable being explained over the radio. A train may not arrive. We were hearing the messages from the RTA on the radio: 'I need to turn up at a certain time and the bus network will get me there.'

If we do that for a traffic or transport network, how we are going to do it for a national broadband network needs to be thought about pretty early on. We have six to eight years for the rollout of this, and people will take up the applications very fast. If they take that up with—not naivety—a sense that government is there encouraging them to do this, I think government, along with industry, has a responsibility to make sure that those citizens are digitally ready and are going to use the network in the best, most efficient way so that the money that government is going to spend on the network is returned to the citizen. Government also needs to have done a trustworthy model, because if it does not then that trust is going to be broken and that investment is going to be seen to be not the best use of either government money or the faith that citizens have in the promise of the whole new digital economy.

CHAIR—There is one question I have to ask since you are in front of me. Some people have argued that one of the security risks is that, because Microsoft and Windows are so prevalent, because there is a known operating system it becomes a challenge. I suppose it is like having the design of the locks distributed widely; people know what it is like so they can spend hours working out how to pick it. Maybe open source software is actually more secure because it is different rather than being the same in every case.

Mr Strathdee—It is an interesting argument. However, the situation allows Microsoft to have a unique capability in our telemetry and our ability to collect data around current threats and trends. That expansive telemetry means that when we look at our trends we are able to validate them and align our product. Only last week we released a free security product that is very much in line with the current threats.

CHAIR—What is that product?

Mr Strathdee—It is called Microsoft Security Essentials and it is a free product. Coming back to the end-to-end trust logic again, having that unique view across our entire Windows ecosystem has allowed us to build Windows Defender into the operating system. It has allowed us to develop Windows Update so that we can actually distribute security updates to a very large proportion of the global computing horsepower. As we have moved from Internet Explorer versions 6, 7 and 8 we have increased the phishing filters and that type of thing on our browser technology. We have introduced memory randomisation into Windows Vista and Windows 7 so whilst in one way you can say that having one primary system may pose a threat, in another way it also gives us a unique capability. It allows Microsoft to be in a position to respond in a way that few other companies can and it also allows us to defend our platform and keep those defences moving on as our customers demand change as well. A lot of the testimony that we have heard today has really highlighted the fact that the threat landscape is extremely dynamic and my personal view is that I do not see it as a doom and gloom situation. I see it as just a moving target and we just need to stay in touch with where the current threats are and keep moving along that same path. I think that things like our new products set, Windows 7, Internet Explorer 8 and the release of Security Essentials, highlight that we are in tune with those needs.

Mr Watson—I think getting updates to software was discussed before. All software regardless of whether it is an application or an operating system gets updates, so the reality is that having a view that changing vendors or changing products is going to make us less susceptible to risks or security exploits is a bit naive because any application or any software that is from a good vendor should be getting updates. The reality is that software is written by individuals; it is written by people. That means software comes with exploits that are developed into it. It is interesting and it is a bit of an education thing that John was talking about that we as an organisation, probably because of our position, attract a lot of media coverage when a potential or supposed security incident is out there. For example, the one that occurred recently was in relation to some Hotmail accounts where like IDs were being phished. A number of articles were written about Microsoft, saying that thousands of Microsoft accounts were being phished. What was missed out in those articles was that we were not the only platform that was phished. A lot of the other online mail providers were also phished but they did not get as much attention in the coverage by the media. I also find it a bit perplexing—as I am sure the government does—that when we see all of these media articles about all the security vulnerabilities that are occurring out there, very rarely does the media then point to a link to a Microsoft site or somebody else’s site that tells you how you can secure your computer. So the media is very good at focusing on exploits that are out there and talking about hundreds of computers that have been affected, but it very rarely puts the focus on the education sites by providing four easy steps that you can do to avoid it. Those phishing articles missed a great opportunity to communicate to people the ways to avoid it, things like not clicking on emails from people that you do not know and reporting suspicious activity. The media never seems to focus on that.

Mr BILLSON—You have this release of Microsoft Security Essentials. How do people who are interested get hold of it?

Mr Strathdee—It is a free download. If you go to a Microsoft website and search on Microsoft Security Essentials, it will take you—

Mr BILLSON—That was an ad to get the message out. Moving on though—

Mr Strathdee—It’s not the ABC!

Mr BILLSON—No, there are probably about 20 people listening at the moment. They all rang in yesterday to give us wise counsel on our questioning. We had pages of questions to ask you, none of which we have got to, so if you are available for us to follow up at some point that would be helpful.

Mr Strathdee—Sure.

Mr BILLSON—Picking our way through your Identity Metasystem and seeing the sophistication that sits behind it, it segues into the community change management strategy. There is a lot of technology literacy sitting behind that concept and a lot of ground to be made up when, as research tells us, even the most literate are very aware of risks but one in four do absolutely nothing about them, according to some of the research. Talk me through that.

Mr Strathdee—The digital divide used to be—I suppose five or six years ago—about those who had access to technology and those who did not. Now it has moved on to those who can use technology—

Mr BILLSON—Who optimise it.

Mr Strathdee—and those who cannot—correct. There is increasingly going to be a divide between those with the ability to use a social networking site and those who do not in terms of how you are going to be able to use new rich applications that come through that social media. For a company like Microsoft we have, I suppose, a commercial advantage to make sure that there are more people conversant with technology. But there is also a pretty strong moral obligation too to make sure that people are not introduced to technology without the bare essentials of knowing the appropriate way to use it.

We do a lot of investment in community technology learning through community partners, from seniors' groups right through to organisations like the Smith Family and workforce groups such as WorkVentures et cetera, to make sure that the most underserved in the community, once they have technology put in their hands, understand the risks around it and the opportunities as well. We train between 100,000 and 120,000 people through those centres each year. We also provide a lot of literature and pedagogical work with teachers to make sure that as netbooks are rolled into schools the teachers understand that security is a core element of their responsibilities and the way the digital education revolution is going to be delivered.

But we can only scratch the surface of that new community, be it a senior who is going online for the first time or a long-term unemployed person who managed to get a computer kitted up in a housing estate. The risks around someone thinking that the internet is trustworthy, going for the first time through a browser and seeing the vast array of opportunities that might be out there for phishing scams right through to other nefarious opportunities, is a real problem.

Mr BILLSON—You have got delicious and rich telemetry. Picking up Ms Rea's example, when I get sent routinely advertisements of houses available in the outskirts of Moscow—gripping stuff!—I would have thought that your telemetry would be sophisticated enough, using one of your browsers, to green light that content, to amber light it, or to red light it when you are doing adventure surfing on stuff that is quite hazardous. Why isn't that part of your product? In terms of the algorithms that sit behind your browser rankings—and I accept that your browser algorithms are your KFC's secret herbs and spices and no-one will tell you what the 200-odd parameters are that add to the ranking—and given the richness of your data—these clean, reliable, non-botnet viral hosting that can go there and check it out with some confidence—what I do not understand is that with the technology you have why we cannot do that now.

Mr Strathdee—With Internet Explorer 8 we actually do a lot of that. We have phishing filters, and you will see that the address bar has different colours behind it. It is that whole stop-light mentality—green, amber or red. Also on other assets such as the Bing search engine, when we index pages we scan those pages for security vulnerabilities and page behaviour that we think may be risky. So on the client end, we do have a whole range of technologies and the phishing filter is but one. Also on the content provision end, we are also applying additional security.

As you have highlighted, with the sheer volume of data and the sheer volume of the telemetry that we have, it is about having the pure capacity to match those two datasets up. Whilst we are constantly refining how we do that—and I can assure you the products are under development continually—it is a continual process and we are only at a certain point at this point in time. It will get better and better as time passes.

CHAIR—We very much appreciate you coming along. It has been very interesting. Our secretariat may contact you if any further matters come up.

Mr Galligan—If you would like a private briefing we would be more than happy to provide that. Some of these things require visual aids.

CHAIR—We will certainly consider that.

Proceedings suspended from 11.16 am to 11.23 am

BROOKS, Dr Paul Westley, Member, E-Security Taskforce, Australian Computer Society

MacGIBBON, Mr Alastair, Member, E-Security Taskforce, Australian Computer Society

RAICHE, Ms Holly, Member, E-Security Taskforce, Australian Computer Society

VARADHARAJAN, Professor Vijay, Chair, E-Security Taskforce, Australian Computer Society

CHAIR—Welcome. Do you have any comments to make on the capacity in which you appear?

Prof. Varadharajan—I am from Macquarie University and am a technical board director of ACS.

CHAIR—Although the committee does not require you to give evidence on oath, this hearing is a legal proceeding of the parliament and should be given the same respect as the proceedings of the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Would any or all of you like to make an opening statement? If all four of you would, I would appreciate short opening statements.

Prof. Varadharajan—I am happy to make one. First of all, we would like to thank you for this opportunity. We are all members of the Australian Computer Society, with different roles, and we have come together as part of the E-Security Taskforce. As you know, the Australian Computer Society is a recognised association of ICT professionals in Australia. It is a member of the Australian Council of Professions and therefore it is the public voice of the ICT profession and the guardian of professional ethics and standards in the ICT industry.

Thank you again for this opportunity. This is an important inquiry and a timely one, we feel, given the dramatic developments that have been happening in the ICT industry generally across the world over the last decade and that will happen increasingly in the future, in particular in Australia with the development of the National Broadband Network and 24/7 online availability across the community.

We know that ICT is transforming every part of our lives. Along with this phenomenal growth in the technology, there is the phenomenal growth of computer crime, cybercrime. This is posing significant challenges across multiple fronts. Certainly in the technology world we all know that the development of dependable large-scale systems—as you talked about, for such things as online booking, with trustworthy services—is posing a lot of challenges. But it is also at the policy level. A critical issue is how to apply or formulate policies which will enable businesses to grow while protecting consumers and businesses from the bad things that are happening out there as well as achieving international cooperation in this area.

In the business world we need to build and maintain confidence in the infrastructure that enables this digital economy to develop. In the user community world out there, there are challenges about user awareness. Increasing the responsibility of the users and the ability of the users to take precautions is critical. From the developers' or the vendors' point of view, it is important that they develop products which have at least some level of security and that they provide information to the community so that the community is better informed in making whatever decisions they want to make. So the problem of cybercrime is a multifaceted one which includes business, technology and some legal aspects.

I want to briefly say two things and then come to some of the recommendations that the society is making. What we are witnessing here is an increasing threat velocity, a change in the nature of the landscape of threats. When I say 'threat velocity', what I mean is that the nature of threats is changing, on the internet and in the technology world; the types of players who are doing this are changing; the grace time allowed to deal with the threat is becoming pretty much zero; and the sophistication of the tools available for the attackers—who can be ordinary users—is amazing now, so that anybody can become an attacker.

The nature of the threat is changing because of the technologies. We have wide convergence of wired, wireless and mobile technologies. We are dealing with systems of systems, and the threats have a dynamic nature. The players range from individuals to hacker groups, to terrorist networks, up to state-sponsored attackers. In terms of the time for these attacks, it used to be a month—it used to happen with a slammer worm and so on—but nowadays we are talking about hours and seconds. So the time has gone to zero for the attacks. Then, as I said, there are lots of tools available on the internet for anybody to become an attacker.

Given this is the scenario, there are some recommendations that the society would like to make to this committee. I will go over a couple of them, because you have the submission in front of you. The first is that we applaud the federal government's initiative in establishing the Cyber Security Operations Centre. We believe this an important outcome and that the centre should work collaboratively with industry as well as with bodies such as AusCERT, GovCERT, AUSTRAC, CrimTrac and ensure cooperation.

The second, as I mentioned, is to do with the increasing threat velocity, which means that Australia, in particular, needs to take the opportunity to invest more in R&D efforts in this area to solve some of these issues. In particular, one of the things which are happening in this space is that there is an increasing adoption of mobile technologies and the use of these mobile technologies in conducting transactions. That will open up new opportunities for these threats to occur. The way we are working is also changing. We are allowing our employees to commute to do remote working. What this has done technically is to expand the security perimeter so that there is an opportunity for the threats to come inside the perimeter. Therefore ACS believes that the government should encourage Windows to double up systems with adequate security, informing the users about what features they are offering in their security. Whether the users—ordinary mums and pops—understand it or not is one thing, but at least they have some information at hand to make better decisions. ACS feels that with SMEs, in particular, there is a need to improve knowledge so that they can establish a security culture within their organisation so that—

CHAIR—Sorry; what was that?

Prof. Varadharajan—SMEs—small and medium enterprises. Sorry.

CHAIR—So it was a non-technical term.

Dr Brooks—Some people call them SMBs.

Mr MacGibbon—There is another one: it has a home-based business thrown in there as well.

