



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

**HOUSE OF
REPRESENTATIVES**

STANDING COMMITTEE ON COMMUNICATIONS

Reference: Cybercrime

FRIDAY, 11 SEPTEMBER 2009

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

TO EXPEDITE DELIVERY, THIS TRANSCRIPT HAS NOT BEEN SUBEDITED

INTERNET

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

The internet address is:

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

To search the parliamentary database, go to:

<http://parlinfoweb.aph.gov.au>

HOUSE OF REPRESENTATIVES
STANDING COMMITTEE ON COMMUNICATIONS

Friday, 11 September 2009

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

Members in attendance: Ms Marino, 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

CHISHOLM, Mr Glenn Lindores, General Manager, Network Security, Telstra Corporation Ltd	32
CORONEOS, Mr Peter, Chief Executive, Internet Industry Association	13
HAMILTON, Mr Christopher John, Chief Executive Officer, Australian Payments Clearing Association Ltd.....	70
INGRAM, Mr Graham, General Manager, Australian Computer Emergency Response Team—AusCERT	1
JOHNSON, Ms Loretta Frances, General Manager, Policy and Government Relations, Australian Information Industry Association	24
KANE, Mr Darren, Director, Corporate Security and Investigations, Telstra Corporation Ltd	32
MacGIBBON, Mr Alastair, Director, Internet Safety Institute.....	57
PEARCE, Ms Caroline, Head of Fraud, Risk and Compliance, Australian Payments Clearing Association Ltd.....	70
SHAW, Mr James, Director, Government Relations, Telstra Corporation Ltd	32
SINKOWITSCH, Mr Michael Anthony, Business Development Manager, Fujitsu Australia Ltd.....	47

Committee met at 9.21 am**INGRAM, Mr Graham, General Manager, Australian Computer Emergency Response Team—AusCERT**

CHAIR (Ms Neal)—I declare open this public hearing for the House of Representatives Standing Committee on Communications inquiry into cybercrime. This is the third public hearing for this inquiry. The inquiry into cybercrime will examine, amongst other things, the nature and prevalence of cybercrime and investigate the adequacy of current measures to prevent and mitigate the impact of cybercrime on consumers. Seven organisations representing a cross-section of interests will appear and give evidence today. The committee has scheduled a further two full days of hearings in Sydney in October and will continue to hear witnesses in Canberra until the end of the parliamentary year. The program for these hearings will be published soon.

I welcome our first witness today. Although the committee does not require you to give evidence on 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 contempt of the parliament. Would you care to make an opening statement before we proceed with questions?

Mr Ingram—Yes, that would be fine. First of all, thank you for the opportunity of attending today and discussing a topic that is very dear to me and others. I know you have the submission and I feel that a lot of the information is contained there so I am not going to go through that again. I just want to give some broader comments on questions that are generally asked of me.

CHAIR—You might commence by explaining AusCERT.

Mr Ingram—AusCERT is an organisation—we are not government and we are not industry per se. We arose in the days when the internet was an academic research network. To best explain it, in the early 1990s there were a number of attacks against US defence and other installations from Australia. From what I can determine—I was not around at the time—the history is that the Australian Federal Police and the Australian government wanted these attacks stopped. The Federal Police engaged with the universities, basically in South-East Queensland, and a group was formed which did manage to track where some of this activity was coming from, which led to what I understand were some of the first successful prosecutions in Australia for hacking.

Ms REA—The attacks were hacking—is that what you mean by attacks?

Mr Ingram—Yes. Australia at that time, in the 1990s, had some very high profile hackers. From what I can understand, one of them actually did manage to abort a shuttle launch event at NASA. That is the level that these people were dealing at.

Ms REA—We've always been better at breaking the law than abiding by it!

Mr Ingram—Those romantic days of things like—

Ms REA—The bushrangers of the internet.

Mr Ingram—Exactly. That concept of having a group of people who could look at issues on the internet and fix them continued and basically, from what I can understand, was the genesis of AusCERT. We have been around for 15 years. We are one of the oldest CERTs in the world.

We are not a law enforcement agency and we have no capacity in that sense. The best way to describe what we do is that we are a technical team that looks at attacks and tries to determine how the attacks occur and ways that we can mitigate and stop the attacks. We work very closely with the law enforcement agencies, who are more interested in who is responsible for the attacks and how those people can be prosecuted for their activities. The best way to describe it, I think, is if you can imagine AusCERT as the fire brigade: we put out the fires, we try to understand how the fires were lit and we try to determine how they may be prevented in the future. We do not presume that law enforcement officers are very good at putting out fires and we do not try to do their job. The idea of a fire brigade on the internet is probably what we do.

The other thing is that AusCERT is focused very much on the internet itself. A lot of the security people you will meet—

Ms MARINO—Your engagement—does that include the AFP?

Mr Ingram—Yes. We have a very close engagement with the AFP.

Ms REA—Where does your funding come from, then? Are you contracted by those agencies to do that work?

Mr Ingram—Initially we had funding, but what we developed was a membership funding model. We have a range of members who pay us to provide services back to them. At the moment the whole of the Commonwealth is a member of AusCERT. The whole of the Victorian government, for example, is a member of AusCERT, but also small businesses. We do not have individual memberships. Generally, this is enough to pay our salaries and wages. We are based at the University of Queensland, but we are budget neutral and cost recover on our operations. Recently we put in a submission to the government's e-Security National Agenda review in which we did lament the fact that the level of funding we had to do this work was not enough. The bottom line is that the rate of increase in cybercrime and internet issues is just growing faster than we can possibly meet. So a change is needed and that is now coming through as a different argument. If you read some of the newspapers you will see we are talking to the Attorney-General's Department to try to integrate a capacity. What I am desperately hoping to do is to see that we do not lose a capacity.

Ms MARINO—Do you see that as a positive outcome for you and the services you are providing?

Mr Ingram—All I can say is: watch this space. I would like to see the idea of a partnership with government. A takeover would not be a good outcome because we have 20 people who are literally geeks who do this stuff really well. If you replace those 20 people with 20 policy bureaucrats I do not think you are going to have that good outcome. It certainly will not be an increase in our capacity to do the job. But, again, I think it is probably the taxpayer who needs to make that judgment in terms of an investment well spent.

Ms MARINO—Sure.

CHAIR—We might let Mr Ingram finish his opening statement.

Ms MARINO—Apologies, Chair.

Mr Ingram—Actually I think it is nice because it gives you a feeling of where we are coming from and what our credibility is. I am not here to sell you widgets. I am not here to sell you the latest product that is going to fix the internet. What I am going to say to you is that the question is: ‘Where is this all heading?’ We work very much at the coalface. Everyone else, as far as I am concerned—apart from a few people like the AFP—are back from the coalface. We meet this stuff head on, and unfortunately the view is not good. I can say that it is getting out of control and we are losing. And I think that, with the pressures coming on us over the next few years, if nothing is done to change the current direction we will lose faster.

The things that are probably going to hurt us more, but also give us tremendous advantages—that is the dual nature of the internet itself—are things like the NBN and cloud computing, where a lot of the information that we currently have in our PCs in terms of storage and applications is going up into the internet. These are all things that are going to be an advantage for the criminals as well as for the people who want to use these services. If we continue to go down this road in an unsecured manner then we are simply creating a bigger problem.

Unfortunately, I do not see any way that we are going to solve this, because it is like we are on a drug. The internet is a drug and we cannot get enough of it and we cannot turn it around. We will continue to consume this drug and, unfortunately, that means the problems I would like to present to you are not going to be resolved. One of my concerns is that, when we do not have a solution and we do not know the way forward, it is easier to ignore the problem, and we do that at our peril. I think Mick Keelty put it quite well when he said that the level of crime on the internet almost defies belief. The problem is that it is all under the radar. It is not in the newspapers. It is not in the criminals’ interests to make headlines. Therefore, this whole background level of activity, and the underground criminal economy that has been built on it, continues to grow at an alarming rate.

Ms MARINO—Is it an exponential rate?

Mr Ingram—It is exponential. I have been trying to think of a way of explaining this to people. I have read some of the submissions and some of them are very good. I must admit that I liked what I read. It is as though we are on a boat and the boat is sinking. A lot of the submissions talk about how we have structures in place for bailing—we know how to bail—but, ultimately, the only question that we need to resolve is, are we bailing faster than the water is coming in? If we are not, we are going to sink. I do not know when it is going to occur, but that is the situation we are currently in. In reading these submissions, the question at the back of my mind was: is it going to make a difference? Does it mean that we are getting on top of it, rather than, ‘Yes, we know how to bail or we have policies in place that tell us how to bail?’ The other thing we need to work out is that at some point we have to stop bailing and start fixing the leaks. There is only one solution and that is to fix the problem. There are multiple leaks and there is not one solution that is going to fix them.

That was an image I had in my mind. The fundamental question is that, if we are not getting the water out faster than it is coming in, the cybercriminals are winning. Their motivation for winning is making more money, which is a change that occurred on the internet about four or five years ago. As far as I am concerned, when criminals worked out how to make money on the internet, that was the watershed for the whole nature of crime on the internet. Up until then, we had hackers who basically did it for fame and fortune. They were annoying, but they did not do very much. Now we have dedicated criminals who will most likely never set foot in this country. I have these interesting debates with some of the legislative people who say that we have strong laws. We do have wonderful laws, but a Russian cybercriminal is not going to give a damn about our laws. Because of the way that you can be faceless on the internet, we will probably never identify this person. It is a low-risk, high-gain position for the criminals. Part of our submission, if you look at it, is about the international approach. If Australia does this alone, even if we were to perform a miracle, I do not believe we will achieve much. It has to be a global mind-shift in terms of how deal with crime on the internet, which is a borderless environment.

Ms MARINO—You touched on the global issue, and that you believe the growth is incredible. In your experience, how aware are other nations of the depth and breadth of the problem?