Prof. Varadharajan—The challenge is often that larger companies have better resources to tackle the problem whereas SMEs now have been opened up to the same environment as the larger companies. They are talking to customers in different parts of the world and they allow remote working for their employees. They have techno system setting which is very similar to that of large companies, but unfortunately they do not have the financial resources or, most importantly, the staff with expertise to do that. So I think that is an important thing, especially given the fact that SMEs play a critical role in the development of economies like Australia and other countries. In summary, ACS believes increased professionalism amongst ICT professional practitioners, training and education of business end users and improved ICT literacy among communities must form an integral part of any program to reduce cybercrime.

Dr Brooks—I would like to point out that Graham Ingram, who is the general manager of AusCERT—the Australian Computer Emergency Response Team—was expected to be here today as part of the ACS team. Unfortunately he has been detained up in Brisbane, so we will carry on to the best of our ability.

Ms Raiche—‘Detained’ could be a bad word.

Dr Brooks—Not detained, but he was unable to get here this morning.

Mr MacGibbon—It was not an e-ticket malfunction, was it?

Dr Brooks—It was not an e-ticket malfunction, no. I believe they are tied up. Being a computer emergency response team, they are involved in real-time activities and actually fighting the very things we are here to discuss. Much of the ACS written submission uses statistics and things that Graham has carried around in his head. We will do the best that we can to provide a similar level of environment.

CHAIR—I am sure you will manage quite well. As a starting point for parliamentary committees, we tend to first look at what potential legislative changes can be made to improve the e-security of Australia. Does your organisation have any suggestions in that regard?

Prof. Varadharajan—Legislative changes? I do not think, at least from my knowledge, that there are any specific ones. But one of the things ACS is quite keen on is for the government to help establish a register of ICT security professionals, particularly for people who are engaged in activities involving critical information infrastructures—security professionals working in that space. In the past on behalf of ACS I have been involved with committees, along with NOIE—the National Office for the Information Economy—in a similar capacity. I am not quite sure whether it is legislation—

CHAIR—Or the regulator. It is close enough.

Prof. Varadharajan—A regulatory framework would enable us to get a better handle on the quality of ICT security professionals and the different organisations that are employing them, especially in the critical information infrastructures—to some extent, like the professions of law and medicine, or even trades like plumbing and painting, having some sorts of standards.

Mr BILLSON—You are thinking of something like the ICT equivalent of the ports and airports security arrangements where, if you are going to be working in those seriously important and potentially risky places, you have some validation of competency and security.

Prof. Varadharajan—Yes.

CHAIR—If there were a register like that, what would be required to be provided by someone seeking registration? What would be the criteria?

Prof. Varadharajan—In this as in others, there are three components with respect to the requirements: typically, knowledge and education, experience and maintenance in terms of competency definitions. So there are some education-type qualifications you would need for the person to be—

CHAIR—So they would need what?

Ms REA—What do you require now? And what would this registry require?

Prof. Varadharajan—As far as I am aware, in Australia and elsewhere there is not a clear mandatory requirement for employment of ICT professionals in these sectors.

Mr BILLSON—The employers satisfy themselves, essentially, unless they are working on defence contracts or something like that.

Dr Brooks—And some vendors have dedicated education programs where they certify people who have passed their course as security professionals in that particular field. But it is, in effect, a bit of self-certification in that I do not think anyone is going around and externally auditing those programs to identify just what level of security awareness or background in general goes into those courses, for someone to call themselves a vendor security professional, whether it is for Cisco or Microsoft or Loaded or any of those organisations—without wanting to endorse anybody.

Ms REA—So the register is not just a list; it also would require some level of qualification to allow you to be on the list—which is another issue—other than just being a register.

Prof. Varadharajan—Yes. In order for somebody to qualify to be on the list there must be some qualification. There are a number of qualifications. CISSP is one of the ones which is often referred to in the industry sector—that stands for Certified Information System Security Professional—but there are other certificates which are being run by private organisations, such as GIAC, the Global Information Assurance Certificate, which is run by the SANS institute.

Coming back to the original question: we need some sort of a quality-checking mechanism. The quality-checking mechanism of a professional would have some component of education, and that could be characterised as having a degree—a masters degree in IT security or one of these certificates. Then there is the experience component: has this person worked in this field for a certain number of years? And then there is the maintenance component. Because it is a rapidly changing field with dynamic changes in the security technology, there is a need to maintain competency. So, in order for somebody to qualify to be on that list, on the register, they would need to show these three competencies—knowledge, experience and maintenance—and then there would need to be some policy and guidelines associated with the registry and how they are dynamically changed over time, because there are some international liaison activities with other professionals in other parts of the world who are in this.

So the components would have some policies and guidelines and an independent board maintaining that. You would set up a registry where people would be registered when they passed through certain thresholds, and the thresholds would involve the components of education, knowledge and experience. So that is the international setting; that is how people tend to think of it. This leads to regulating ICT professionals in the security industry, which may or may not be appropriate in all sectors, in my view, but perhaps would be, at least, in the sector case of critical information infrastructure protection, where we need to have, clearly, a standard for people working in the sector, because it does have dramatic impacts if things go wrong. I would say that, as a professional society, we need to encourage government to help establish such a thing.

Mr BILLSON—Can’t you do it yourself?

Prof. Varadharajan—As a professional society we can suggest this framework, but we need the blessing of the government agency or authority. The proof of the pudding is how well it is taken by the industry. I might set up a registry and if employers start employing without taking this into account—

Mr BILLSON—So you need some impetus to get the street cred to make it happen.

Prof. Varadharajan—Absolutely.

Dr Brooks—If it is a voluntary thing then there is a need to get critical mass. To go back to the original question about legislation, the unfortunate thing about legislation is that it is really only something that is going to apply to honest criminals. We are talking about criminal activity here and people who have absolutely no regard at all for laws. Apart from setting appropriate penalties and ensuring that cybercrime is recognised as crime, we need to ensure that there are not forms of cybercrime that fall outside the definitions so that people can be taken through the court system and be penalised and thrown in jail or punished for doing criminal activity. Legislation is one of those things that criminals tend not to take great notice of.

CHAIR—It tends to be a solution of last resort.

Dr Brooks—It does. There may well be benefits in putting requirements of liability on organisations to have the appropriate mechanisms in place to try to prevent, detect, chase or identify cybercrime in the way that we expect companies or individuals to take responsibility for personal safety by having appropriate locks and security pass mechanisms for people to get physical access in and out of offices and those sorts of things. I think those aspects of creating offences of liability for not having appropriate mechanisms in place are probably already there. We try where we can to not treat cybercrime or things that happen in the online world differently from the way we would approach things in the offline world. Where it is appropriate, we try to have similar requirements in both environments. A crime is a crime and someone needs to be punished for it. People should still have the same obligations to try to prevent it from happening, regardless of whether it happens in the online world or the offline world.

Prof. Varadharajan—One of the challenges is that legislation always lags behind technology. Take the telephone, which was invented in the 1920s. It was only in the 1960s that congress passed a law that eavesdropping on telephone lines was illegal. Until that time, the legislative view was that we all know that the telephone lines go outside your house, but you still decide to make calls and put sensitive information through the lines, so therefore it is not illegal. One of the problems in the internet cybercrime world is that the legislative requirements are lagging behind. But at the same time the dilemma often is that legislation curbs the innovation part of it, so you want to increase the legislation with the private-public partnership so that the innovation is not curtailed. That is the sort of dilemma that we have—that is, that the legislation usually lags behind.

Mr BILLSON—I have a couple of questions on that. The deficiencies that have been brought before the committee have largely been twofold. One is that the Spam Act does not take malware seriously enough and we should pick that up. The second one is to do with crimes against a person, such as vilification, stalking and those kinds of things. There is an argument about whether addressing that is doable or not. A third area that I have flagged—and I am curious to hear your point of view—is that it should be unlawful to have something loaded up on someone else’s computer without their informed consent, but what about functionality on someone else’s system network hardware that is there without your consent? I am thinking of the British Telecom case. Price was imperative in some of the broadband infrastructure they had sourced from a country, and the allegation is that that hardware has functionality on it beyond what they wanted that would enable a third party to have some influence over its operation. Do you have a view on those latter two categories?

Dr Brooks—I guess if the vendor has sold equipment with a back door in it that would allow somebody else to control it without the knowledge of the owner once they have bought it and put it into place, to my mind that would be a deficiency on the part of the vendor. It would possibly also reflect on the organisation that bought it not doing sufficient due diligence in their RFP and evaluation process. But the organisation operating the equipment ultimately has the responsibility for the protection and security of the network and the service that they are operating with it. If their equipment is deficient and has that security vulnerability then they have a clear responsibility to fix the vulnerability in some way, even if that is to disconnect the equipment.

Mr MacGibbon—Can I make an observation about the Spam Act.

Mr BILLSON—Please do.

Mr MacGibbon—There are references in the Spam Act to where the purposes of the electronic communication are to the detriment of the other person. Perhaps there is some need for a better technical definition of malware in there. That might be a possibility. But I think there is a gap in the Spam Act that relates to the misuse of corporate messaging systems—for example, social networks. If I were to send an email to you as an unsolicited commercial communication, the definition would say that would fall under the Spam Act. But if I was on a social networking site spamming you and you were receiving that within the inbox of the social networking site, I believe ACMA question whether or not the Spam Act will apply. I think they would like it to. It would make sense, as more and more organisations that provide either an e-commerce or some other social experience online like to control those communications for a whole range of reasons. The good reason is that they want to control the user experience as best they can. But I believe it should be an offence to abuse those networks, just as it would be across the normal network.

Mr BILLSON—There is a Twitter example of someone flogging their coffee and cakes. That was thought to be very funky. I just wondered to what extent that meant—

Ms REA—There are even more examples. On the radio the other day there was a very interesting segment about the fact that the tobacco industry is now using social networking sites as a form of advertising because they are banned from other media outlets. They are getting around those bans by using those sites, so it is quite an interesting question.

Dr Brooks—It is a problem with the narrow definition of the communications medium. The Spam Act applies to email, which then goes to the question: what is email? It also applies to SMS.

Mr BILLSON—There is an argument as to whether video streaming on the net is a broadcast or not and whether you are a broadcaster.

Dr Brooks—That is right. They are laws that apply to a fairly narrow number of applications or methods of communicating. In fact, the concept of not being forced to look at a pile of unwanted material could be extended to a vastly wider range of communication methods. As far as I know, it does not apply to instant messaging, MSN, Yahoo! all those sorts of things. Arguably, it should. There are ways of sending an electronic message that may not be email but is another method.

Ms Raiche—I think the barrier is in the definition that it is electronic commercial messaging. There is a commercial element in there. And what is commercial? That may be a problem. Why can it not be all electronic communication? You had the Privacy Commissioner here. Did you have anybody who worked on the Law Reform Commission review of the Privacy Act? Granted, it is about 3,000 pages. It is a hard read.

Mr BILLSON—Yes, he spoke about that at length.

CHAIR—I do not think he actually undertook the review.

Mr BILLSON—He referred to it.

Ms Raiche—There are a range of recommendations coming out of that report. Unfortunately, it is all about the Privacy Commissioner developing guidelines as opposed to any kind of legislative change. I think that is because the technology is changing. What we have said in response to the Law Reform commission report is that we would like to be involved in some of the discussions about those guidelines, basically because of the breadth of spam. I would also like to say that if something is on the net and it is defamatory it is still a defamation. If it is against any of the discrimination acts it is still—

Mr BILLSON—The issue was touched upon by the Cyberspace Law and Policy Centre. The strict application of the law may be a very slow and cumbersome way than a more direct way of dealing with the harm. In a preventative and disruption model—a quicker take-down arrangement model, like the blacklist infrastructure—where is there space for someone profoundly aggrieved or hurt, or even contemplating self-harm? We get parents ringing our offices and talking about e-bullying that has immobilised a young person because of the effect on them emotionally. There is no free speech value in that, it is just malicious, yet the way of dealing with it is so cumbersome. A person’s self-worth is dissolved many times over long before any action gets taken. I am just curious whether an extended take-down arrangement for that kind of thing in collaboration with ISPs may be a better option than the purely legal pathway?

Ms Raiche—I will put on a non-practising lawyer hat: I would take a deep breath and say you would want to be very careful that there is an offence. The way the law operates is slow, but sometimes for good reason. That is not to say there is not harm and that you cannot have policies in place, particularly in schools and so forth—awareness of cyberbullying and that sort of stuff. But do you want a mechanism that is going to operate very quickly against something that may or may not be damaging?

Mr BILLSON—That is a calibration question, though.

Ms Raiche—It is.