Mr Ingram—That is an interesting question. Particularly over the last two or three years there has been a much greater understanding of it. If you had said how many ‘governments’ are aware of the problem as opposed to ‘countries’, I would say, that, generally, governments are lacking in their knowledge and their understanding of this. Whereas, the UK banks, for example, are very aware of this. Fortunately, the UK government through the House of Lords report—which is an excellent report that I would recommend that you skim—brings out a lot of the issues.

CHAIR—We will need to get that.

Mr Ingram—If you want to cheat and cut-and-paste from that one, it would probably be an excellent way. A lot of the stuff is there. The other report is the OECD report. This is the one that we helped contribute to. It lays it all out; it says what the consequences are. Unfortunately, governments are not entirely across this issue. In some cases their focus is on the state sponsored cyberespionage as being the threat.

CHAIR—Certainly the US has that focus.

Mr Ingram—Exactly. Now that is convenient, because it is much easier as a government to have a foe that you can put a face to and you can actually put things in place. I sometimes ask people: what will ultimately kill you? Is it going to be the cancer or the meteor? What I believe we have is a cancer in the internet that is slowly, but surely, killing. That has to be addressed. Alistair, who is behind me, has said for a long time that we need to look at this more as a public health issue rather than a nation-state attacking, and that we need to have the defences in place and the armed forces ready to defend Australia’s cyberspace. Yes, we need that, but that is not what cybercrime is all about. Also, one of the things that are hurting us is that there is a blur, because a cybercriminal, a Russian or a Chinese might be working on behalf of the state and the state is using the capability that the criminal has put in place. Unfortunately, the internet does not play by the rules. That is one of the complications. The other thing is that, the internet, in many cases, has only been around, in a commercial sense, for about 10 years. That is a minuscule time

to work out how we are going to deal with these issues. As I said before at the NBN hearing, if we had the same compromised computers today and we simply unplug them tomorrow and plug them into a higher speed network, we would have simply escalated cybercrime. That is one of my concerns about the whole nature of cybercrime. The cybercriminals do value speed just as we like speed. That will make Australia a very big target with the speeds that we are promoting online.

CHAIR—You said earlier that you did not really have a solution. Do you mean that literally or do you have some ideas?

Mr Ingram—In our paper we have put forward a few things that will help. Certainly, everything we do reduces the risk and reduces the harm. But if someone asked me, ‘Can we stop cybercrime on the internet?’ I would say no. I have no idea how to do this. The criminals are literally making so much money. There are one or two idiots who do get caught and who are probably not the people we are worried about. My understanding, in talking to law enforcement agencies around the world, is that the people who are really involved in this, are, for example, Eastern Europe organised crime gangs, particularly the Russians and also the Romanians. We are now starting to see Asian organised crime. This is such a fantastic business model for them. The more money they make, and the more opportunities we provide them, the more they will continue to do this. I do not have a solution.

Ms REA—If we cannot come up with broad-scale solutions, often you can at least deal with a problem of this size by targeting some of the key areas that might put a dint in their armour. Is that a possibility? Are you able to break up the nature of the crimes? Obviously you have got the internet but there are different sorts of activities going on. If you are going to choose a particular crime either because of its volume or because of its severity, could you do that to try and take on one element and perhaps at least deal with that rather than a broad-based solution that is really not going to have an impact on anybody? Where would you start, do you think?

Mr Ingram—I could go back to the paper. Let me run through some of the things that I think would work. First, you need to have everyone working together.

Ms REA—You mean law-enforcement agencies?

Mr Ingram—Everyone, because law enforcement agencies cannot address this issue. I am talking about the people who run the internet. We are talking about ISPs, domain name registrars. This whole community needs to be brought together. We need to have a national response, the same way as if we have a response to a pandemic. We need everyone to know what they are doing and having it coordinated. We do not have that strategic approach to this problem currently. But if we can solicit the help of the ISPs, the domain name registrars and the people who run the networks then people like us, the law enforcement agencies, can start to make a difference. If you look at it, the whole problem stems from the fact that the software we use on the internet is not secure. We could start to put in place schemas for creating better software that is harder for the criminals to attack. This will not stop them but will slow them down. So we should aim to have secure software or software that consumers can look at and say, ‘Yes, this is safer than that.’ At the moment you can do that for a car but you cannot do it for a piece of software. Consumers can then have choices based on ‘I would like to have secure software over one I do not know how secure it is’.

CHAIR—Like a star system on software so when people buy it they know how high the security is.

Mr Ingram—Yes. It is part of the approach, the thinking. I am not sure that it will happen but it is part of the thinking strategies we need to start bringing into place. Ultimately malware, which is what the criminals write to compromise the machines, is based on exploiting software vulnerabilities. Ultimately that is what it will do. Then the consequence of the malware is the botnet. The botnet is ultimately the most lethal weapon on the internet. It is where you have multiple machines that are under the control of the attacker. For example, at the moment the Conficker botnet sits around two million machines at any one time. The largest botnet that I am aware of is one the Dutch police took over, so we know exactly how big it is because all the computers phone home that get infected. From what I can work out, the latest report was about 28 million machines that were part of that botnet.

CHAIR—They can use Omnimove.

Mr Ingram—My point is that if the criminals want to flex their muscles there are not many countries in the world that can stand a botnet attack of that order. It does not happen because the criminals get more value by selling their botnets to send out spam. That is why you see levels of spam of 80 or 90 per cent on the internet, because these botnets are now so powerful in sending out spam. Spam is annoying but it is not necessarily going to cause us grief.

CHAIR—That is what I was going to ask you. Isn't the core of virtually all cybercrime spam? Isn't that the starting point?

Mr Ingram—It used to be.

CHAIR—We supposedly have secure firewalls here in Parliament House, but we get criminal type spam.

Mr Ingram—You haven't won the lottery this week?

Ms REA—Several times.

CHAIR—I get about 20 criminal type spams a day, and this is meant to be a firewall. If we are getting that level and there is a whole department that is meant to be monitoring and protecting—

Mr Ingram—What are the mums and dads out there getting and how are they dealing with it? I worry about my dad when we get these spams that really are quite convincing.

The issue about spam is that, yes, most of the spam is produced by botnets and the criminals are renting the botnets out to spammers. That is why spam is becoming more difficult to deal with. But, unfortunately for us, the real criminals who are using the malware have done this: when you get a piece of spam it generally has a link on it and the idea is to trick you into clicking on the link. If you then click on the link you go to a website that hosts the malware, and if you have got a vulnerable browser the malware is downloaded and they have simply compromised your machine.

We can say, ‘Don’t click on links in spam.’ That is a very good policy position to use. Unfortunately, the criminals are now compromising legitimate websites so you do not have to have the spam any more.

Ms REA—So that is why you get the ANZ Bank one or the Commonwealth Bank emails that you know are not legitimate?

Mr Ingram—No—those are phishing sites. Phishing is different again.

Ms REA—Okay.

Mr Ingram—Phishing is a copy of a website that is linked to spam email. In Australia at the moment I believe we look at about four websites per week that are hacked by the criminals, but you do not see any change. They put a link in there that basically takes you to a malware hosting site. For example, if I were going to do this to the Parliament of Australia website, that is what I would do. You do not rely on the spams any more, you rely on the legitimate traffic to and the trust in that website as the means of infecting machines. You have now taken spam out of the equation for compromising machines.

Ms REA—And you have now taken email out of the equation?

Mr Ingram—Yes.

Ms REA—This is about going into a website that you would often go to?

Mr Ingram—Yes. One of the websites that we recently worked with—

CHAIR—I am never using my computer again!

Mr Ingram—Google says that one in 10 websites is currently hosting malware—I can give you the quote. This is deeply concerning to us because while we can say, ‘Don’t click on links in spam,’ if I were to say to you, ‘Don’t click on links on the internet,’ and you follow that through it sort of renders the internet useless.

Ms REA—Yes—what is the point of using it?

Mr Ingram—Yes, and this is what the criminals are now doing. The UK banks, with which we have a very close working relationship, believe that around 80 per cent of the financial-targeting malware, that is the Trojans, that look for those details are delivered by what we call ‘drive-by downloads’—when criminals infect a legitimate website and use that to host malware.

Ms REA—Are these links obvious? They are obviously not obvious to the ordinary user, but when you know the signs are they obvious? If you have got a bank site and it says, ‘Click here to win a holiday in the Bahamas,’ or ‘Click here for information about ...’—

Mr Ingram—No. One of the first websites that we dealt with was the Sydney Opera House site.

Ms REA—So what did they do?

Mr Ingram—I do not know, exactly, but generally what happens is they put a line of code into the website that you will never see. It is the coding behind the website. You open the website in your browser and it basically pulls down the malicious code and your machine is infected. There is no visible sign that anything has changed. This is really good stuff!

Ms MARINO—That is incredible.

Ms REA—And the people who click on the opera house website you assume would be quite reasonably well off.

Ms MARINO—It is a clever target.

Mr Ingram—One of the websites we dealt with recently was one of the top 20 traffic websites in this country, and it was infected for about six weeks.

CHAIR—I suppose you not going to tell us which one it was?

Mr Ingram—No, I cannot—in camera I could probably tell you who it was, and you would be shocked. The problem is that the people who host these websites often cannot deal with it because they have contracted out to someone to develop the website for them, and when we, as AusCERT, ring them up and say, ‘You are currently hosting malicious code,’ they say, ‘Oh, no! We had no idea.’ Generally, within 24 hours it will be fixed and then it will be done again because what they have simply done is loaded the website from backup with the same vulnerability. The criminals are using things like Google to do automated ‘scan and exploit’, as we call it. They look for the vulnerability in the websites using Google. I have had a case where 71,000 web pages have come up as vulnerable. The criminals have automated the attacks so that once found they are automatically exploited and the criminals just get a list of all the websites that are currently available for them to host the malicious code on or the malicious code has been loaded and is currently actively distributing malware.

Ms MARINO—One of the things that is happening in so many households now is internet banking. My question to you is: given what you have said about malware and its prevalence how safe can we as individuals feel about the details that we are using to get in and out of those sites just to do our daily banking and our business?

Mr Ingram—Let me start by saying that we have done survey work where we are estimating about one in six PCs in this country are infected with something. We are not sure what it is; we have not been able to do that level of the survey. That is consistent with what other people are saying.

Ms MARINO—In other countries?

Mr Ingram—Yes. The chances are that that is not the financial trojans, the data-mining trojans. But ultimately as the malware gets better and as our capacity to detect it reduces we can only expect that number to increase. With the banks we are primarily concerned with the integrity of the transaction, because the banks have been fighting this and we have been working

with them for about five years and the banks have some tremendous capability in place. For example, a lot of the work that the banks do is anomaly detection. If I sent \$5,000 to my daughter on a pay anyone transaction, that would probably come up as an anomaly because I only give her \$20 at a time. So the banks have the capacity to say, 'what is this person's normal transaction?' or 'has this person ever looked on to their account from Estonia?' and, honestly, it is quite effective.

CHAIR—Is that operating now?

Ms REA—Yes, it is. I have had a call when there was an overseas transaction.

Mr Ingram—They will do that. Honestly, I have yet to hear of someone who has lost a dollar from internet banking fraud in this country because the banks reimburse the money, so I am not concerned about the transactions. The issue of integrity is something the banks can work with. There are issues of confidentiality, in other words that criminals have access to the transaction data itself. For a banking account it may not be that important. It might be my name, my password and the account numbers. The greater concern we have is with e-business and e-government, because it is when I do my tax return online that I start to give significant personal details. If you look at the internet at the moment and the number of sites and the amount of information they are asking you to provide, for example your mother's maiden name, et cetera. Currently there is no way that we are aware of that you can protect the confidentiality of that transaction if there is malware on your computer.

Ms MARINO—How much of an issue would you believe patients' health information could be? We have talked about banking and touched on e-business and e-government. If we had a lot of medical information, is there an opportunity or a perceived opportunity in that area?

Mr Ingram—At AusCERT we have been trying to draw attention to the fact that this is a significant issue.

Ms MARINO—It is a huge issue.

Mr Ingram—It is critical. But what is happening is that the level of understanding of what is going on is very low, so when we talk to these people generally they say, 'Our backend databases are safe' but that is not the question. If you have two participants in an online transaction, you have the backend database and you have the client's machine. If either of those two is compromised, the data between the two is also compromised. So when the government agency says that their backend systems are secure, it is probably true. But the data leakage and the compromise will come from the client machine, so your machine at home is where the data is going to be extracted from. The problem is that the government and the e-business people say, 'Your machine at home is not my responsibility.'

Ms MARINO—Yes, but the problem is still there.

Mr Ingram—If we as a society are moving people to an online transaction environment, we are basically putting people in a situation where they need to be online to get the work done we need to understand that we are exposing them to a greater level of threat.

Ms MARINO—Creating a vulnerability.

Mr Ingram—We are. Unfortunately, this is where we see a rather large conflict of interest. If you look at many government departments, or businesses, you will see that the cost savings that they have projected into the future are based on getting people online—online transacting. It is like where we were with the banks about six years ago. The marketing people are saying, ‘For God’s sake, don’t tell people that there’s a problem here,’ and the security people are saying, ‘We have to tell them there’s a problem, because if we don’t we’re actually creating a situation’—

Ms REA—Sorry to interrupt. Isn’t that in some ways a good thing, given that we know from the private sector and, indeed, government, that one of the driving forces behind policy is cost-effectiveness? We know that online transactions are significantly cheaper than any other form and there is an inbuilt incentive to spend money on building the security that you need in order to allow people to continue to do that, because in the long run it is a cost benefit to you or your organisation.

Mr Ingram—Exactly.

Ms REA—It is different to other areas where you have to say to people, ‘Go and fit smoke alarms in your house because it will save you,’ but people say, ‘I don’t really want to bother spending the money, because what are the chances?’ At least with this you have the incentive to build in securities for online transactions.

Mr Ingram—I think you have missed the point, though. I agree totally with you in one sense, but, as I said, it is about the responsibility for security of the client machine. In other words, your home machine is not something that a government department can mandate you to secure. If your machine at home is compromised and you do your tax return online, then that data is effectively stolen.

Ms REA—I understand that. What I am putting to you is that, whilst that is not the case now, there could well be an argument that it is actually cheaper and more cost-effective for the government, or whoever it is, to assist you in securing that machine because they want you to continue to do business with them online. If your security is compromised, a crime occurs and you are the victim of it, you will not lodge your tax return online ever again; you will go to a face-to-face situation which, in the long run, costs more money.

Mr Ingram—I totally agree with you on that.

Ms REA—Do you see what I mean?

Mr Ingram—I do. The problem that we have in that sense is that organisations accepting responsibility for the people transacting externally does not happen at the moment.

Ms REA—No, but there is—

Mr Ingram—A need for it.

Ms REA—a need and a benefit to that organisation for doing it, because they want you to continue to use that path.

Mr Ingram—Yes. Unfortunately, at the moment, with the software and the machines we use, we have no way of really securing those computers.

Ms REA—That is the critical question.

Mr Ingram—That is the critical question. What the banks are saying is: ‘If your money is stolen, we will return it.’ That is a good outcome. But if my personal data from Centrelink, CSA, tax—all the things that I am currently asked to do online—is stolen, it can never be returned. People talk about identity theft. If my date and place of birth, driver’s license number and mother’s maiden name are somehow stolen, they can never be returned to me. These things can be used in perpetuity for crime. Unfortunately, as I see it, because it is getting harder to confirm who you are dealing with online, then I as a business will ask you more questions about yourself to see—

Ms REA—That is right. So you are revealing more personal details.

Mr Ingram—You are revealing more. One of the things about cybercrime is that we have not really looked at the privacy issues involved. I think the privacy review that David Weisbrot did—I think last year—was incredibly insightful in bringing the two things together. Ultimately, as a society, if we end up in a situation where just about everything about who we are is exposed to criminals over a period of time, where do we go?

CHAIR—We are going to have to wrap this up now.

Mr Ingram—Sorry to—

CHAIR—No, it has been fascinating.

Ms REA—I have one last question, if I may, very quickly. Is all the antivirus software and spyware that is out there now effective? Or have they gone beyond that? It can be a very brief answer.

Mr Ingram—I hear different figures, but I am hearing that somewhere between 10,000 and 40,000 new pieces of malware per day are being released onto the internet. Part of the work that AusCERT does—and I think this is in our submission—with the malware we get, which is generally very close to release, is to monitor the activity. We see that roughly 50 per cent of the malware is undetectable by current up-to-date AV. The other thing that you need to be concerned about is that criminals are very business-minded. For example, they will test their malware before they launch it. If it is detectable by a market leader, it is going to be an unsuccessful effort, so they will re-engineer the malware. What we generally find is that the market leaders have a lower detection rate than the ones that are less known.

Ms REA—Thanks. That is exactly the answer I needed.

CHAIR—I have one brief question. Bearing in mind that the use of the internet by mainly business and government is compromising the security of information on computers at home, do you think there is a responsibility for those people getting the benefit to fund the fight against that problem?

Mr Ingram—I think there is, actually. I would probably agree with that. It is probably not going to happen tomorrow, but eventually if we keep going down this track we will have to work out how to deal with it. For example, as I think we said in our submission, as a community do we allow large corporate websites to host malware? It is sort of like asking: is it acceptable for business to hand out drugs? I know it is not quite the same, but I would suggest that being on the internet and having a public presence also carries a responsibility. For example, if AusCERT were to ring you up and say, 'You are currently hosting malware,' the response should not be, 'We don't care,' or, 'It's going to cost us too much to fix.' Also all, we do not have a national capacity to detect this stuff. We are not monitoring it. This is not good. If we have a pandemic at the moment we monitor the ports and have infrared sensors on people coming into the country because we are trying to detect it. There is no detection capacity in this country, apart from what is done ad hoc and things that AusCERT do and other people come across. This is what I am saying: we do not have a structured systematic or holistic approach to this problem. This is why Microsoft and Symantec are suggesting that the idea of the cyberczar is a good one because it will bring together a holistic view of dealing with this problem rather than individual government departments running off in different directions.

Ms REA—Did you say a cyberczar?

Mr Ingram—Yes—an industry based authority. So you have that idea, and I think we need to have social responsibilities on the internet which we do not currently have.

Ms REA—Thank you. That was very useful.

CHAIR—Thank you, Mr Ingram. We very much appreciate you appearing. The secretariat may be in touch with you to get further information, if that is all right with you.

Mr Ingram—I am more than happy to help in any way I can. I wish the committee the best of luck and I hope it reaches a useful conclusion.

[10.04 am]

CORONEOS, Mr Peter, Chief Executive, Internet Industry Association

CHAIR—Thank you for making yourself available today. Although the committee does not require you to give evidence under oath, I should advise you that the hearing is a legal proceeding of the parliament and warrants the same respect as proceedings in 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?

Mr Coroneos—Thank you. The committee would be aware of the submission that we have provided to you. I will speak briefly to elements of that, because there are parts of it that warrant a little bit of walking through, so to speak. But, by way of a general introduction, I will begin by telling you a little bit about the association. We are the national industry body for the internet in Australia. We were established in 1995. We have a very broad range of members operating in the ISP sector and in the content sector: companies like Yahoo, Google and Facebook. We also have a number of very important members in the internet security space, companies like Symantec, McAfee and Sophos. So we have a very broad range of inputs that feed into our policy work. As a result, we are able to provide government with a fairly diverse but highly authoritative range of views on these kinds of issues.