Mr BILLSON—Where it is clear and vivid, and some ex-boyfriend is trash-talking his girlfriend; there is no free speech, there is no competing value that the law would ordinarily weigh. It is just a knucklehead behaving like a peanut. There is that end of it.

Ms Raiche—Sure.

Mr BILLSON—Then there are gradations that may need a different approach.

Ms Raiche—But if you were an ISP, you would want somebody authoritative to be able to say, ‘That is wrong,’ and then be able to do something about it.

Mr BILLSON—Or put it through the codes; a code review.

Dr Brooks—It may not actually sit with the ISP, but with the owner of the site and bulletin boards there. On a bulletin board or comment system where that sort of material could appear and then obviously be damaging because of the number of peers of the person concerned that can see that—and there is a time period involved in that—surely, the owner of the site has an onus to have a complaints mechanism that operates quickly. They are the ones that can take that material offline the most rapidly.

Mr BILLSON—You talked about risk to SMEs, vulnerability and mobility of workers and the changing workplace; what about, potentially, the social side and the Wi-Fi networks that are everywhere? You rock up to a restaurant and they go, 'We have got Wi-Fi, knock yourselves out,' or even that incidental coverage of apartments where you can hop onto the next door neighbour's Wi-Fi—what is your professional take on risk management in that framework?

Dr Brooks—A lot of it comes into education, that if you put up a new wireless network, the device you buy off the shelf needs to be configured in a certain way and have the security enabled. Unfortunately, it is one of those things that you cannot automate, because the user has to choose their own password, otherwise it would be known to everybody else. You can have a device that, when turned on, by default has a password encrypted thing in there, but then nobody can access it unless they know the password. If it is well known then it does not provide any security. That is one of those things, because it is under end user control, where we need to have education—when they turn it on, they should enable the security. There are lots of messages that come from ISPs and through the media for that side of things. I believe the Queensland Police Service started a program where they actually actively drive around the streets looking for unsecured Wi-Fi hotspots. They presumably stop, knock on the door and say, 'Hey, do you know that you are vulnerable to anybody parked at the bottom of your driveway stealing your download limit and downloading all sorts of things that can get you into trouble?' Those two things: I cannot think of another way that you could force people to turn on the capability for encryption—it absolutely should be there—and unsecured hotspots.

CHAIR—Could you not have it so that you could not activate the system without the person actually creating a password? If you did that they would have to, or they would never be able to use it.

Prof. Varadharajan—I think there are two issues here. One is user awareness. The Department of Broadband, Communications and the Digital Economy in the last two years has done significant work in the wider space educating ordinary moms and pops. I think they are doing a good job. In fact, their website is very friendly and very informal; a common human being can understand it without technical knowledge. So that is happening. But, yes, the point you make is absolutely valid. It is for product developers to ensure that you cannot activate the system. I think this is happening now. In the security world in the product industry, typically what happens is you get this trade off between feature and the security seen as an overhead. That is baggage this technology industry has had for a long time. Luckily, over the last decade or so people have been moving into lockdown products. For instance, you get operating systems—say, Microsoft—giving operating systems which are completely locked down and that you need to unlock to make open. Previously they used to ship open systems. Now people are shipping lockdown systems.

In the Wi-Fi case, previously they used to ship open systems in the sense that you did not have to put the password in. Nowadays there are more and more Wi-Fi products and chips, and the product manufacturers are saying you have to put the password in. It is an education exercise not only in the user community but also in the developer community, because the vendor community needs to hear from the users that they need security. Often they go by the fact that features are more important than security, because their customers tell them features are important: 'I want to play games faster on my machine rather than worry about putting passwords in it.'

Mr BILLSON—There is no greater vendor driven market in the world than yours, though, is there?

Ms REA—I go back to a couple of the points that you made at the beginning. First of all, one of the things that people have raised with us consistently is that legislation is fine; but, given that this is an international criminal circuit, how do we deal with that? What is the extent to which we can manage that when we have massive criminal activity from overseas? The second thing you were talking about is the idea of the register. I wonder what impact you think that will have. I will confess that when I go into a shop to buy something I do not check out their security system first. I know we probably all should, but we do not, and I imagine we treat the internet in exactly the same way. Whilst I think it is a good idea, what real impact do you think it will have if businesses and those operating on the net have professional security people managing their sites?

Prof. Varadharajan—Because the internet is borderless, one of our objectives is to have some regulatory framework within here and liaison and cooperation with international bodies. That is absolutely clear in this space, because you are not going to control the internet from one country, whatever the country is. ACS’s view—and I think governments across the world are doing this, and I know Australia is very proactive in this space—is to support international cooperation and alliances. The alliances come in two forms. One is government alliances, but there are also de facto industry alliances which span the globe. I would only add with respect to that part that to continue the international dimension is critically important for security.

Ms REA—But is it important that we have a legislative framework as well in order to build those relationships and connections overseas?

Prof. Varadharajan—I think so.

Ms REA—That is the benefit.

Dr Brooks—There are two parts. By having the legislation in Australia we can affect what happens in Australia and push that type of activity outside the borders of Australia. The more countries that do that, the harder that activity is. You do not reduce the possibility of anything happening at all, but you reduce the volume and the number of places on the planet that you can operate those sorts of activities from.

There is also a best practice dissemination. If what we do in this country is seen as good and effective, it will then be taken up by other countries in their own patches to further increase the level of security on a global basis—that ‘act local, think global’ sort of activity. But the other thing that does is increase the awareness of the number of people within Australia that have the expertise to deal with the attacks that come from the other parts of the planet that do not have those sorts of laws in place as a form of protection. It is a belt and braces approach. You try to stop it from happening as much as you can but then you recognise that it is going to happen anyway so you need to have in place measures to protect yourself.

So there needs to be an education program that increases the number of people that are savvy about how to counteract such activities that can be seeded within the business community, recognising that it is going to be the larger businesses that have those people on staff. Smaller organisations may be able to access the type of expertise through some sort of consultancy or part-time arrangement, but it is going to be the bigger organisations that are protected by the recognised register of security professionals more than the small mum-and-dad cake shop or fruit-and-veg shop operator.

CHAIR—Did you want to comment, Mr MacGibbon?

Mr MacGibbon—Thank you, Chair. Just on the international cooperation side, if I can talk tactically—my background is that I was in the Federal Police previously—I believe that Australia needs to take a similar approach to what Australia has done with, say, drug production and importation: the forward deployment of police officers to potential trouble spots, which is actually a very useful way of combating criminals. That has been done in Indonesia with terrorism. It has been done in Colombia with cocaine. It is done in Afghanistan with opiates, and the same in South-East Asia. In my view, law enforcement needs to come to a place where it realises that the pervasiveness of this type of crime means that you need to invest in that type of staffing so that you have formal law enforcement relationships in place and forward-deployed police in potential trouble spots.

The other thing is to have a range of other tactical investigative arrangements in place—for example, AusCERTs relationships with a range of other computer emergency response teams around the world. They are extraordinarily well placed to protect Australia through their very substantial international outreach. So it is a multilayered approach of very tactical, investigation/intelligence sharing, and then a much broader regime of creating a safer Australia legislatively that, as Paul was saying, you can then push out by way of example while creating a safer place as things come across the border here. But I would argue that it does take investment from a policing and an operational agency point of view.

Ms Raiche—Could I also add something? To pick up on Paul’s point about examples, I would use the example of the Australian Domain Name Administrator. In the international space, the ICANN Registrar Accreditation Agreement, which has recently been amended—and strengthened, I would add—to include resellers and a number of things, is fine. But auDA does a lot more. Not only does auDA have a registrar agreement which is very similar if not identical to ICANN’s agreement but it also has a code of practice that says, ‘If we give you a .au name’—it manages the open names—‘then you must abide by the code of practice.’ So there are a whole new set of arrangements under the code of practice in Australia that do not apply internationally. The international agreement lists the possibility of a code of practice but it just has not been developed. The fact that we have got one—and I actually think it needs strengthening, but it is a start—means that we can go out and say, ‘You need this.’ Because they do not have legislation in that space, it is very useful to have the sort of model that says, ‘We do it; why can’t you?’ The example I use is .com. We have a very strict .com.au: you have to have a business number.

CHAIR—It is a point well made. Thank you very much for coming. We have run a bit over time. We very much appreciate your time. If we feel we need to come back to you, I hope you do not mind.

Ms Raiche—No, that is fine.

CHAIR—Thank you very much.

[12.05 pm]

WILSON, Mr Stephen, Managing Director, Lockstep Technologies Pty Ltd

CHAIR—Although the committee does not require you to give evidence under oath, I advise you that this hearing is a legal proceeding of the parliament and warrants the same respect as a proceeding of the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. Would you care to make an opening statement?

Mr Wilson—I would like to make some really careful comments about identity. I stress 'careful' because experience tells us that this is an area that can drag us into the black hole of identity cards if we are not careful. I would like to state at the outset that we do not support the idea of any new identity card. We do not think that this is a necessary or even efficient approach to deal with the predominant cybercrime problems that we are here to talk about.

We do, I think, a pretty good job of identifying people already in the real world. There are a few cases like banking where identification is regulated, but for the most part identification is a local issue, meaning that identification rules are not set globally or centrally but tend to be worked out locally from one sector to another. For example, different credentials are used by lawyers compared to doctors. Lawyers will sign conveyancing materials and doctors will sign prescriptions using different systems and qualifications. Indeed, when consumers use their credit card, they are using a different identity.

I will tell a personal anecdote. I am a small business person. For convenience I opened my business bank account at the same bank where I do my personal banking, but I use different identities to do personal banking and business banking. I think it is actually the law that my corporate bank account has a different corporate identity from my personal bank account. Except at one time the bank mixed this up. I presented my business banking card to transact and the teller was able to access my credit card and my mortgage account from my business bank account through a bank error. I was personally affronted that those two identities had been mixed up. I think that was quite telling.

So in the real world I put it to you that identification and relationships are pretty well managed. The pressing problem in cybersecurity is to translate real world identities and credentials and relationships online. We said in our submission that credit card fraud online is the model cybercrime. By 'model' I mean that it illustrates the ease with which digital identities can be assumed and appropriated. We all know about stolen credit card black markets. I think you have heard this already in submissions. There is a huge black market. It is possible that tens of billions of dollars are changing hands. It is definite that a proportion of that is going to fund terrorist activities.

Crucially, most card details are stolen not from people as they go about using their credit card online, but rather the credit card details are stolen en masse by organised attacks on department store databases and third-party credit card bureau processes. This means that the best safe shopping advice in the world is moot. It does not matter how careful you are shopping online, you are still subject to identity theft.

The problem is that stolen identities are valuable. There is this huge black market where people buy and sell stolen credit card details and Lord knows what else. The technological problem is that stolen identities can be reused without anybody knowing. They can be replayed and stolen. This goes to Ms Rea’s question before about the risk of divulging more personal information like your CVV number on the back of the card. Indeed, these things get stolen and used against you behind your back.

To really curtail this problem we need to stop putting fire out with gasoline. The state of the art at the moment is that people just keep asking more and more secret questions. To curtail this we need to take steps to stop stolen identity data being replayable and reusable. There are so-called intelligent security technologies that you can use to release your identity data point to point in a very limited and controlled way. These identities are used one time and they cannot be reused and replayed against your will. These technologies really replicate our existing real world credentials and they do not involve imposing any new arbitrary global identification practices. It preserves what we heard before about different levels of identity being used for different contexts.

CHAIR—Were you here when Microsoft were making their submission?

Mr Wilson—Yes, I was.

CHAIR—How does your proposal differ from the meta identity that they are suggesting?

Mr Wilson—It is an extension, if you like. I am speaking specifically and frankly about intelligent identity devices—things like smart cards and SIM cards—that act as physical keys. In an encrypted form in the firmware of these devices they protect a whole portfolio of identities in the same way that your purse will hold a number of real world identities. The identity metasystem is like the business process behind that that allows electronic replication of your different identities—like your Medicare identity, your drivers licence and all of your different bank accounts.

What I am talking about is, where the rubber hits the road with the identity metasystem, that there will still be a weakness if the person accessing a computer system in trying to release the precise identity that they need in that context. The identity metasystem helps you get that identity and it helps paint a secure online experience where you know what you are doing, but the weak link is still going to be that your identity numbers can still be stolen if you are not very careful.

We are in a technology neutral environment. We like to frame approaches and regulations in a technology neutral way—I understand that—but the fact remains that some technologies are stronger than others in this regard. This brings me to the idea of smart cards and other intelligent devices which have small computers in them and they know what the user is trying to do. They know on your behalf that you are trying to do banking so that they will on your behalf communicate banking details to a website. If you are accessing a personal health record, you would use a different chip and that chip would know the context that you are trying to communicate to a personal health record and it would protect your privacy in that context without letting these different websites be linked.