The association is a non-profit body. We are funded by our members. Occasionally we get some government grant funding to do certain initiatives. I can talk about a few of the initiatives that we have done in the last few years. I would like to also talk a little bit about the nature of the threats—Graham has covered quite well the basic situation on the ground. More importantly, I would like to focus today on where the areas for further work lie and the kinds of things that we are doing as an association to try and improve the situation in Australia at least.

I think it is fair to say as a general statement that the work that we are doing in Australia is groundbreaking by world standards. It is partly a product of the fact that we have a smaller internet community, but I think we also have a far lower degree of fragmentation as well, so we are able to coalesce support from the industry into initiatives that will have good support and provide a very unified response to some of these issues. I think Australia is in a good position, at least in terms of what we can do domestically, but, as you have heard already today, a large part of the problem does not originate in Australia and therefore we have got to look at what we can do in a defensive capacity as well as things that we can do proactively.

In about 1998, we first identified spam as a growing problem. We lobbied hard for legislation in Australia and in fact helped craft the current Spam Act that was passed in at 2003. That has been recognised internationally as one of the most advanced pieces of regulatory work and—

Ms REA—Why?

Mr Coroneos—Because of the approach that it adopts. It seeks to balance the ability of businesses to use email for legitimate commercial reasons with taking a very conservative view of the kind of permission that we require from users before they are emailed to. In America, the

spam legislation—the CAN-SPAM Act, as they call it—basically takes the position that the default is that any business can email to anybody, even if there is no pre-existing relationship, until the person indicates that they do not want to receive the emails. It is an opt-out system.

In Australia we generally have created an opt-in system, where the presumption is that you do not send spam, or at least unsolicited electronic commercial messages, to people unless you have a prior commercial relationship with them, and even then they have the capacity to opt out of that. So we have opt-in as the default and then you have got exemptions for prior relationships and then you have still got an opt-out capacity there.

As a result of that, we have reduced the degree to which Australia contributes to the global spam problem through the activities of businesses. But, of course, this work that we did from about 1998 through to about 2003 has been somewhat superseded by the rise of botnets, and so we are in a situation now where Australian users themselves may inadvertently be the disseminators of spam, not necessarily—and I would say probably not—originating in Australia but being relayed through Australia using spare capacity on unprotected Australian computers in people's homes.

CHAIR—Do you think botnets are a greater problem in Australia than elsewhere or is it the other way round?

Mr Coroneos—It is hard to judge. The nature of botnets is such that they can be difficult to detect. We have seen some evidence in reports by one of our members, which is cited in our submission, that suggests that Australia is towards the top end of botnet infected countries; but, elsewhere, you see statistics that argue the other way. I think it is fair to say that we are in no better a position in respect of the zombie-botnet problem than any other country. The work we are doing to address that, we would say, is probably a little bit more ahead of the curve, but, in terms of the actual infection rates, there is no reason to believe that Australia should be in any better position than other countries are in.

CHAIR—In terms of a computer being a botnet, is it possible to distribute software that someone could put in and say with absolute certainty whether or not their computer has been compromised? Or would it be technically possible for a site be set up that people could log into and be told whether or not their computer was infected?

Mr Coroneos—I am not a technical person, so I would have to take that on notice, but my initial answer would be no, probably not. Even to the extent that that were possible, as Graham has intimated, there is so much commercial force behind cybercriminals that the more sort of centralised solutions you create, the more likely it is they are going to say, 'Okay, this is the problem we have to solve here', and they basically rout around that. The short answer is that there are no simple solutions to these problems. We need to therefore take a multilayered approach.

Back in the early 2000s the OECD was doing some very good work on cybersecurity. In fact, one of the key committees was chaired by an Australian, Peter Ford, from the Attorney-General's Department. He coined the term 'culture of security'. The idea there is that we have to embrace this idea that, again as Graham has intimated, the responsibility for security does not reside with any particular part of the process—it is not the entire purview of the end user, nor is the role of

the ISP, nor is it the role of government; everyone bears a responsibility here. I think the work that we are doing is really designed to work hand in hand with other initiatives that are occurring, within government and through the commercial efforts of our individual members, and then through what we can do collaboratively as an association.

I might just talk you through some of the things that we have been doing in the last 10 or 12 years in this area. I mentioned the spam legislation. We complemented that with a national anti-spam campaign whereby we worked with those of our members that were providing anti-spam software that you could put on your computer, to provide free trial software to all Australians. We had a lot of media coverage of this, and we had a high degree of responsiveness from people who were worried about spam. The basic model is that the association provides a unified place where people can go. We have a range of products that people can access from there. We have fact sheets, information and other empowerment methods whereby we provide people with some protective services and information. We have applied the same model to spyware, which is a related problem; it is a form of malware. We have also done this for viruses. So we have really had three campaigns in the last 10 years addressing each of those elements.

Earlier this year we launched what we called National Zombie Awareness Week, in recognition of the fact that the problem has now moved beyond just the individual computer to these entire networks of compromised machines. It was largely intended as an awareness raising campaign. We took on a fairly light-hearted approach, because we thought that it is necessary not to terrify people with this but to actually show them that there are solutions available. The balance that we are trying to strike here, of course, is that we have to maintain trust and confidence in the use of the internet in Australia—that is paramount—but equally we have to be honest about the nature and extent of threats and then work towards providing solutions that will address those things. So that is the balance that we are trying to strike.

Importantly, we have commenced work on an e-security code of practice—in fact, the first consultation draft will be launched today. I will talk through that a bit, because that is a world first; it is something that has not been done in any other country. Zombie week was also a world first. The extent to which you can get groups of competitor companies coming together to support an initiative seems to be a thing that is unique to this country. In other jurisdictions, you have individual companies doing that, but it is quite a rare thing to have a whole sector come together in the national interest, as it were, in order to try to promote awareness.

The e-security code of practice that we are currently developing is primarily addressed to ISPs; it is about recognising that there are an increasing number of zombie computers on the networks of ISPs in Australia. You have heard some statistics today; there are statistics in our submission as well. We have heard numbers from ACMA, the Communications and Media Authority, that there are in the order of 10,000 reports per day of active zombie computers in Australia. The numbers are very hard to pin down, and I would caution the committee not to get too thrown out by different statistics that they might hear. That is not the point; the point is that it is a large and growing problem.

ISPs are concerned that having zombie computers on their networks is not only a threat and a problem for their customers but also a threat and a problem for the integrity of the network itself. There is a high degree of self-interest in the sense that the ISPs see a win-win benefit in engaging in this initiative. It comes off the back of work that ACMA has already been doing for

the last three or four years under the aegis of the Australian Internet Security Initiative. Essentially, that involves ACMA applying forensic tools, scanning tools, to networks, where they can get evidence that a certain IP address—that is the internet address that computer users each time it connects to the network—indicates activity suggesting that it has been compromised. For example, if an IP address seems to be sending a lot more traffic than it is receiving, that could be indicative of the fact that it has been infected and that it is being used as a zombie to send spam or to engage in a denial-of-service attack against a website. In that instance, ACMA notifies the ISP—there are lists in Australia you can look up and see which IP addresses are assigned to which ISPs. So, if it is within a certain range, you might say, ‘We will send this ISP a notification letting them know that we believe that there is this compromised computer or computers on its network.’ Then the ISP notifies its customer, saying, ‘We have reason to believe that your computer has been infected.’ In fact, different ISPs do different things at that point—

CHAIR—Is this already operating here?

Mr Coroneos—This is already happening in Australia.

CHAIR—So customers are sometimes rung up and told that there is something wrong?

Mr Coroneos—Yes. They are receiving either phone calls or emails from their ISPs saying ‘We think there is a problem with your computer,’ and then being directed to resources where they can have that problem fixed. It has been happening in a bit of an ad hoc way, but I do not mean ad hoc in the sense that you are not getting broad cooperation from ISPs; there are about 68 ISPs now cooperating in that scheme, including some of the major ISPs in Australia.

CHAIR—But there would be many more than 68 in Australia.

Mr Coroneos—There are indeed, but those 68 would probably be providing in excess of 80 per cent of internet services in Australia, so we are coming off a pretty good trajectory already. But, with this code, we are trying to systematise the messages that the consumers are going to be getting in those situations so that we can have some standard language that people will get, irrespective of who their ISP is.

We are also creating a branding scheme through the use of a little tortoise logo. It will be a voluntary code, but we expect a high level of uptake because of the self-interest that I referred to earlier. The ISPs will carry a little tortoise on their websites, and that will signify to their customers that the ISP is security aware. When the user clicks on that little tortoise on the ISPs website, it will take them to a standardised information page. We will create that as an industry body, but we are also saying that if ISPs want to take that and brand it themselves they can—some would prefer to do that. But, particularly for the smaller ISPs, we want to alleviate the workload of having to craft an authoritative, up-to-date page that people can be directed to. That page will contain basic information answering questions such as: what is wrong with my computer? How do I know that I have been compromised and what steps can I take to remediate that?

In particular, we are very interested to work with a couple of companies in Australia that have been set up and do house calls for people. They do it to help people set up computers—generally to get them on the internet—but they are finding that, more and more, they are getting demand

for people to help them get spyware off their machines, clean their computer and basically ‘unzombie’ them, as it were. Part of this approach will be to provide resources where people can go to get their computers sorted out. There will be a charge for that. It is like when your washing machine breaks down and you call a serviceman. We are not putting that cost on the ISP—it is clearly not their responsibility that the user has been infected—but we are at least getting the cooperation of the ISPs to be the conduits, where they can convey to the user (a) the fact that there is a possibility of an infection and (b) something they can do to get it fixed. This is a very unique approach that we are taking in Australia.