CHAIR—Could you have a number of chips in one card?

Mr Wilson—Certainly.

CHAIR—Or could you have a card that you could just add different identities to? I have a whole heap of cards now. It is becoming ridiculous. I assume that if you had one for every computer identity you would have double the number of cards that you have now. Could you put it into one?

Mr Wilson—Absolutely, in the same way that your cell phone has multiple codes in it so that you can roam across different telephone networks. You can travel internationally and your phone is smart enough, through the magic of the SIM, to know what part of the world you are in and how to log onto the right network. Certainly smart cards can combine multiple identities. It might be quite sensible to have a health card that was used to access health sites, and you might have different logons for different sites all automated on the one card. We see this a lot in patient centric health care at the moment where people are making more and more sophisticated elections about who they want to divulge information to. In mental health services, and psychiatry in particular, it is very important. I think it is almost accepted now amongst professionals that, when you communicate details to a psychiatrist or in a counselling session, those details are firewalled from your general practitioner, for example—unless of course you elected to open up the files. So the technologies will allow that in a single chip.

CHAIR—I have recently been exposed to a computer which uses physical identification as a way of gaining access to the computer.

Mr Wilson—Biometric identification?

CHAIR—Yes. Couldn’t you do that for internet access, and then no-one could be you? I do not know how secure it is.

Mr Wilson—It is not.

Ms REA—Unless you have an evil twin somewhere.

CHAIR—I suppose if you had an identical twin you would be in trouble.

Mr Wilson—I would like to find a way to curtail the biometric debate because I think that the biometric technologies are not ready for what we are talking about. Biometrics are assumed to be—and in fact they are presented by their proponents as being—unique markers of who you are. The truth is they are not unique. In practice biometric systems always confuse small sets of people with one another. Moreover, there is no biometric that I am aware of that will allow you in the event of a theft to have your biometric identity revoked and then reissued. So it is distinctly unlike a bank card.

CHAIR—You cannot cancel it—unless you have a facial search!

Mr Wilson—That is exactly right. From a security point of view they are not perfect, and we have no way of dealing with the imperfection.

CHAIR—Sci-fi movies used to always have eye readers. I do not know if you remember those movies.

Mr Wilson—They look great because you stare into the camera and a split second later it says, ‘Hello, Tom Cruise.’ But those systems can take minutes and minutes to identify you against a big database, and then they will make a mistake. They will come back and say, ‘Are you Tom Cruise or are you Stephen Wilson,’ and you then have to clarify.

Ms REA—It is really hard to tell!

Mr Wilson—So I am told!

CHAIR—So you do not think those are viable options at this time.

Mr Wilson—They are very important technologies in limited doses. They are very important for things like data centres. Half-a-dozen people in the whole world might have access to a bank’s data centre. They might stare into a camera for several seconds, and the camera will take its time and be very precise. It might say: ‘I reject you. Would you have another go.’ If it is very high security, the biometric system is adjusted to not make any mistakes. So it might reject you, and you say, ‘Oh gosh, I need to stare again.’ I have used these systems, and if you are a data centre operator then you are used to that. It is part and parcel of the job. But if you are trying to access your funds in an ATM and there is a queue of people behind you, to begin with it has taken half a minute to recognise you, and then it might make a mistake, and the people behind you are waiting. There is really no biometric system that I know of that has solved those sorts of compromises in practice. Biometrics are very good for—

CHAIR—Identification out of a small group.

Mr Wilson—Yes, it performs well there. When you are enrolling people for passports, say, and you want to make sure that the photograph you have just taken does not match anybody else that you have previously photographed, you can take your time and do data cleansing and have your mainframe computers look for repeat photographs. But that is a distinctly different use from the science fiction idea of looking at the camera and money popping out. Coming back to digital identity, which is my theme, how do you cope with multiple digital relationships without linking them together so that people maintain their privacy and their autonomy? Biometrics really is not the answer for that, because all it conveys is your biological self. If you want to go to a Medicare office and say, ‘This is me,’ they do not want to know you DNA; they actually just want to know your Medicare number. One of the really important e-health applications now is online counselling and online patient consultation.

CHAIR—If you were a doctor trained over many years in psychiatry this would be a bit off-putting, but I have heard they actually receive better results from online counselling than from personal counselling.

Mr Wilson—Yes, it is phenomenal. If that is true then participation in those systems absolutely rests on privacy and preserving people’s anonymity. The last thing you would want somebody to be able to do is to insert your Medicare card and receive anonymous counselling, obviously. But you might insert some sort of other key that has been given to you by your counsellor, and you know it is a separate device and you know that it is going to log you on securely to an anonymous system.

Ms REA—Like a token.

Mr Wilson—Yes. One of the paradoxes in all of this is that these digital identities are the keys to e-health, e-banking and e-government, but we have this ‘anything goes’ kind of Wild West environment at the moment. We have a number of different passwords and some people give you random logon generators and other people give you plastic cards, and it is really like the Wild West.

It is interesting to me that we take a lot more care with car keys. My car has got a modern key that you cannot duplicate at the locksmith; you have to take it back to the manufacturer. It has an engine immobiliser and all of these electronics and smarts. But electronic service providers are still very timid about authentication. They are very timid that authentication technologies will compromise convenience. Convenience trumps all else at the moment. We have got ourselves into a situation where, believe it or not, the cost of identity fraud every year far exceeds the cost of car theft. There is half a billion dollars of car theft every year and at least $2 billion of identity fraud, according to the AFP.

CHAIR—That is four times as much.

Mr Wilson—We are in this situation because we take more care with car keys than we do with logons. If you would like me to continue my remarks, I have some thoughts about the role of government that I would like to share.

CHAIR—Yes, that would be good.

Mr Wilson—I would reiterate that we need no new identification regime to solve cybercrime. I think what we need instead is a better way of taking our digital identities or our existing physical identities and using them online. So I would like to see government lead by example. I believe that governments should commit to the public that some of the new e-government services will use state-of-the-art identity safeguards. We especially have to take care with the new programs like the national individual health identifier.

CHAIR—I think that will be a real testing ground for all of these sorts of issues.

Mr Wilson—I do too. It is a work in progress but some of the things that were said about this thing a year or two ago suggested that not a great deal of care was going into security. I heard once that the health identifier was compared to a pin number. That would be a very dangerous mindset because, as we know, when your PIN number gets stolen, you go and get a new one. The idea of the IHI is that you do not ever get a new one and so it needs to have that commensurate safeguard in place.

I would suggest that the Attorney-General’s Department, which has had carriage of something called the National Identity Security Strategy, should re-energise that work and expand its scope to look at digital identity as well as birth certificates, passports and what have you. We have heard already that the National Broadband Network needs to factor in security. I would suggest that it really takes care to factor in digital identity security as well. I would like to suggest that idea of the smart Medicare card, which gets a run every now and again, be taken progressively. The idea of a smart Medicare card devoted to health care and protecting things like health identifiers is a very powerful idea and is long overdue. I could see the smart Medicare card being married to the individual health identifier in a really useful way.

CHAIR—Yes, it sounds like an obvious combination.

Mr Wilson—It does. Politically it produces a lot of anxiety, it is fair to say. But I would put it to you that the political risk of the smart Medicare card could be reduced in three ways. We could make it dedicated to health care, we could produce express engineering designs that protect privacy and, above and beyond all else, we need to make sure that any new chip card does not introduce arbitrary identification processes. We have tried that before. We have had the concept of photographing everybody before they get their Medicare card. Clearly, that is such a jolt to the way we interface to Medicare that it is risky. If we follow the line that your existing relationships in the real world can be transferred online with the proper technology then you can have a chip enabled Medicare card that replaces your existing card. Then we can allow people to start using the technology to access healthcare services online as well as the new emerging electronic health record systems.

CHAIR—How do you do that online? If it is like a Medicare card and is credit card size, how does that allow you to access health information online?

Mr Wilson—My company advocates the use of chip technologies in smartcard readers.

CHAIR—But how would your computer read it?

Mr Wilson—You would use it just like you do an ATM or an EFTPOS terminal. You would have a reader connected to your workstation or terminal at home, you would insert the right card, like a Medicare card, and the chip in the card then talks to the website. The chip, on your behalf, will make sure that you are talking to the real Medicare site and not some fraudulent site or, if you are attempting to talk to a personal health record site, the chip on your behalf can hold back your Medicare number and release just your nickname or your handle. People in psychiatric online counselling sites are going to have their own handle and be completely anonymous. You can protect that anonymity by simply coding or encrypting their nickname into the chip. The chip will communicate to the website on your behalf and make sure that you are going to the right site and then release the information on your behalf that is required to authenticate you. We are seeing a lot of this sort of technology being reused especially in Europe.

CHAIR—Where in Europe?

Mr Wilson—The most advanced system is actually in Estonia.

CHAIR—Really? How extraordinary.

Mr Wilson—When I say ‘advanced’, there are chip cards that are used for multiple applications.

CHAIR—I see; they are not just used for health.

Mr Wilson—They are used for multiple health applications: health records and prescriptions as well as rebates. France has had a smart health card for over 10 years, but it is fairly low-tech. It is just about taking magnetic stripe information and securing it in a chip, and it is not used online. But I believe that the French technology has been refreshed so that you can start to use it online at home. That may be the case with the German card, but that has not been determined yet.

Ms REA—That is very interesting.

Mr Wilson—Estonia's national card is a really interesting program. They do internet voting using the card.

CHAIR—Voting as in national elections?

Mr Wilson—Election voting.

Ms REA—Is it a smart card? Is it a multipurpose card?

Mr Wilson—Yes, it is.

Ms REA—Does it include health?

Mr Wilson—In Estonia, yes.

Ms REA—It would be interesting to know what their security issues are. Have they identified security issues with having all of those applications on one card? That was an issue that you raised earlier.

Mr Wilson—Yes. The card has been engineered from the outset with those advanced encryption technologies in the chip. It is also optional, I believe. It is not compulsory to use your card to vote online. It is an extra that people are electing, pardon the pun, to do or not. That level of consumer acceptance and consumer election is always going to be important.

CHAIR—I do not think we would want to do that first off. I think most people would see that as some sort of conspiracy.

Mr Wilson—I agree, Chair, that that would be a step too far in the first instance.

Ms REA—But I am interested that there is a country that has got quite a sophisticated level of applications on one card. There must be some learnings coming out of there. What do they do, for example, about lost cards and all of those sorts of things? Is that data protected?

Mr Wilson—Definitely. They have an encrypted database for replacing lost cards and there are protocols for facing up to a government agency and proving your legitimacy to retract or reproduce a lost card. I certainly do not advocate the one-card-fits-all approach in the Australian environment or indeed as a cybercrime response. What I am suggesting to you is that there are these smart technologies that are congruent with our existing relationships. So what I do suggest is that the Medicare card could have a chip in it and be used to conduct health care relationships online securely in the same way that your bank card has probably got a chip in it now, if you check. Increasingly, those chip cards are going to be used online to do secure internet banking. I think that we should be mapping things from the real world onto the online world and preserving those relationships and keeping things separate.

CHAIR—I imagine there is a great deal of advantage in terms of how you could record things. You could record what you are allergic to and your blood type. If it included prescriptions, it could record what other prescriptions you have, whether you prefer to have no-name prescriptions when you go to the pharmacy—a range of things which would make it more effective in terms of your personal health care.

Mr Wilson—Again, going back to cybercrime, one of the intelligent things that these chips can do is without revealing to the world—and certainly without revealing everything to a central database—they can self monitor how they are being used and they can look out for abuse, if you like, intelligently and locally.

One of the problems in health care—it is not a huge problem, but it is a problem—is prescription shopping, where somebody will go to a dozen GPs in one afternoon and get precursors for speed or whatever. It is said that you could stop that by data mining every prescription, but I do not think you want to send all mom-and-pop prescription data to Canberra and data mine it to look for the tiny proportion of crime. Instead, you could have your smart Medicare card involved with the prescription event so that, when the doctor fills out prescriptions for opiates or narcotics, that is flagged in the chip, and the chip will know if you are doing that multiple times.

There is always the convenience trade-off, and some people will say that it would be poor form to limit people’s access because they do not have their chip card. But, on the other hand, if you are dealing with prescribing scheduled narcotic prescriptions, there are rules and barriers in place anyway, and it might be a reasonable trade-off to insist that people involve a chip card in that prescribing event so that the chip can look out for abuse.

It is analogous to the way that chip cards are used to prevent credit card fraud in Europe. In Australia, our EFTPOS system is largely online, which is why we have relatively low rates of card fraud in Australia, but in Europe, because telecommunications is more expensive, your retailers are usually offline. The crooks know that, so they can take a stolen credit card and they can buy 10 VCRs—there are no VCRs anymore, are there?—or they can buy 10 DVDs.

CHAIR—I think they are still around; I do not think many people use them!

Mr Wilson—You know what I mean. You can make 10 huge purchases without busting the credit limit. But the chips now have come in, and the chips will actually keep tally of your credit card transactions in the chip, so if you try and buy more than €1000 worth of stuff in one day the chip itself will block the transaction. It is a lesson, a learning, about how these intelligent technologies can curtail crime in a decentralised way. We are not talking about taking every transaction and sending it centrally and data mining it, but rather we are saying, ‘Let’s use the technology locally.’

That is all about card abuse, but equally these technologies can protect people against misadventure online, because they can check the validity of websites. We heard previously that browsers now can flag a green light or a red light. All of these things are good measures, but there is an arms race going on, and phishing sites can beat those traffic light colours in a variety of ways.

Ms REA—Already?

Mr Wilson—Already. So what you need to do is to peer deeper into the cryptographic codes that are being exchanged between the browser and the website.

CHAIR—‘Fast flashing’ or whatever it is called; isn’t it?

Secretary—Fast fluxing.

CHAIR—Fluxing.

Mr Wilson—Yes. It is beyond the ability of the lay user to check out those codes for themselves. What you could do is put that into the chip so that when you access an important website the chip in your card is communicating to the website, knocking on the door and checking the answer as to who is there.

CHAIR—Fascinating.

Ms REA—I found that very informative.

CHAIR—I have to say it was absolutely fascinating. It has not only given me great ideas for this particular inquiry but also given me great ideas for my other areas of interest, so I very much appreciate your coming in.

Mr Wilson—I hope that is useful.

CHAIR—Thank you for appearing.

Mr Wilson—I would like to just add that, on the point of the anxiety that these technologies generate, I do understand that, but it is somewhat disproportionate when you look at SIM cards. I think we spoke before about learnings. Some of the most important learnings are actually in Australia, where we have a whole generation now of experience with smartcard technology in the form of SIM cards. My kids have an amazing first-hand understanding of SIM cards. They know about the importance of the PIN. They know that, if they swap a SIM into another phone, your phone numbers go with it by magic. They have also experienced SIM lock, where you cannot put the SIM into some handsets. That is a privacy sort of issue.

All of those learnings, I think, are really important. We use SIM card technology without giving a second thought to the idea that we have a smartcard in our phone that might be monitoring what we are doing, because it does not. I would like to suggest that we could take a more level headed view of some of these smartcard technology options if we drew the parallels with the SIM card. SIM cards are obviously subject to telecommunication regulation and a whole lot of frameworks that prevent abuse and regulate their use, but we are in an environment where people no longer have that level of anxiety that maybe somebody is monitoring their phone calls just because they have a smartcard in their phone.

It is a really deep learning that we take this sort of stuff for granted, and yet when somebody comes along and suggests a progressive idea like a smart Medicare card then it sends the hares running on the basis of anxieties that the technology would be an aid for surveillance or an aid for monitoring. In fact, it can be just like SIM lock. SIM lock means that if you put your SIM into another handset it will not work. If I had a smart Medicare card, I could put it into an ATM and it would not work, or a hacker could take my smart Medicare card and put it into a reader, but it would not work, because of SIM lock.

I would just like to close on that note. We have a technology that is about 20 years old that is well habituated and well embedded in a lot of what we do. Certainly, in terms of cybercrime, the same technology could be leveraged again in things like smartcards.

CHAIR—Thank you very much, Mr Wilson. Our committee may contact you again if we have further matters. Thank you again.

Proceedings suspended from 12.36 pm to 1.33 pm

SCROGGIE, Mr Craig, Vice President and Managing Director, Pacific Region, Symantec Corporation

CHAIR—Welcome. I have had a request that someone be allowed to take photographs. I would like to formally move that we authorise the taking of photographs and it is so resolved. Although the committee does not require you to give evidence under oath I advise you that this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Would you like to make an opening statement?

Mr Scroggie—I would like to thank the committee for giving Symantec the opportunity to participate in this inquiry. It is our honour to share our views and knowledge about cybercrime. We have done this previously with the House of Lords and the US Senate.

Symantec's perspective is largely derived from research conducted by our global intelligence network, which monitors more than 30 per cent of the entire world's email traffic and gathers intelligence from 240,000 sensors deployed worldwide in more than 200 countries. The intelligence we gather tells us that it is very hard to protect yourself or to protect confidential information online. As an indicator of how prevalent cybercrime is today, we have learnt that every fraction of a second a crime is committed or attempted on the web.

While statistics on the impact of cybercrime are difficult to quantify for Australia specifically, we know that in the United States one in five people will be a victim of cybercrime this year. By many estimates the collective efforts of the online criminal community now generate more revenue than the illegal drugs trade. The online underground economy is organised, professional and ruthless. Their activities include corruption of ordinary citizens so that they send spam email, distribute pornographic content and even attack other computers.

Criminal activity online is not retreating. Symantec has observed the number of computers controlled by criminals each day increased by 31 per cent in 2008. Many individuals are falling prey to social engineering attacks through phishing scams or threats targeting popular Web 2.0 applications. Some others unknowingly install malware on their computers while surfing legitimate reputable websites that have been compromised.

Credit card information was the most commonly sold item in the underground economy in 2008, accounting for 32 per cent of the items for sale. There are many ways to steal credit card information, and stolen card data can be easily sold for as low as US6c per card when purchased in bulk. Some groups even specialise in manufacturing blank plastic cards with magnetic stripes meant to be encoded with stolen credit card and bankcard data. A further indication of how professionalised the underground economy has become is an increased coordination and competition to produce and distribute items such as compromised malicious code and phishing kits. This has led to a dramatic increase in the proliferation of malicious code.

Whilst it is challenging to capture cybercriminals, there have been some instances of success. For example, earlier this week it was reported that the FBI had arrested a large number of individuals associated with what appeared to be an international phishing ring. The arrests were part of an operation dubbed Operation Phish Fry and the individuals arrested were suspected of defrauding computer users in order to steal money directly from their bank accounts. Earlier this year there were two significant cases of ISPs that were shut down because of malicious activity. These ISPs were hosting malicious code, phishing websites, bot command and control servers and spam relays. This includes an incident where Symantec saw a 65 per cent drop in spam and a 30 per cent decrease in bot activity within 24 hours of one particular ISP being taken offline.

Greater cooperation amongst internet security stakeholders is needed to identify, mitigate and limit the impact of these types of threats. For instance, a coalition was formed to address the aggressive spread of the Conficker worm at the end of 2008 and still currently in 2009. Due to its multiple propagation techniques, the worm was able to spread rapidly and infect millions of PCs. We have also seen it infect major corporations in this country. The Conficker worm even contains an update mechanism that can allow new versions of the worm or other threats such as a bot to be installed on compromised computers.

Given these threats and the dangerous intent of the criminals behind them, there are several issues that Symantec believes the Australian government must consider in fighting cybercrime. Firstly, stronger laws are needed to elevate the importance of information security. Australia already has laws relating to privacy, spam and cybercrime. Data breaches are a serious problem that needs to be tackled as we see the increased proliferation of organised crime gangs targeting and stealing confidential information. Mandating data-breach notification and providing guidance to both business and individuals about what to do in the event of a breach will help reduce loss and harm to the Australian community and its constituents.

In October last year, Symantec conducted a survey into the prevalence, cause and cost of data breaches experienced by Australian businesses. The survey revealed more than 79 per cent of Australian organisations who responded had experienced some form of data breach. Approximately 40 per cent had experienced anywhere from six to 20 known data breaches in the past five years. We therefore welcome the government’s consideration of mandating notification of such breaches. However, a balanced approach should be adopted—for example, through a safe harbour principle whereby organisations whose data has been secured to an adequate level of security need not undertake notification and are relieved from possible liabilities and penalties.

The Australian government should help to secure individuals and small businesses. Unlike large enterprises, these entities have relatively little means and knowledge to protect themselves in a similar way against the challenge that consumers—the mums and dads at home—face. More than half—58 per cent—of small and mid-sized businesses in Australia and New Zealand experience some form of security breach. These are the findings in our Symantec 2009 global small and mid-sized business security survey released in May this year. However, small-to-medium businesses are ignoring basic safeguards. For example, approximately two out of every five, 43 per cent, of respondents have not implemented end-point protection and more than one-third, 39 per cent, of small to medium businesses do not have antivirus protection. According to our intelligence report, the areas experiencing the most spam are generally locations populated with a higher density of small-to-medium businesses. Similarly, the lowest spam places are often home to some of that largest companies. In fact, Auburn in New South Wales, just 30 minutes from here, is the most spammed suburb in Australia. The spam levels reached 94.1 per cent and Auburn is one of four suburbs in New South Wales in the top six, which also includes its neighbouring suburb, Silverwater. Both have a high concentration of small businesses, which are a known target for spammers due to the possibility of less security protection than a larger, more capable enterprise.

Additionally, between four and six million computers are scattered across the globe have been compromised by cybercriminals without the user’s knowledge at all.

Ms REA—I am interested in the fact that it is a specific geographical location. I can appreciate that a certain type of small business or a group of them would be targeted, but why one particular geographical area?

CHAIR—And how?

Mr Scroggie—Generally it is where we see a larger concentration of smaller businesses. Depending on size and capability, smaller businesses such as small retail outlets are very much like consumers in that they do not have protection. If you are a more mature small business and have more sensitive information—for example, an accounting practice or a legal practice—you may be better prepared or have more knowledge to protect yourself.

Ms REA—But the spammers do not necessarily know that they are targeting Auburn. It is just that there is a large number of businesses there. Do you see what I mean? It is interesting that it should be a defined area.

Mr Scroggie—Yes. Whether it is that suburb or any other, they are not looking at the suburb particularly but more the profile of the individuals that they are able to breach.

CHAIR—It is really that the profile of the suburb happens to match the profile of what they are targeting.

Mr Scroggie—That is correct. These computers now form robotic networks, or botnets, which are controlled by cybercriminals and used to send out more than 87 per cent of all unsolicited email. More than 90 per cent of all email today is spam. That equates to approximately 151 billion email messages a day. The global spam rate in September 2009 was 86.4 per cent, but Australian businesses were receiving more than their fair share and currently the level in Australia is 90.7 per cent. For many SMBs the issue of strengthening their IT security infrastructure is compounded not only by the challenge of staffing, budget and time but also by trying to keep up with the growing amount of information that now resides on mobile devices such as laptops, PDAs, smart phones, USB drives, DVDs and anything that is able to be moved.

There is a general lack of awareness about the nature of today’s threats. We believe that the government should explore ways to provide more incentives for individuals and small to medium businesses to enhance their security through the purchase of technologies or risk assessments or through participation in training and education programs. Government could partner with industry to provide and promote low-cost security packages and education for consumers and small to medium businesses. Earlier this year Symantec participated in the National E-security Awareness Week, where the government conducted information sessions in Perth and Darwin to educate small to medium businesses on how to better protect their information and business online. We also participate in a number of education programs targeted at consumers, including the National Zombie Awareness Week, National Identity Fraud Awareness Week, World Computer Security and the Australasian Consumer Fraud Taskforce. Symantec recommends the Australian government continue to invest in education and awareness campaigns for consumers and small business that have longevity to reduce the risk of complacency.

Let me turn briefly to advances in security technology itself. We believe that we are reaching a point where it no longer makes sense to focus on analysing malware. Rather we should focus our efforts on analysing ‘goodware’, which is more economical and less time consuming. The traditional signature approach used by almost all security companies works well with highly prevalent threats such as Code Red, Nimda or Conficker, where many users have been impacted. However, the landscape is changing. Increasingly, malware is microdistributed largely via web based attacks to only a very small number of machines across the entire internet. This is the reason why Symantec has recently created a reputation based security technology, codenamed Quorum, where information is provided both on good and bad executed files rather than just the bad ones. Every application is assigned a reputation value, which supplements the classic black-listing approach. Quorum also leverages the community wisdom, the wisdom of crowds, by harvesting reputation information about websites and applications from more than 35 million users who have opted in to the service.

CHAIR—Is that in real time?

Mr Scroggie—Yes. On the topic of our national internet infrastructure, we need to consider ways of making it more secure, especially in view of plans to construct the National Broadband Network. Faster broadband connections will carry criminal attacks to Australian computers more quickly than is possible today. This is a serious issue and will make them more vulnerable. We should make our infrastructure secure to make our citizens secure. It is also important to note that with the NBN there is an opportunity to raise protection levels for consumers and business. A faster connection means that updating virus definitions and patches is no longer a long and arduous task. With the appropriate level of awareness and the message of convenience, some of the risks to consumers and business can be prevented by simply using up-to-date security software and patching it in a timely manner. Again, a coordinated education and awareness campaign between the public and private sectors aimed at changing the behaviour of consumers and business should be considered.