Beyond that, the remediation piece, the final piece, is the reporting element of the code. Where it becomes evident that there is a major problem on their network, affecting more than just a few computers—let’s say there is evidence of some sort of systematic attack occurring on their network—we are encouraging ISPs to report to a central authority. At this point it will be Graham’s organisation, AusCERT. The idea is that we want to create a situation where we can feed into a centralised body a whole lot of disparate intelligence which, taken individually, might not suggest anything, but when it is viewed in aggregate could very well be suggestive of a cyberattack against Australia, in the context of a state sponsored attack or something of that nature. So this actually goes beyond e-commerce and takes us into the sphere of national security. We are working with the attorney-generals on the creation of this code as well, because they see some great advantages in this pioneering work that we are doing. I just wanted to come here today and convey to you this important initiative.

Ms REA—It is very interesting.

Mr Coroneos—We have no budget for this kind of thing. We are doing it out of our own resources. We got a little bit of funding from the Commonwealth to just get the program going, but I think—

CHAIR—Through ACMA?

Mr Coroneos—Through the Department of Broadband, Communications and the Digital Economy. That was some seed money which has now been exhausted. Everyone comes to parliamentary committees asking for money, but in this case we believe that we can be much more effective in the work that we are doing on a voluntary basis, where we can see some ongoing funding support from agencies that see that they have an interest in our scheme being successful. In particular, we want to do a big promotional launch and get people—

CHAIR—You are funded by your membership now—

Mr Coroneos—Just by the industry—yes—but we are not well-resourced. We run on a shoestring. That is often the case with non-profit associations. We have a lot of great ideas, skill, expertise and innovation, but where we typically fall down is that we just do not have the momentum to necessarily take this to the depths that we would like to see occur if we were a bigger organisation or a better funded organisation. Be that as it may, it will not deter us. For the record, I would at least like to say that any funding support would be appreciated.

CHAIR—We have noted it down.

Ms REA—‘Money’.

Mr Coroneos—I did not come here today to ask for money.

Ms REA—Never miss an opportunity.

Mr Coroneos—Yes. Moving beyond that specific initiative, I would like to talk a little bit more about education. Members of this committee have raised the question: how well do you think people are aware of the threats? The answer, of course, is: not enough. One of the things we have observed in the past is that the government has engaged in awareness campaigns. An example is E-security Awareness Week. We think more needs to be done in that way. One week a year is not really going to be enough to generate the kind of behavioural change that we think is necessary. It is not enough to make people aware. You know human nature: people have the overriding predisposition to say, ‘It’s not going to happen to me,’ until it happens and then it is too late.

What do we do to get people to modify the kind of behaviour that they are already engaging in, before something bad happens to them? How do we go from awareness raising, and beyond awareness raising, to avoiding the kinds of risky behaviours that are going to increase the likelihood of their machines being infected? Secondly, how do we get them to take responsibility for their part within a general culture of security? We have to think clearly about how we can achieve that. In the past we have seen public campaigns in the health arena: there is a lot of work happening in the antismoking arena, we have seen a lot of work on AIDS and there is the SunSmart initiative with primary school children. I think we as an industry can learn from established campaigns that are targeted towards engendering behavioural change. That is where a lot of the effort and thinking from both government and industry have to go.

CHAIR—If there were a campaign to change behaviour, obviously the first step would be to ask what behaviours needed to be changed and what way they should be changed.

Mr Coroneos—Indeed. As much as we acknowledge that there are going to be some elements of the threat here, education and even behavioural change are going to be difficult to address. Nevertheless, there is what we might call the low-hanging fruit. There are clearly things that people should be doing, and should not be doing, right now that the evidence shows they are not. An example would be keeping your operating system patched and up to date. Whether you are on a Windows system, a Macintosh system or a Linux system—or whatever operating system—as Graham said, the criminals make a living out of employing highly skilled computer technologists to identify flaws in existing operating systems. Remember that these operating systems were never built for the current security environment. When the internet was invented it was a means by which academic institutions could share information and research and military institutions could maintain a decentralised command and control structure. That is what the internet was for and only been since it became a mainstream medium have these security issues become an issue. What everyone is trying to do is to retrofit security into a medium that was never designed to be secure because it never had to be.

The kinds of behaviours we want people to engage in are these. We want people to patch their operating systems so that when a flaw becomes identified by the manufacturer there are automatic updates that you can have installed on your machine. We want people to understand

how that can be done. It is not difficult stuff but it is stuff that you have to be vigilant about. Again, it is a bit like the road safety analogy: we all have a duty to keep our cars roadworthy, to ensure the brakes are working and the tyres are not bald. It is the same thing when you are online. You have to make sure that you have antivirus software installed, operational and updated; you have to make sure that your operating system is patched. Then we go to the next level: what kinds of behaviours are internet users engaging in online? Are they visiting sites that might be a little bit dubious or downloading things?

CHAIR—How can you know they are dubious?

Mr Coroneos—That is part of the problem. The early file-sharing programs—that is, peer-to-peer file sharing—that kids use were notorious for including malware in downloads, so one of the messages is, ‘Be careful what you download.’ Kids do not have the level of caution that comes with age—

Ms REA—That is true.

Mr Coroneos—We have to try and get them across to the idea that they have to engage in safer online behaviours.

Ms MARINO—I would like to ask about the point of sale—that is, the point where someone buys a computer and away they go. What level of information is provided at that point to the purchaser about what the vulnerabilities are? Do you believe that there should be more information provided to someone who is updating their equipment or buying a computer for the first time? Do you believe that there is a real need for more information at that point?

Mr Coroneos—Absolutely. This is where we need to be lateral in our thinking. We need to look at every point in the chain from the initial purchase of the computer through the setting up of the computer to the ongoing usage of the computer. Each of those points represents an opportunity for awareness raising and behavioural change.

At the point of sale, another initiative we are working on is to do with the sale and configuration of routers or modems that people put in their homes when they connect their computer to the internet. A router or a modem is a device that sits between the computer and the internet. These days many of them are wireless. You can set up a wireless network in your home. But, in any event, the evidence is that many of these routers come preconfigured with a default password. The username might be ‘admin’ and the password might be ‘useradmin’—just a range of generic words. Many users never change those defaults.

There was an exploit that occurred in Australia about four or five months ago called ‘psyb0t’. This is a naming convention that hackers often use where they torture the language to invent a word that is somewhat geeky and cool.

Ms REA—At the same time!

Mr Coroneos—At the same time. In the early days of hackerdom there were a lot of what they call ‘bragging rights’ where young hackers could move satellites or do certain things and

they got their thrills from the notoriety in the hacker community for doing that. You saw many of these kinds of words back then.

CHAIR—Impressing your own gang.

Mr Coroneos—Exactly. They have their own names—their own handles, they call them—where people come to recognise that this person is very competent. But it is more of a demonstration of their own prowess as a programmer.

Ms REA—It is a tag.

Mr Coroneos—Exactly. That was the name of the game back then and they were called ‘script kiddies’—script being computer code. They were the young people who were writing new code that could do these naughty things. Nowadays, of course, we are into full-on commercial fraud and organised crime, so it has moved beyond that.

Returning to the psyb0t example: this is what is called a ‘worm’. It is a kind of computer program, a piece of code that can go in and break open the security of a router or a modem. Basically it hijacks it. You might have great antivirus software and an up-to-date operating system on your computer, but if your router has been compromised you have no way of knowing that that has happened. You are doing all the right things that we have taught people to do but, notwithstanding that, there is a vulnerability there, which means that the unprotected router can have its own firmware upgraded to turn it into an attack machine, or at least to take control of the computer transmissions and render them under the control of the third party. You would have no way of knowing that that has occurred. That is an imperfect explanation of what the problem is.

What is the solution? Again, we are looking for behavioural change here. We want to educate people that when they first buy their router or modem and set it up, the first thing they do is go in and replace that password with what we call a strong password. So instead of it being ‘admin’ and ‘admin’, it might be your name. That is not a problem but the password itself should have a minimum of eight letters, characters, numbers, exclamation marks, hatch marks, uppercase and lowercase—things that are hard for people to guess. The bad guys are not silly. They will always go for the low-hanging fruit. If we can at least raise the layout of protection another level, we have eliminated one source of the compromise, which is currently not being done.

How we are attempting to do this is through direct cooperation with the manufacturers and distributors of those modems. When I get back to the office I will email the committee a sample brochure that we are writing to have included at point of sale when the routers and modems are actually sold. It will again carry the same tortoise logo, so we are trying to integrate this whole branding idea of security through the ISP, through the router and modem manufacturer. The idea is that you will sit down and it is a three-step thing. Before you connect this device to the internet, we want you to change the password to a strong password; we want you to write it on the sticker with the tortoise on it, we want you to peel it off and stick it on the device so that if you ever have to go and reconfigure it you are not calling the manufacturer or the ISP saying, ‘What is my password?’

CHAIR—Couldn't you set it up automatically? I mean, these days when you put on new hardware the computer automatically sets it up for you. So you could actually incorporate in that automatic setup process 'Change your password here'.

Mr Coroneos—In theory yes, but the problem is that security cannot be mass-produced in this way. What we are trying to do actually achieves two things. Automating it would add to the costs of the setting up of the router and modem. It would also add to the support costs, because by having a default there it means that the manufacturer is able to ensure that the thing will be able to work when you first plug it in. But by getting the user to go that extra step it is giving them a sense of responsibility that now they have got to have done something before they can go online. I think inherent in your question is the risk that if everything is done for them they might begin to feel that they do not have to do anything.

CHAIR—The trouble is that there is a very large number of people who use computers these days who can use it as in type and go on the internet but really have no comprehension of how it works, how to control it, how to fix anything. And even just changing a password I would say there would be a large number of people who would think, 'That is too hard.'

Mr Coroneos—Let me show you the brochure. You will see that we have worded it in a way that even your grandmother could do this.

Ms MARINO—Some are really good at it, you know.

Mr Coroneos—Indeed. Look, it is one thing that we are trying to do. We have looked at the automated approach but we have arrived at the view that for a variety of reasons this is not a difficult thing to do and I think it will get people starting to think a bit more about things that they need to do themselves. As I say, this will not be an initiative that sits in isolation; it is something that will work in conjunction with the e-security code of practice and the awareness raising and other work that is being done elsewhere. It is an example of the layered approach that we are talking about.

CHAIR—Do members of the committee have any questions at this stage? No.

Mr Coroneos—I will use the last five minutes just to talk about some other areas where we think improvements can be made. In our submission we gave an example of a recent court case where a hacker was apprehended, charged, prosecuted and convicted but let off with a fairly light penalty. We are concerned that the signal this sends to the hacker community is that, notwithstanding that we have got a very good piece of legislation in the Cybercrime Act, if you go before a magistrate who does not have a good technical understanding—and I am not saying that is what happened in this case specifically, but you may be able to make a case that 'I was just playing around. Nobody was hurt. I'm just a young kid, go easy on me.' We think that the threat is far more serious than that and we think it is important that if you have got legislation as we have that carries with it jail penalties of up to two to three years that we need to provide some better guidance for the judiciary in terms of how they sentence in instances where the potential severity of the conduct goes beyond victimless crime, so to speak. That is one observation that we would make, that there is support within the industry. They were pleased that the person was apprehended but they were dismayed at the relatively light penalty. I think they got a \$150 fine and a 12-month good behaviour bond when in fact the legislation, as I say, provides for

imprisonment. We are not necessarily saying this person should have been imprisoned, I am not commenting on this case, but I think that is the fear that you have.

Ms MARINO—Is part of your fear the fact that magistrates and others need to also have a greater level of information provided to them, not just more information as to the law itself in its current form, but also as to what the crime is and what the potential is? Is that what you are alluding to, not just the law side of what they have available to apply, but also the other issues surrounding that?

Mr Coroneos—If we are calling for sentencing guidelines, I do not think it is inappropriate to call for judicial education as well. Having said that, we work with many people in the legal profession and we are not under any misapprehensions as to the workload that magistrates labour under. Perhaps—and it is not in our submission but is a thought that just occurred to me—there could be consideration given to the formation of specialist courts that could be better trained and equipped in dealing with instances of this kind.

CHAIR—It is similar in relation to the investigation of cybercrime around Australia. I have a particular example of a person who complained to me about losing an amount of money that they thought was a lot, but it was less than \$1,000. They went to the police, who took it all down, but they did not really have any capacity, technical or otherwise, to investigate it. There is a higher level internet or cybercrime type operation in New South Wales but they only deal with the really important crimes and they are not going to waste their time on something less than \$1,000. I guess I was wondering if you have any ideas of how this sort of crime can be more effectively investigated and prosecuted.

Mr Coroneos—This might be a good question to put to my colleague, Alastair MacGibbon, who is giving evidence this afternoon as a former law enforcement agent. My only observation would be to point to the example that we have put in the attachment of our submission where we de-identified a report that we got from one of our members that had exactly that situation where they went and reported a cybercrime to the police. They were told that they had to go back and report it through the local police station and of course the local police station did not have the first clue about any of this. As helpful as they were, I think the member felt very underserved by the way in which they were responded to. More particularly—where do people go? That would be a very fair point if the committee were to arrive at a view that we need a more customised point of contact where people can go in this situation. We have the Australian High Tech Crime Centre, but as you point out it is for the larger crimes. We would certainly support moves in that direction.

I realise I am just about out of time. I would like to talk about a couple of other issues. The National Broadband Network, the NBN, is a huge infrastructure project and one that we have lobbied for. We were pleased when this government picked up our targets and built them into the policy and has now gone far beyond that. It will absolutely revolutionise the internet in many aspects of our society, there is no question in our mind about that. But by putting everyone on a very fast connection we increase the level of vulnerability exponentially and increase the level of damage that can be done if we do not adequately secure the network.

We would probably have to take advice on how this could be done, but our starting point is that we believe that an allocation out of that \$43 billion should be put towards ensuring that, to

the greatest degree possible, this network should be built securely so that we are not going backwards. If it were 30 years ago and we were looking at building the internet as it then was knowing what we know now, we would have built much more security into the way it was being done. Here is an opportunity to start again and we are putting it out there that \$1 billion or two per cent of the budget for the NBN should be dedicated towards making it as secure as possible and building that security into the network.

Finally, the point about a national coordinating body, the cyberczar as it is called, certainly warrants consideration. It was raised by two of our members, Symantec and Microsoft, in their submissions. It is a model that has worked in the United States. The cyberczar has typically come from industry. I think there is a lot to be said for having—

CHAIR—Would that be a person or an organisation?

Mr Coroneos—It would be an organisation, but it would be headed by someone that would have industry experience and an appreciation of the rapidly moving nature of these problems. We still seem to have a degree of fragmentation within government, even around who has responsibility for cybersecurity. I know that the Attorney-General's Department plays a very large role in this regard, and also the Department of Broadband, Communications and the Digital Economy. I would anticipate broad support in the industry and in the community generally were the government to think about a dedicated department or organisation whose purview was cybersecurity, cybersafety and cybercrime. It has become such a specialised area now that I think it warrants that degree of attention and funding. That really concludes my evidence.

CHAIR—We really appreciate you coming along very much. The committee may be in touch with you to get further information, if that is suitable for you.

Mr Coroneos—I would be happy to provide that.

CHAIR—Thanks for your effort in coming here today.

Proceedings suspended from 10.46 am to 11.07 am

JOHNSON, Ms Loretta Frances, General Manager, Policy and Government Relations, Australian Information Industry Association

CHAIR—I welcome the representative from the Australian Information Industry Association. Thank you for making yourself available, particularly dealing with your situation where I understand you are here on short notice because the CEO has been struck down.

Ms Johnson—Not fatally, Chair. It was food poisoning.

Ms REA—Don't we have software for that!

CHAIR—I think we will move on from that. Although this 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 parliament. At the conclusion of your evidence please ensure that Hansard has had the opportunity to clarify any matters with you before you leave. Would you care to make an opening statement before we start with questions?

Ms Johnson—Yes, a very brief one; thank you, Chair. AIIA commends this government for establishing the review into the incidence and impact of cybercrime on users and the Australian economy. Thank you very much for inviting us to appear before the committee this is morning. Again, on the record, my apologies for my CEO's absence.

Our members are both users and providers of the products and services that go to make up cyberspace infrastructure, and as such they are acutely aware of the critical need to balance online safety and security with the increasing consumer and business demand for innovative service delivery and fast, unfettered online engagement. Expectations of free and open access to this internet environment stem from its genesis as a totally inter-operable architecture but not necessarily a secure one. The internet has democratised the use, creation and dissemination of all types of information and, relative to other types of infrastructural platforms, it allows use almost without permission or regulation. Social and economic commentators now assume that the use of, and reliance on, ICT—information communications technology—will become more pervasive in the future, at least in most developed economies.

The productivity, efficiency and economic growth advantages that can be delivered by our rapidly developing digital infrastructure are recognised by governments and users alike. The secure and safe use of that infrastructure should be a focus for governments which are concerned with enhancing their nation's GDP for the benefit of their own citizens. If that focus is lost, users will lose confidence in the internet as a business and commercial tool, leading to a consequent decrease in the efficiencies and productivities that digital engagement can deliver.

Conversely, we note in our submission that overzealous regulation or restrictive technological protection mechanisms may similarly reduce digital engagement by discouraging legitimate online users who are traditionally accustomed to the unfettered access I mentioned before. This is mainly an issue in online retail activity. This may, in turn, have consequential impacts on

smaller businesses, which are currently trying to digitise their activities. AIIA is aware that this government now has a development underway to encourage small businesses through the Small Business Online program.

AIIA welcomes this government's decision to take an ongoing and vigilant approach to safety and cyberspace security. That said, there will always be ill-intentioned individuals with access to increasingly sophisticated attack tools. So we consider it is neither practicable nor possible to prevent all types of cybercrime, at all times and in all circumstances, just as it is impossible to do with traditional mainstream crime. But we do believe that consumer and user education, awareness and understanding must be pursued with vigour in collaboration and engagement with the industry so that a more responsible individual ethos develops in preference to shifting all the responsibility to government, to suppliers, to providers or to a mixture of all three.

Cybercrime and internet abuse know no borders. Detection of perpetrators is notoriously difficult because attacks can be launched from any geographical jurisdiction in the world. As well as being a truly international platform, the digital space facilitates anonymity, which is a great advantage for criminal activity. Certainty of detection, notwithstanding the acknowledged difficulties, will likely be a more potent deterrent for would-be criminals. Any efforts to coordinate international jurisdictions, legislative and administrative regimes would send clear signals to cybercriminals, we believe, that the international community is serious about reducing opportunities for crime. In this regard, as we have said in our submission, we urge the government to move towards signing and ratifying the Council of Europe Convention on Cybercrime, which is a model legal framework and has already been adopted by 26 countries including our major trading partners.

A significant element in the range of cybercrime activity is the need for criminals to assume identities so that they can then commit traditional crime such as fraud. If identity theft were to be made an offence in its own right, we believe law enforcement agencies might have a better chance of success in detecting and prosecuting this prerequisite to wider cybercrime activity. At the moment, it is not an offence in Australia, with the exception of South Australia and Queensland, to steal another person's identity. AIIA welcomes the government's introduction earlier this year of new measures to criminalise identity theft. We are hopeful that the bill currently before parliament will in fact become law before year's end.