Protecting children online is also an important area where new strategies are needed. As parental control software tends to drive children underground, new approaches are needed to foster greater trust and healthy dialogue between parents and children, while allowing parents to reduce the risks that their children face online. Lastly, the protection of critical infrastructure is another key focus area. The internet infrastructure is susceptible to attacks, and so are information systems in critical sectors like utilities, transport and telecommunications. With the upcoming Spring Racing Carnival some of the online betting communities are also being targeted with distributed denial of service attacks. So it is not only public critical infrastructure but also private enterprise that is being targeted. An effective system of early warning, intelligence and security response is paramount to enable quick response to and recovery from any cyberattacks on these sectors.

At Symantec, keeping people safe online has been our focus and our passion for more than 20 years. As in the real world, we believe that every individual and every business should have the right to feel safe online and to be free from any online exploitation. We believe in creating confidence in a connected world, confidence in our community and confidence in the internet. We look forward to working with you, as we do with many governments, businesses and consumers around the world, to turn that vision into a reality and create an internet that is a safe and clean place for everyone. Thank you.

CHAIR—Thank you very much for that opening statement. Quite early on in your opening statement you referred to encouraging governments to provide a subsidy for small businesses, and I think you said consumers as well, to put in place protections. My very loose assessment of what it costs for pretty basic protection, I suppose, is that you can probably get a reasonable protection for your computer for less than $100. Is the barrier for people doing that really the $100 dollars—or perhaps it is really $50 or $60? Is it really the amount of money that is the barrier or is it just that they do not really know how to do it—it is all a bit fuzzy—so they just do not bother? You look somewhere else.

Mr Scroggie—It is a great question. You touch on a really interesting topic. There is also security technology available on the internet free of charge yet only a third of small businesses have security technology implemented. A lot of it really relies more heavily from an investment point of view on education and understanding the threats and helping businesses understand that taking those simple protection measures can protect their confidential information and protect their consumers from that data being bought and sold in what is becoming a very mature online underground economy where basically anything can be bought, sold and traded.

CHAIR—I am quite curious that you are saying you can buy credit card identification data for as little as 6c an identity—

Mr Scroggie—Yes.

CHAIR—Where do people go? Is there something like a supermarket for credit cards? How do they make contact with one another?

Mr Scroggie—In a similar way that reputation is important if you were buying or selling something online, say, using eBay. You have an identity on eBay and to go and buy and to get a reputation score and they say that you paid on time and it was good service and the goods were delivered as described. In the underground economy, because it is more organised crime, that organised crime is highly distributed. What we see is actually quite a mature process of infiltration: entering an organisation, collection of the data and the exfiltration of the information. At those different stages, from the infiltration to the exfiltration where the information is then sold in the underground economy, there are different people and different skills required, everything from getting the code—the malware that is installed on your computer, the keystroke logger or the screen scraper that steals your information—to the next step where once the attacker has the information they then need to be able to turn that into some form of currency.

We would see, particularly in more challenging economic climates, ads for people to be finance brokers or to work from home, perhaps for five hours a week. Those people would be told, ‘You only have to do this or that.’ What happens is that their job is to go to the bank with some bank account numbers and withdraw X amount of money and transfer that into other accounts. These are kinds of muling activities, whether in the banking system or in any other form of online transaction where the money is moved.

But specifically, how do the criminals communicate with each other? There are bulletin boards. In a similar way to finding anything else online, those communities know where information is. Basically the information is publicly available but you need to know where to look. If you are in that community, it is not difficult to find those backdoor channels where that chat takes place and that underground economy exists.

CHAIR—So if it is that easy to find you would think that law enforcement agencies could find it too.

Mr Scroggie—Law enforcement agencies are better equipped today than they have ever been in the past to monitor those activities. Recently the US Secret Service took down the very large ShadowCrew. They monitored ShadowCrew’s activities—the sale and advertising of malicious code authors, mules, credit cards and scanning systems—and they were able to not only shut down the bulletin board but then put up a warning from the Secret Service saying, ‘We have been tracing all of the activity and all of the identities of people buying and selling in this underground economy and we are now coming for you, because these are the things that you have breached from a regulatory violations point of view and these are the crimes that you will have to pay for.’

CHAIR—That must have made them think very hard. You mentioned that there was an ISP taken down; I think you said it produced and amount of 30 per cent spam in 24 hours?

Mr Scroggie—Yes.

CHAIR—Did that ISP know they were doing this, or were they being utilised? Was it a self-aware breach?

Mr Scroggie—It is actually a difficult question to answer because the role of the ISP is to provide the service, not police it.

CHAIR—Exactly.

Mr Scroggie—A lot of the debate that we are faced with today, whether it is content filtering or providing clean pipe, is very much around what the role is that each individual plays in providing something like the National Broadband Network. The role of ISPs is to deliver a service and make the internet available to consumers or businesses. Their role is not to be the policer of content, whether that is illegal or not.

CHAIR—But that is a very pure sort of view of it. If it is just policing content in terms of good taste or quality of work maybe you can take that attitude. But if it is actually illegal activity, is that not a higher level where maybe we should consider that ISPs have some responsibility—particularly where it can be readily apparent to them—and put in place some sort of control?

Mr Scroggie—If we had a legislative framework in place that required those ISPs to report that activity?

CHAIR—That is what we are sort of considering. Obviously, one of the issues that I hope we get to look at as a committee is what the responsibility of an ISP is. What is reasonable and how serious does it have to be before that responsibility arises? If there are botnets operating, what is their responsibility in terms of the consumer to notify them? All those sorts of things are issues we are very interested in, so if you have a view we would be very keen to hear it.

Mr Scroggie—Content awareness is a challenging thing that you are trying to consider. Where does censorship start or stop and where does the responsibility to monitor what would be classified as, say, malicious, sit? Leaving the censorship part of the debate out, and saying that regardless of whether we define a particular type of content as not available, if we purely just focused on malicious crimeware and said that was what the ISPs needed to look for, we can do that today. We can identify malicious code and malicious websites—

CHAIR—An ISP can do that?

Mr Scroggie—The ISP would have the technology to be able to identify that in an email. If you were sent an email to your inbox, and that email had a link or a file attached to it, the file would be scanned and you would be informed by the ISP that if you ran that file on your machine there is malicious code in it that is designed to steal your identity or capture your key strokes and send them to wherever the server is that it is designed to send that information to.

The other component would be the links that are included in email attachments. A lot of phishing comes as a result of being sent an email by trusted brands. Sometimes it comes from your bank; recently, we have even seen it come from the Australian tax office as an email—there are lots of those.

CHAIR—Yes, I have seen quite a few of those.

Mr Scroggie—When you click on that link you go to a phishing website. The reality is that today we have the technology to be able to screen those emails as they are on the wire and even stop them from getting through the National Broadband Network—we could do it at that level. Or we could let them through, but provide the consumer or the business with the ability to make the decision: even though you have been warned that it is either malicious content or a malicious link to a known phishing website, you can still click it if you want to.

CHAIR—What sort of an imposition would that be on an ISP in terms of cost?

Mr Scroggie—We provide that service today, and we provide it to businesses rather than ISPs. If you are a large enterprise you can use our mail scanning products or our web products, and they are of no performance impact.

CHAIR—Are they just like a software application attached to your server?

Mr Scroggie—As the mail moves through the internet cloud, instead of the mail going from the sender directly to your inbox, the mail goes from the sender through our system, which scans—

CHAIR—It is like a cloud?

Mr Scroggie—It is like a cloud service; it scans for malicious content or malicious links to known phishing websites. It still delivers the message to the user, but it just advises them whether it is malicious or not.

CHAIR—But can a server do it? I mean, assuming a server is there, can they do the same thing rather than go into a particular cloud service?

Mr Scroggie—Could an ISP do that?

CHAIR—Yes.

Mr Scroggie—Yes, they could.

CHAIR—What sort of costs are involved in that sort of thing?

Mr Scroggie—Consumers have the ability to do that with the antivirus and intrusion detection/intrusion prevention and web-surfing product that we put in our consumer technology today, which is called Norton or PC Tools. So, in the Norton technology, if you click on a website but you go to a known website that is malicious, it will actually come up with a big red cross and say, ‘This is a known malicious website; you may be compromised if you provide confidential information on this site.’ So we can do that at the consumer or the business level directly, without it needing to be provided as a service today. But the problem is: only a third of those small businesses are actually putting that software on their machines—even though, in some cases, it is freely available.

Ms REA—I guess I might be asking you to argue against your business, but we have heard a lot of evidence over the course of this inquiry about the sort of cat-and-mouse game that has been played in terms of antiviral software—effectively, good security barriers that prevent stuff coming in. You have also talked in the submission and today about the particularly vulnerable people—small businesses and those sorts of people—who are not investing in security. But also we have heard a bit of evidence today about the effect of using encryption and other forms of security—accepting, in a sense, that people are going to give information out via the net but therefore having some protections that prevent that information being reused. I am wondering whether, even from your business perspective, you are moving into that area as well. Do you think that that is possibly going to be the way that we go, rather than trying to out-hack the hackers, if you like—to look at other ways in which we can prevent that information being used further, rather than just stopping it getting through at all? I would be interested to know what you think about that.

Mr Scroggie—It is a fabulous question. It is a big one!

Ms REA—Yes, I know.

Mr Scroggie—Let me break it down into a couple of pieces. First of all, to take the concept of data loss: whether it is laptops, USBs or mobile phones, the proliferation and the volume of information is significantly greater than it has ever been before. That is only going to continue to grow. We know information is growing at 50 per cent a year. Many people are unaware of the simple risks. For instance, if you leave a USB on your desk at night, the cleaning crew that comes through could go around and pick up every USB off every desk and then sell those USBs, because at some point there will be some valuable corporate information on there that somebody is going to want to buy. Organisations can take very simple steps to protect themselves so that, where any classified or sensitive information is copied to a USB or a DVD or emailed or uploaded to a sharepoint or a wiki—

Ms REA—Or put on a card.

Mr Scroggie—or a social networking site or a card—anything; any way information is transported—if that information is deemed confidential, before the information is transferred the system scans it and says, ‘There is something in there that would be a policy violation’—it might be AML or payment card industry standards; or credit cards, a social security number or a tax file number or whatever—‘that information cannot be copied unless it is encrypted.’ So it automatically encrypts it, or it says, ‘I’m not going to allow you to copy it until it is encrypted.’

But here is the problem—and this is the second part to what you described. Why doesn’t that happen? It does not happen today for the same reason that only a third of small businesses in the community actually protect themselves, and that is: the businesses have the technology at their disposal, but either they do not appreciate the significance of the risks, or they do not see the value of the information and how it is being bought and sold and the risk to themselves and their constituents from an information-trading point of view. But you can automate, through policies and technology, so that those things happen automatically without anyone in the business needing to do some form of intervention.

Before you send an email a message would automatically pop up saying that you are about to email a file with something in the submission that was deemed confidential, that it will still let you send it because we do not want security to be seen as an inhibitor to productivity, government or enterprise and what you need to do is go back and write ‘encrypt’ in the header line before the email gets sent. Therefore, if the information is lost or stolen it is no harm, no foul, and in the proposed changes to the Privacy Act and the introduction of data breach disclosure notification laws the proposed safe harbour within the legislation for mandatory breach would include encryption, so those recommendations are very good. The types of voluntary breach notification guidelines that already exist from Karen Curtis and the Office of the Privacy Commissioner are also very good. For those types of things the reality is we have the technology but it is not being adopted, so education has a large role to play in solving the problem at large that you described.

Ms REA—That is very informative. Is there anything more, other than an education and awareness raising campaign, that the government could do coming out of this inquiry that would see more take-up of those sorts of measures? What role do you think the government can play in trying to encourage people to do that more?

Mr Scroggie—Outside of education I think there is one very significant thing. There is no question that the introduction of the broadband network will bring extraordinary productivity gains to the Australian community. But the government could take protective measures to ensure that whilst we may not filter content we are content aware. They are very different things. So if we were able to inform consumers that even if they do not have antivirus software on their machine—they are a small business and one of the 66 per cent who do not use it—they are going to get something that has come through the network that says, 'This is a malicious, known phishing website or the code here is suspect', the government would have advised. The government would have done its part in advising the community that there is some harm or risk that might take place as a result of this. The government would not decide what content could get through or not. It would not be managing the black list or the white list, but based on the global intelligence network it would have been able to advise that we know the information is at risk. Just that process alone would be enough education to get many people in the community to realise that if they had not known that the file was malicious and had opened it, their information could have been stolen, keystroked, screen scraped and sent off and sold in what is a maturing underground economy. From the point of view of education, the ability to be content aware could significantly shift the protection profile of Australian constituents at large.

CHAIR—You have indicated that there may be some gaps in the Australian legislation to protect against cybercrime. Can you be more specific about where those gaps are and what type of legislation you think would be beneficial?

Mr Scroggie—Not in a short period of time.

CHAIR—We are happy for you to take homework if you would like to.

Mr Scroggie—Yes, we have a number of recommendations specifically in relation to the legislative framework. It is comprehensive and I would like to take that as homework and make it a submission with another piece of confidential information that we are going to share with the committee that is not publicly available, a new report on the threat landscape.

CHAIR—If you forward them to us we can have a look at them and receive them with confidentiality if that seems appropriate.

Mr Scroggie—We spoke about it earlier.

CHAIR—How can the government stop the automatic installation of spyware or adware?

Mr Scroggie—It is a very difficult thing for the government to be able to do. Again it comes back to the fact that if the individual users are unaware that they have downloaded a file with drive-by downloads, it is a very difficult thing for the government to ensure that consumers at home are not accidentally compromised on a legitimate website let alone an illegitimate website. Again it is about having the content awareness when you are connecting to the website. But when our consumers who use Norton Antivirus technology—and there are 130 million of them worldwide—either open an email or go to a website, they are informed that it is a known malicious site. So we can do it today. The government could do it if it mandated the use of some form of end-point security technology.

CHAIR—Wouldn’t the most convenient way of doing that be to require all computers be sold with that sort of software attached?

Mr Scroggie—That is an interesting concept; however, there is a problem with that. It is a problem we see at large in most enterprises today. We actually do not see it as much from the consumer side. I will explain to you why it is a great question. Most people who have antivirus or end-point protection technology at home have a system called LiveUpdate. Every day—whether they are at home or not—the computer is connected to broadband and it gets the latest virus signatures. But many organisations which are large and complex and have a lot of network security want to make sure that any updates they get from Microsoft—operating system resident updates or any application updates—are tested before they are put out into the production environment. That is to see if there is a problem with any changes in code that are brought down at a retail shop front or a banking system that could impact the business. The problem is that today, even though consumers are able to get those new virus definitions immediately—the Conficker outbreak as a worm is a great example—a lot of the problems that businesses are facing already have solutions available. Many Conficker outbreaks could have been prevented for large- and medium-sized businesses if only they had updated their operating systems and their security software.

CHAIR—They were not agile enough to do it quickly whilst consumers could do it virtually overnight.

Mr Scroggie—That is correct.

Ms REA—Obviously you would have a very good perspective on the international situation. We clearly have had lots of discussions around here that, whilst there is probably legislatively quite a lot that the government can do, we cannot solve this problem just within our own country; it is an international problem. We have had evidence presented that we can be leaders in this respect but that we also need to maintain our relationships and communications with other countries. I am wondering if from your or your company’s experience you can perhaps identify some countries or companies that really are working well on this one and where even the committee could benefit from some examples overseas of countries or governments that are having an impact.

Mr Scroggie—A position we would love to get to is where globally law enforcement and government agencies are collaborating closely on protecting consumers. The issue that we face, in the same fashion as for traditional law enforcement, is that it is hard to get that global coordination. The establishment of task forces and working groups, in which we do participate within the US, the European Union, the Asia-Pacific and Japan—

CHAIR—When you talk about ‘us’, are you talking about Symantec or about Australia?

Mr Scroggie—Symantec, in terms of participation. The challenge is really that, for many of the countries where we see the threat landscape emerging strongly, such as the Russian Business Network—in our internet security threat report we see China and Russia as two areas where a large volume of the spam and the coordination or control of the bot networks originates—many of the organised crime groups invest in those communities because either the communities do not have the legislative profile or buffers in place to ensure that they can manage down that crime. That type of crime in itself is becoming a booming industry within those economies. So it is not so much that the more mature economies are not collaborating; it is that many economies are growing but cybercrime is a growing business within those communities. That creates a challenge on a global scale from a policing point of view.

CHAIR—I thought that the People's Republic of China actually filtered all of its internet access.

Mr Scroggie—Yes, they have tried to.

CHAIR—But they do not filter it for illegal activity?

Mr Scroggie—I think the interesting part is that it does not necessarily stop illegal activities from being undertaken, and we see this in many cases. The best real world example I would give is that if intellectual property and brand protection was an issue we would not see a lot of fakes coming out of a country like that. That country largely distributes products that are not licensed by the brand but are purporting to be the brand and it is still seen as a legitimate business. I think we probably suffer a similar fate in the electronic context. Whilst it is known on a global scale that that is breaching intellectual property protection and brand protection rights, it is still not an issue for that government per se to necessarily take action on.

CHAIR—Do you think it should be made illegal to load software onto a computer without the consent of the person who owns or is in possession of the computer?

Mr Scroggie—If the penalties existed for doing that, that would certainly be a way to ensure that the cybercriminals themselves, assuming that we had access to them for prosecution, which is really the issue—

CHAIR—Finding them is another issue.

Mr Scroggie—Finding them and then being able to bring them within our legal jurisdiction is a challenge. So, whilst having the legislation in place may be interesting for us, I do not know that on a local scale within the Australian community we are producing a large enough volume of malware for that action alone to really change the shape of the volume of malware in the community today. When you consider that 90 per cent of all email is spam, a very, very large percentage of that is coming into this country from overseas.

CHAIR—I suppose the objective would be that we would enact that sort of legislation and all the other countries would enact the same thing.

Mr Scroggie—Yes.

CHAIR—Obviously that would be a fairly long-term process, but it would have the desired impact.

Mr Scroggie—I think it is not dissimilar to the globally coordinated activities that monitor and control the drug trade. We have a similar long-term battle in front of us. We tend to refer to the growth of the underground economy, the proliferation of organised crime and the distribution of fraud and identities on the internet as something that would effectively represent a similar style of industry to the drug trade. It is going to continue to need all governments to work in collaboration on a global basis to ensure that we can provide better levels of protection for, and build confidence in, our communities.

CHAIR—Thank you very much for appearing. It has been very interesting.

Mr Scroggie—Thank you. It is my pleasure.

CHAIR—It may be that the committee contacts you further. I know that we are going to receive a bit more information from you.

Mr Scroggie—You will.

CHAIR—We may also contact you about other matters. Thank you very much.

[2.18 pm]

DUCA, Mr Sean, Technical Solutions Manager, Australia and New Zealand, McAfee Australia Pty Ltd

LITTLEPROUD, Mr Andrew, Managing Director, Australia and New Zealand, McAfee Australia Pty Ltd

CHAIR—Thank you for making yourself available. It is much appreciated. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Would you like to make an opening statement?

Mr Littleproud—Thank you. First of all, McAfee appreciates the opportunity to respond to this important cybercrime inquiry and applauds the Australian government for addressing such a critical issue. As McAfee we are able to provide analysis of and thoughts on the current cybercrime environment, both in Australia and globally, and can provide views on the existing status of Australia's prevention and enforcement efforts. With the impending rollout of the National Broadband Network and the important security operations within that context, we believe that time is of the essence in addressing some of these important issues.

McAfee is concerned with the exponential increase in and ongoing sophistication of both the targeting tools used and the cyber criminal organisations developed to prey upon consumers, businesses and government agencies. Cybercrime today is worth more than US$100 billion around the world and now surpasses the value of the illegal drug trade worldwide. Despite the proliferation of security tools and ongoing education efforts, consumers, businesses and governments continue to underestimate the threat from things like phishing attacks, data loss and other cyber vulnerabilities.

Last year, in 2008, the number of malware designed just to steal passwords alone increased by 400 per cent. Just in the first half of this year, more new malware appeared than was ever created in the whole of 2008. In Australia, the McAfee Global Threat Intelligence unit has identified that there are more than 135,000 senders generating almost one billion malicious emails every single day. The number of malicious URLs located in Australia increased by 847 per cent from the first to the second quarter of this year and the number of suspicious web servers located in our country grew by over 300 per cent in the same period. Despite this growth, Australia is still relatively near the bottom of the list of countries hosting malicious websites.

This growth will continue and McAfee would like to work with the Australian government to support your efforts in fighting online crime. We are able to support your education and other efforts with our expertise in blocking malicious threats and identification of cybercrime trends globally. Some examples of how McAfee can assist include cybercrime trending, updates and personal briefings of the more significant findings in our major reports. Upcoming McAfee reports will address the state of cyber warfare and the security status of critical infrastructure. McAfee continues to work with global cybercrime fighting organisations such as the US FBI, the United States Secret Service and the Police Central e-crime Unit in the UK as well as other cybercrime-fighting organisations around the world.

We feel that extending this work to Australia is of significant importance. Assisting organisations like the Australian High Tech Crime Centre to coordinate the response across sectors, the expertise and global coordination of AusCERT as well as the sophistication of the Australian financial services and telecom sectors will help us in responding to and fighting online crime.

We also commend and see the value in the ongoing education and awareness efforts such as the National E-security Awareness Week. However, governments and business need to continue to focus on education and awareness not only to improve prevention of threats but also, just as importantly, to provide the appropriate processes and resources to help victims. Equally, we need to update the laws to punish cyber criminals appropriately and to improve resources and training for law enforcement agencies to better tackle the issues of cybercrime, especially across international borders.

Finally, as the country prepares for the NBN, McAfee has offered assistance in developing a centralised e-crime reporting portal. This leverages McAfee’s web portal threat research and other relevant expertise in coordination with regulators, law enforcement agencies, telecom providers, financial service providers, CERTS and others. McAfee has deployed such a portal elsewhere in the world to great effect. McAfee is the world’s largest single focused internet security company in the world. We proactively seek to secure systems and networks from known and as yet undiscovered threats worldwide. We cover home users, businesses, service providers and government agencies. Our partners all trust our security expertise and have confidence in our comprehensive improvement solutions to effectively block cybercrime attacks and prevent disruptions.

Thank you again from this opportunity to respond in order to support your efforts, and we are pleased to answer any questions that you may have.

CHAIR—I am very interested in your portal for the reporting of e-crime. How extensive is it? Where have you done it before? How effective is it? How does it work?

Mr Littleproud—Predominantly, we have done it in the US.

CHAIR—For the whole of the US?

Mr Littleproud—Yes. We basically created an online portal where we connected information from our own laboratories that monitor and manage the threats on the landscape with information from government agencies and industries so that we could find out where the threats are coming from in that respect. It also provides educational facilities where users can go online and try to understand the threats that they should be aware of as well as providing a facility where the users can report on e-crime activities and attacks undertaken. Finally, it provides facilities for people who have been subjected to cybercrime to seek help in terms of rectifying the situation and where to go next for ongoing assistance.

CHAIR—So it does not just collect the data; it actually provides the person who has made the report with information about where they go? Does it actually refer the complaint, or does it just get back to them and say, 'You should go here,' or, 'You should go there'?

Mr Littleproud—It is a combination of both, dependent on where we can take this type of strategy. That will dictate how automated we can get in sending on to the relevant authorities information about people who have suffered cybercrime, but it would be a combination of advice about what to do in the event of being attacked and also, as I said, if we can get the working parties working more closely aligned so that any sort of response from a policing agency could be redirected to those, providing that they were part of the community, basically bringing that together.

CHAIR—How is the cost of that process borne?

Mr Littleproud—In the example that we have in the US, the cost was borne by McAfee initially to get that portal up and running. I am not quite sure now whether there are other sources of income in terms of how that is supported and maintained. Sean, do you know?

Mr Duca—I am not aware of it.

CHAIR—We would be very interested if you could have a look at that, because obviously cost is always an issue.

Mr Littleproud—Yes.

CHAIR—If you could possibly have a look at that issue and get back to us, we would very much appreciate that.

Mr Littleproud—Yes. We have already presented some initial ideas to the Department of Broadband, Communications and the Digital Economy, in Canberra.

CHAIR—Our difficulty is that we are a parliamentary committee, so, despite the fact that there is obviously a very close relationship, there is a division of power: they are the executive; we are the parliament. We can ask them, but they may or may not provide us with that sort of information. So, if you are able to provide what you can—I understand that there may be commercial-in-confidence issues, but maybe just using the example of the US—it would be interesting to us to know how that system operates on a financial basis.

Mr Littleproud—Absolutely.