AIIA's role is to lead and represent the ICT industry in Australia to maximise the potential of the Australian economy and society. Our members constantly focus on customer education and awareness of the risks and threats surrounding the use of the digital infrastructure and the applications that sit on it. Many members and key industry players conduct regular in-depth trend analysis of cybercrime and its characteristics. Collaboration and engagement with the industry will assist governments to manage the increase in crime we are now seeing. Our membership encompasses all sectors of the ICT industry including hardware, software, services and telecommunications. Our members employ over 100,000 Australians. We generate combined annual revenues of more than \$40 billion a year and export more than \$2 billion in goods and services each year. Our members include senior CEOs and management of major multinationals such as Microsoft, IBM, Google, Fujitsu and Intel. We also have large local Australian organisations on our board and in our membership such as Telstra. That is the conclusion of my statement.

Ms MARINO—Considering those whom you represent and what we have heard here previously regarding the issue of the vulnerability of existing software, do your member organisations today have a position on that particular issue?

Ms Johnson—The vulnerability of their own software or software generally?

Ms MARINO—Software generally.

Ms Johnson—As I said in the opening statement and I hope we made clear in the submission, those members such as Microsoft, IBM and the others are constantly working to improve their own position in relation to software vulnerabilities and, as I said in the statement, are also conducting a lot of analysis on the characteristics of those vulnerabilities and how best to (a) fix them and (b) educate the customer.

Ms MARINO—Educating new customers or existing customers?

Ms Johnson—Both, usually through learned papers and, as I said, industry and market analysis—that sort of thing. They are very active in that area.

CHAIR—You have talked about the Council of Europe Convention on Cybercrime. Obviously your organisation must think it is quite effective. Would you tell us how and why you think it is effective and what benefits there would be in Australia signing the convention and, of course, ratifying it.

Ms Johnson—I am aware that the Attorney-General's Department is looking into this issue at the moment. What the convention does is normalise all the jurisdictional approaches—in other words, coordinate all of the legislative approaches in all the jurisdictions so that they all roughly do the same thing. My understanding from reading the Attorney-General's submission is that at the moment there are some domestic Australian national laws which would need to be altered or changed to fit within the framework of the convention. I understand that is what is holding the Australian government up. But the benefits of these sorts of conventions are twofold. As I said in the statement, they will send a message, hopefully, to the international criminal community that these 26 or more important jurisdictions are serious about coordinating the legislation, not by making it all the same in every country but by making it work in similar ways so that the internationalisation of cybercrime can then be nationalised in the sense that the US approach will be the same as or similar to the Australian approach, the Japanese approach, the Canadian approach et cetera. So wherever they go there will not be, we hope, legal bottlenecks to catching, prosecuting and charging them.

CHAIR—It would allow us to prosecute people across borders?

Ms Johnson—If you could find them. We are not saying it is a silver bullet, but it is a leadership position for nations to take. It is, as you know, the accepted international legal mechanism for nations to act as one—we frequently have conventions on human rights et cetera. The only reason we are suggesting it is to get in with our major trading partners to send that message and to take a bit of leadership.

Ms REA—Does it cover countries other than in Europe? Obviously it is the European convention—

CHAIR—There are 23 countries.

Ms Johnson—There are 23 or 26 that have signed and ratified. I did not bring the list with me, but I could send it to you.

Ms REA—Would we be the first non-European country if we signed the convention?

Ms Johnson—No, Japan is a party, as are some of the other Asian countries. As you know, anyone can sign and ratify a convention—it is open to the world.

Ms REA—Are any of the eastern European countries signed up, given, I guess, the general area from which a lot of this crime is occurring?

Ms Johnson—Off the top of my head I do not know, but I can find out for you and send the list of 26 nations to you.

CHAIR—I am very interested in your suggestion of making identity fraud a crime. In fact, I would have assumed—

Ms Johnson—Identity theft. Fraud is already a crime.

CHAIR—I would have assumed that that was a crime already, frankly. I am quite surprised.

Ms Johnson—So did we.

Ms REA—How is it defined? Is it simply if you have information about another person in your possession? Is that theft? How do you define identity theft?

Ms Johnson—If I go to your letterbox and take a letter addressed to you—apart from the fact that I would be trespassing; putting that to one side—and then take your identity and introduce myself to the chair as Kerry Rea, having stolen your name, that in itself is not a crime yet. As you know and as I said in the statement, there is a bill before—

Ms REA—So it is not fraud that you are pretending to be me?

Ms Johnson—No. If I then use it to say to the chair, ‘You owe me money,’ or whatever and I defraud you of money by using your identity, the fraud is the crime. What we are hoping is to go back in that chain so that my taking your name or your identity does become a crime. According to the law enforcement agencies we have spoken to, it would make it a lot easier for them. Identities are stolen now through letterboxes, and then I can go and say, ‘I’m Belinda Neal and I’ve lost my drivers license. I’d like to get another drivers licence.’ I will have some points for identity as soon as I get that licence. If you work upwards you could get 100 points of identity and become another person. That is happening now.

Ms REA—It is a crime to steal something out of someone’s mailbox.

Ms Johnson—Yes, because you are trespassing.

Ms REA—But it is not a crime to take it off the internet. Is that the difference?

Ms Johnson—Correct, if you can get the identity off the internet. It will hopefully be a crime by the end of this year. It just clarifies the situation for the law enforcement agencies.

CHAIR—You said ‘by the end of this year’, so you are saying that is included in the bill that is before the parliament.

Ms Johnson—That is my understanding.

CHAIR—You say that your organisation spends a lot of time in education and training.

Ms Johnson—Our members do, through their engagement with their customers and also through writing the learned papers that I referred to earlier.

CHAIR—How far do you think that should go? Should people be required to be trained in relation to cybersecurity before they work in the industry? Should they be certified that way?

Ms Johnson—By working ‘in the industry’ do you mean repairing people’s systems and that sort of thing?

CHAIR—Should anyone who works in the IT industry be required to have a certificate that says they are trained in internet security?

Ms Johnson—If they are working in an area that is relevant to internet security then I would assume that the market would determine that they have to be. Our members would not hire people who are not qualified in that area, and hopefully government would not hire consultants who would not be certified in that area either.

CHAIR—But there is no formal qualification for awareness of cybersecurity.

Ms Johnson—I will check whether the Australian Computer Society has certification courses for that. It is a good point.

Ms MARINO—Regarding identity theft, the amount of information that some young people put onto social websites is extraordinary and it is there for anyone, even in a social sense, to access. What is the view of your members on managing the security issues around this? We have touched on identity theft in a physical sense, but how would you see that being dealt with in what we are discussing as a committee?

Ms Johnson—The social-networking platforms have come a long after my formative years, so I am not social network user or expert. However, it seems to us that, as with all cases of knowledge, education of those younger people would be a good first step. It is not necessarily just the government’s responsibility to educate the community. It is obviously a layered approach and a matrix approach. We all have a responsibility to educate those young people. That said, our observation is that their attitude is one of, as I said earlier, completely unfettered and unregulated

access to this platform. I am not sure whether they feel they are bulletproof or whether they do not care. They are not in a situation where, like businesses or government, they can see that anyone can do any harm to them. Obviously that is a seriously incorrect assumption on their part. We believe that they need to be educated out of that bulletproof, 'I'm immortal' sort of attitude that they might have to social networking. That said, because it is such a pervasive platform it is extremely difficult for governments, which is why we do not believe it is just the government's role to do this. It needs a layered approach and we all need to work in collaboration to address that issue.

Ms MARINO—We could have some form of education process through schools. It probably needs to get to that level.

Ms Johnson—Correct. I believe you are hearing after this from one of our members, Telstra. Their submission gave examples of nationwide education programs that governments have done in the past, such as those for GST, decimal currency—I can still remember how pervasive that education program was; surprisingly enough I can still sing the jingle!—and Slip Slop Slap. It is not beyond our ken to do this as government and community.

So I think that is an extremely good suggestion that Telstra made in their submission. It is surprising how powerful those nationwide education programs can be. The one that you have raised is possibly a very good example of where that would help, particularly if you did it on the platforms that they understand—not necessarily just through the print media or television; my understanding is that they are not platforms that younger people are familiar with or care about. It would be through the platforms that you have just mentioned—the social networking platforms. Then it comes right up in front of them: 'Do you realise that ...'

CHAIR—It is almost happening by default through schools—

Ms Johnson—Is it?

CHAIR—because, with the rollout of these computers in schools a lot of the training they are putting in place before students can get issued with computers requires them to go through that sort of process.

Ms Johnson—I was not aware of that. That is a very good development.

CHAIR—I am speaking about New South Wales, where I come from. I do not know about the other states but I would be very surprised if other schools were not doing the same thing. Almost coincidentally, it appears that that is happening in our schools. That is in the age group of 15 or 16.

Ms Johnson—That may well be a bit late—I am not sure—but it is certainly better than nothing.

Ms REA—I guess I was a little interested in the convention—not just the signing of it but because we are always keen not to have to reinvent the wheel. So if there is already a convention that is useful that we could sign up to then I think we should. I am just interested to know: is it

just good because it is the first multi-nation convention that has been signed or is it good because of its content?

Ms Johnson—That content is good. It is brief. I attached a copy of it to the submission and I am happy to send it again if—

Ms REA—What obligations come out of it? Obviously, with most conventions there are obligations—

Ms Johnson—As with other conventions the obligations are to get your own legislative house in order.

Ms REA—Right.

Ms Johnson—And my understanding, from talking to AGD here is that that is what they are trying to do.

Ms REA—Right.

Ms Johnson—It is not easy. When you think of the diversity of the nations involved, particularly from Eastern Europe and Asia and to Western democracies, you can understand that their legislative frameworks differ.

Ms REA—How old is it? Has it been around long enough now to measure whether, as a result of the convention, nations that are going back and dealing with their own legislation—

Ms Johnson—Benchmarking; correct.

Ms REA—Has it had an impact?