Ms REA—A lot of what you have said is very useful, and I guess it is information that we have heard from a number of other people as well, but the one area that we have not explored a lot so far is the issue of the social networking sites. It seems from what you have said and from what others have said as well that there has clearly been a massive explosion in cybercrime in the last couple of years, but there is also clearly a move so that spam is not the only method. I am not sure if it is still the predominant method of trying to get into people's systems, but clearly there are a lot of issues around networking sites. Even on a legitimate level, we are seeing them used as advertising sites. Companies are coming in and using them as a way of advertising their products. But obviously that is leading to criminal activity as well. Can you enlighten us a little bit about whether that is true, about whether my intuition is right that it is an increasing problem? Secondly, is it something that we need to deal with differently than the way we deal with spam or other forms of cybercrime, or can we start to work on policies that can cover all the ways in which criminals can get into a system?

Mr Duca—Absolutely, your intuition is correct. I think probably the rise of social networking sites is a way to share and collaborate on information, and it obviously has led to ways of cybercrime getting into those specific areas.

Ms REA—I am sorry to interrupt you, but really what I am asking is: is it just because you have a rise in networking sites and people using them that you have a rise of criminal activity, or do they actually make it easier for criminals than other forms such as email or people purchasing online or providing data in other ways? I guess that is my question really.

Mr Duca—Both. Obviously, as something becomes popular, it always becomes a target, but then, at the same time, the way that these types of social networking sites work, you can easily post some information and Andrew can easily post some information, so you are automatically sharing this information, as opposed to one website that you go to where I am the website operator and I post the information. Because everyone can start to share and collaborate on this information, it is a lot easier to start to spread and infect other types of people in the system. If you look at something like Facebook, with over 100 million users, that is a way that you can simply create a new threat and release it to potentially 100 million targets out there. The threat can easily spread on those types of social networking sites. You can easily develop and post your own information and obviously create your own bad applications as well.

Mr Littleproud—The other thing we are seeing with the advent of social networking is obviously that people’s personal information is becoming more readily available, so cybercriminals can use that information to be more targeted in individual attacks, if you like. So there is another dynamic that is happening in that respect.

Ms REA—The second part of my question was: do you need to do something differently to deal with the way that they access that information, whether it is a spam email or something else, or are there policies that we can develop that can attack all ways of criminals getting into personal computers and information?

Mr Duca—Probably a bit of what we have been doing over the years already in terms of user education and awareness. There is sometimes a bit of a perception that it is safe because I know who you are, but your identity could have been compromised. It is people just making users aware of the fact that you are logging on to an open forum and you may not actually be speaking to the person that you think you are speaking to, because their identity may have been compromised. It is always probably just providing that level of education to ensure that, when you do post information, you remember that you are posting it to an open forum, and you could also receive something quite easily onto your system.

CHAIR—In your submission you talk about the McAfee Cybercrime Response Unit in the US. Can you tell us a bit more about how that operates?

Mr Duca—That is based on the e-crime portal. The response unit was set up to try and act as a bit of a middleman so that people can come to us to respond to any threats that they have been a victim of. From there, we can start to work with other agencies that we have had previous dealings with and start to get everyone together, because if you are a victim of cybercrime it is a case of: ‘Who do I go to? What do I do?’ And then it is a case of education: ‘Where do I learn if I have been a victim of cybercrime, or how do I prevent this from happening to me?’ The cybercrime unit effectively works with that and obviously is—

CHAIR—It is an adjunct to the portal.

Mr Duca—Correct.

Ms REA—Have you had any prosecutions as a result of it?

Mr Duca—Information that we have collected from the McAfee Cybercrime Response Unit has helped in prosecutions, but, in terms of specific numbers that are a clear result of it, I do not believe so, no.

Ms REA—So you collect the information and you pass it on to the legal authorities—

Mr Duca—Correct.

Ms REA—who then go and investigate?

Mr Duca—Yes.

Ms REA—In some ways, because it is such a broad area of criminal activity and it is difficult to investigate and apprehend any criminals, obviously the information coming out of your portal gives the information or the particular event that happened another level of legitimacy that would encourage the legal authorities. One of the issues we have is that somebody rings up and says, ‘Look, I think they’ve taken money out of my bank account,’ and the police go, ‘Well, there’s nothing much we can do about it.’ But the fact that you are there providing that information and some level of legitimacy to it assists them in investigating?

Mr Littleproud—I think it does provide a level of legitimacy and it does encourage a little bit more of an active approach to resolving the matter. Quite frankly, if we are to take a similar approach in Australia, it is really going to be dependent on the relevant parties coming together and agreeing to what extent we are going to work together and operate. So if we were to create some form of government e-crime portal then it would need the government to be able to take a stake in that in terms of the type of legislation in place and how you are going to provide information on the portal—and, more importantly, how we are then going to get the police to actually do something about information that comes through that. So we would have to work together—governments, law enforcement and us—as a technology organisation. And it would not be just the provision of the technology but the provision of a service that actually acts as an aggregator of crime statistics and known threats around the world that we can also feed into the portal so that people can log on and get an up-to-date view of the landscape, as well as consumers themselves or organisations being able to go in and register the issues that they are up against. So they are the ingredients. It is really a question of the extent to which people are going to commit to that conglomerate of organisations to make it as effective as it can be.

CHAIR—So as well as being a reporting portal it would also tell you, ‘The latest threat is the worm,’ or whatever the latest thing is; ‘If you have it or you suspect you have it, this is what you need to do.’ Is that what you mean?

Mr Littleproud—Absolutely, yes.

CHAIR—You seem to suggest in your submission that Australia’s investigation and prosecution of cybercrime could be improved. Do you want to provide any more details about that or any suggestions?

Mr Littleproud—Again, it is probably based on the holistic nature of where the legislation starts and ends in including cybercrime activity—what are the cybercrime rules and regulations? I think that could go a little bit further in some respects. Once that is in place and up to date, it is a matter of how law enforcement gets skilled up to be able to enforce those rules and go on to prosecute violations. If we take organisations, we could say that right now there are certain compliance measures that drive organisations to behave in a certain way, depending on the type of industry they are in. What we would like to see is a lot more stringency from a legislative point of view so that there are regulations around people’s personal information, for example, and how organisations store people’s credit card information, because quite frankly there are organisations out there that probably are not as secure as they should be that are taking people’s personal information and storing it in their own environment. If that is then subject to some sort of cybercrime activity and people’s personal information is compromised, through no fault of those individuals, they end up becoming victims.

So it is about trying to set the bar as to what the laws say and making those clear and specific around cybercrime. Then it is about how we train and educate our law enforcement people to follow those through and apply those rules, and the extent to which they can then dole out the necessary consequences, whether they are prison sentences or fines et cetera. Then, from a corporation point of view, we need to have the right stringency and compliance regulations in place that drive organisations to have to make sure that their environments are secure if they are going to secure people’s personal information, for example.

CHAIR—So you think that there is an argument for reviewing the issues of privacy and protection of personal information in the private sector—that there are insufficient safeguards in private sector organisations that collect and store private and confidential information?

Mr Littleproud—In a lot of the world that I talk in, which is with organisations, companies and corporations, there is definitely room for legislative measures to force them to keep individuals’ information a bit more safe, if you like.

CHAIR—We had a detective inspector from the New South Wales Police in here yesterday. He was of the view that there is actually a very small number of investigators—he described it as ‘a very small club’ and did not get down to the nitty-gritty of saying exactly how many there are—who have the skills and capacity to really investigate a lot of cybercrime. With some of the experiences that members of parliament have, as we do from time to time, where you have individuals come into your office who have been victims of cybercrime, generally, unless they are major crimes their only avenue is the local police station. And, let me tell you, most local police stations are not really equipped to investigate cybercrime, so it is a bit difficult for people in that situation.

Mr Littleproud—Absolutely. That is why the cybercrime portal that we have been working on in the USA is at least a step in the right direction to try and give some sort of support to the community at large—or victims, for that matter—to try and see what happens in the event of some sort of criminal activity being perpetrated against them from a computer point of view.

CHAIR—There certainly seem to be a few gaps out there.

Ms REA—I would like to know, in respect of the issue of cloud computing, a little bit more about how it actually works. I have sort of an idea but not a clear one.

Mr Littleproud—Me too!

Ms REA—Secondly, there seems to be a bit of a division of opinion about it. Obviously people are a bit more concerned about it from a security perspective because it means their information is effectively stored elsewhere. But, on the other hand, I think that in your submission and others there is a view that it could be more secure than if it is sitting on my vulnerable PC. Could you elaborate on that a little bit more?

Mr Littleproud—Sean will do that.

Mr Duca—The purpose of cloud computing is that you have the ability to start to use technology as you require it rather than just simply saying, 'I've got a PC; I need to have the following applications and I use them accordingly.' Using cloud computing, I can start to say, 'I've got a requirement now for word processing', or 'I need to do some sort of accounting. I can just simply get access to a lot of this software.'

Ms REA—Without having it stored on your computer?

Mr Duca—Correct. All the data remains online. So, if you think of something like Hotmail or Gmail today, it is email processing that is based purely in the cloud. That is effectively what cloud computing is, but it is expanding to incorporate other applications that a small business or even a consumer at home could actually be using as well. When you start to think about a range of other applications, you can start to store more and more data in the cloud. So it is a case of asking who the organisation that manages the cloud is and what security measures they have in place to protect the data. I know that if I actually installed the software, I manage the software and I manage all the data that I have got on my own PC. I can effectively put a lock and key around it to protect the data that is on there, but I do not know what the cloud computing provider can put in place as a measure. So you need to know what type of security is there, and that is probably the big issue that a lot of people are currently debating right now. If you start to look at things that have happened overseas—and shipping data abroad to overseas countries as well—it is a case of asking, 'Who is going to get access to my data? What third party organisations have access to my data?' The same principle obviously applies with cloud computing.

Ms REA—Is there an argument to say that in fact it could be more secure?

Mr Duca—It could be, but I think you also need to question what type of security is in place in those organisations. Simply saying, ‘It is in the cloud, it is easier and cheaper to use,’ does not necessarily mean that it is completely secure. It is one of those things that I think people need to be aware of and they need to start asking those questions of those providers.

Mr Littleproud—We provide it in the cloud services for certain aspects of what we do. One service is to do in the cloud a comparison of information or data that is flowing to and from the people that have subscribed to this service, so that we are actually doing some security in the cloud before files or data even get to the organisation or the individual. The idea is that by having multimillions of subscribers we are gaining access to more and more traffic across the globe and therefore can get a lot tighter in the provision of that service and how accurate that service is, so that we can actually stop a lot of attacks before they have even got out of our cloud and back into an organisation. If you look at the National Broadband Network, for example, at the moment, from what I understand, it is basically going to be cable and that is that—no intelligence or no security.

CHAIR—I do not think anything has been determined yet.

Mr Littleproud—That is the way that I understand it from what I have read.

Ms REA—In terms of the need for speed, that is obviously the way it is going.

Mr Littleproud—That is it—it is basically a high-speed network. A governing body or an entity could run a cloud service for securing that network, for example, and that might be an option to review, so that an element of responsibility is taken by the network provider or a third-party entity to secure it.

Mr Duca—Effectively providing a clean pipe, so to speak, to the entire broadband network.

Ms REA—Just to clarify the way it works: if you are doing your tax, for example, and you want to access MYOB or something like that, you would do that and then you would put that data back into the cloud? Is that what happens?

Mr Duca—Correct.

Ms REA—So it is not sitting on your PC?

Mr Duca—It is like someone else’s hard drive.

Ms REA—I can see concerns about that, but at the same time I can see a niche for security companies to create clouds specifically, like a bank effectively, saying: ‘Don’t leave your money under the bed. Come and put it in our cloud because we can look after it better than you can.’

Mr Littleproud—It does not have to be stored in the cloud. The provision of the security service could be as the information passes through along the network, the security is provided.

Ms REA—So it goes through the cloud.

Mr Littleproud—You can have storage in the cloud. Anything related to IT can pretty much be offered from the concept of cloud computer.

Ms REA—So it is a bit more like a satellite. The information has to go through the cloud to get somewhere else and in that way you sift it or filter it or do something to make sure it is secure.

Mr Littleproud—Yes.

CHAIR—In terms of marketing, 'cloud' sounds a bit insecure.

Mr Littleproud—It has gone up there somewhere!

CHAIR—We have to draw this to a close because one of our members has to scoot off. Thank you very much for coming along. The committee may contact you for further information, if that is all right with you.

Mr Littleproud—No problems. We are going to come back to the committee anyway on the financial model underpinning the cybercrime portal. I have also made a note of the question on whether it has assisted in any prosecutions.

CHAIR—Thank you very much. Before we conclude, we need to formally accept the submission from the Australian Seniors Computer Clubs Association. There being no objection, it is so ordered.

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

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

Committee adjourned at 2.49 pm