Ms Johnson—I do not have any information on that but I am happy to take that on notice and try to find out for you.

Ms REA—Thank you. That would be good.

CHAIR—That is a very good question.

Ms Johnson—The Attorney-General's Department might be able to help you with that too.

Ms REA—Yes, I was thinking that we could follow that up with them.

CHAIR—We will certainly raise that matter with them.

Ms Johnson—Good.

CHAIR—I think that finishes our questions unless you have anything you want to say, finally, before we finish.

Ms Johnson—That is fine. No; I do not, thank you.

CHAIR—Thank you very much for attending. It is very much appreciated. The secretariat may follow up issues with you.

Ms Johnson—That is not a problem. Thank you.

[11.28 am]

CHISHOLM, Mr Glenn Lindores, General Manager, Network Security, Telstra Corporation Ltd

KANE, Mr Darren, Director, Corporate Security and Investigations, Telstra Corporation Ltd

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

CHAIR—Thank you for making yourselves available for this hearing. Although this 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 contempt of the parliament. Would you care to make an opening statement?

Mr Shaw—No, we do not have an opening statement. I think our submission speaks for itself. We would be happy to take questions.

CHAIR—Obviously the purpose of these hearings is to investigate the issue of cybercrime—essentially, its prevalence and what we can do to reduce this prevalence in the future. What is your view about the prevalence of cybercrime in Australia?

Mr Shaw—Without question, the instance of cybercrime is on the rise. It is becoming of increasing concern to the industry, government and, more generally, the community. It is our view that it is a matter that is deserving of increasing attention from both the industry and the government, working—we hope collaboratively—to try and address it.

CHAIR—You say it is on the rise. Do you have any view about the level of cybercrime in Australia at present?

Mr Shaw—I personally do not have any statistics. If we were to provide some information, it would be off the back of our network rather than from across the industry as a whole. Perhaps my colleagues have some published data.

CHAIR—I am assuming that the level of cybercrime on your network is probably pretty indicative of the entire Australian scene, being one of the major players.

Mr Shaw—Mr Chisholm manages our networks. He might have some insight into the scale of what we are talking about from our experience.

Mr Chisholm—We would be happy to provide you with statistics separately from this hearing as part of a follow-up submission. We have a very good idea with respect to how many machines we detect are infected, how much we communicate with our customers and how much spam, if you are familiar with that term, we receive on a daily basis. On different parts of the network the

scales are obviously different, depending on the part of the network it is in—consumer versus business versus other parts of the environment.

CHAIR—We would very much appreciate if you could pass on those figures to the committee. The systems in place were indicated earlier today. I do not think you were here. If sites or activity that might indicate cybercrime or some sort of improper activity are detected, ISP providers are notified and then the ISP provider generally tells the individual customer. Are you involved in that setup?

Mr Shaw—That is, the Australian Internet Security Initiative?

CHAIR—Yes.

Mr Shaw—Yes. Telstra BigPond is a partner in that particular initiative. We work with the ACMA, who managed it. We also undertake our own investigations across our network with regard to compromised machines and act accordingly if we detect them.

CHAIR—I am interested in how many people you are aware of through those systems? I understand that you have said that you will take that on notice, but perhaps you could ensure that information is incorporated. That would be very much appreciated.

Mr Chisholm—I will definitely incorporate that information in the response. As Mr Shaw said, Telstra BigPond is a member of that initiative, but, with our relationships with critical bodies such as AusCERT and international groups that work in this space, we also pick up a significant amount of other information which we use to try to assist our customers.

CHAIR—It has been suggested that signing the European Convention on Cybercrime would be a big step towards assisting with this problem. Does Telstra have a view on that?

Mr Shaw—Telstra would support any initiative that can assist in dealing with this particular matter. Our view at the moment is that a lot of people are well-intentioned in this space and there is a lot of well-intentioned activity, but anything that can further insist that and assist industry, government and consumers to better deal with cybercrime would be a step forward.

CHAIR—What do you think would be the best initiative to reduce the level of cybercrime in Australia?

Mr Shaw—We would have to say that some mass education would be a very good first step in that space. There have been initiatives from time to time—E-security Awareness Week and other things that the government has sponsored—and they are all very useful first steps. We see that an ongoing program of education for the whole community over time, rather than just over a one-week period, would be a very useful way of highlighting to people their obligations and responsibilities as users of the internet. Equally, it would highlight the steps they can take to protect themselves online, how to utilise the various resources that are there, how to make use of commercial products, how to take proper steps in their own behaviour online to minimise risk and the like, and advise the community to be alert when circumstances exist where cybercrime could be perpetrated and to appropriately report that back.

We protect people through road safety campaigns and we protect people through other public safety campaigns—and these are rolling programs of education—and we think that cybercrime is something that could be elevated to that level with an ongoing campaign of informing people of what the issues and problems are and what resources are available to deal with it. We think that would be useful.

Mr Kane—I want to add that we need to change or embed a change of culture around the use of technology. Instead of it being unusual business it needs to be now treated as business as usual. We believe there is a need for a campaign with mass marketing appeal initially but continuing with a consistent rollout over a long period of time. I know a number of different programs are being commenced but we have to have that coordinated and focused, and supported by mass media campaigns.

CHAIR—I can see the attraction of that and certainly why you would argue it. I want to assure you that what I am going to say next I am not saying just because you are Telstra. I am asking you this because you are an ISP and you are one of the largest, so don't feel that I am picking on you. You are really just an example. If we go to the road safety analogy, we obviously require people to drive their car safely. We educate them that way and we fine them if they do it improperly. But at the same time we also require of those who provide the vehicle that certain safety mechanisms are in place; for example, that there be seat belts and a range of other things. Not being particularly mechanically minded, I cannot rattle them off but I am sure someone could. What do you think ISPs could do to try to help with the issue of cybersecurity?

Mr Shaw—Clearly they have a role. In our case we already have material available through our various channels that we communicate to our customers. There is material in places like our T[life] stores, where people may go in and buy a product. We have a lot of material available online. We also make available to our customers who purchase a broadband product from us a 60-day free trial of a package of software that has virus software, firewalls, antispyware, malware protection and that sort of thing. So we try to put in people's minds at the time that they are purchasing these sorts of products that there is a range of steps that can be taken to make life safer. Just as a car manufacturer cannot force a driver to wear their seatbelt, yes, making the seatbelt available is part of the process. Having this sort of material available on these sorts of products is part of the process. We have got to make people start to realise that if they go online they have a responsibility to minimise the potential for people to perpetrate cybercrime and to take appropriate steps with their technology—their computers, their broadband connections, their modems and routers and that sort of thing.

CHAIR—It was suggested that there is a new type of security risk at the moment, which is the takeover of routers. Obviously many ISPs are involved in the provision of that router. One of the simplest problems is the fact that the password and username are standard, and they are set up that way. I was asking why when you have a setup process it does not automatically prompt you to do various things. If changing the password to something that was less easily guessed or broken would improve the security of the router a great deal, couldn't the system be set in place so that one of the prompts you have is to change your password as you do the set up? Are there any problems with doing that?

Mr Chisholm—Takeover of routers in a home environment is certainly not new; it has been happening for a number of years now. Passwords are very, very difficult. We maintain the

security not only for our network but also for our internal users, and we have 40,000 internal users. We set very stringent password policies for those internal users and we enforce them very, very closely and tightly to make sure that those passwords are changed regularly.

CHAIR—When you say internal users do you mean people within Telstra?

Mr Chisholm—My apologies; this would be Telstra staff members. We rotate those passwords and change them. Our routers are far more prominent on the internet and so obviously are a far larger target, so this is something that people attempt to do to us on a regular basis. For home users, attempting to get home users to set difficult to guess passwords is difficult. We spend a great deal of time educating the internal users who we have a very close relationship. We have desktop support people visit them. We try to get them to set passwords that are unable to be guessed or what they call brute force attacked—in other words, trying many passwords until you hit the password. Educating them is very difficult. There have been many examples of people's Facebook accounts being compromised because they have set very obvious passwords. People's web mail—Google, Hotmail and those types of tools—have been hacked, even though the people who use those tools know that it is very public and easy for people to try to get their passwords in that environment.

This comes back to what Mr Shaw said about education. The key element here is that we can give suggestions. When we hand out routers, we try and secure them. We make sure that when a router uses wireless it uses the appropriate wireless standard, which has an appropriately complex password. We make suggestions with respect to passwords. But what is considered a complex password? This is an example that we use internally—please tell me if I am going into too much detail. You have upper and lower case characters. You have a number and a special character in them. The very obvious one that people do is their first name with the first letter capitalised and they stick a one and an exclamation mark on the end of it. That meets all the criteria for a very complex password. But it is exceptionally easy to guess. The key problem is that what people believe is an unguessable password is a subsecond job for me or one of my team to guess.

CHAIR—Taking you back to what I was asking, is it technically possible to, when a new router goes in, for people to be prompted to change the password?

Mr Chisholm—We do that. They are. It is definitely technically possible.

CHAIR—Okay.

Mr Chisholm—As I said, the problem is that when they set that password they often set it—

CHAIR—I do not mean internally. I mean for your ISP customers.

Mr Chisholm—They are who I am referring to, yes. When you get the package, it comes with instructions on how to change the password, what you should do and how you should choose a password.

CHAIR—That is in written form. But is it automated so that as soon as they set it up it says, 'You should change your password now; please enter the new password'? Many security

systems, after a certain time has elapsed, prompt you. In fact, you cannot go any further until you do. When people set up hotmail accounts, you cannot force people to choose a particular password, but you could say, 'That's very low security.' It can give you feedback about whether it is a good password.

Mr Chisholm—It is technically feasible. It has been a while since I set up my own BigPond connection. I do not remember what we do exactly, unfortunately.

Mr Shaw—We might have to take that on notice and get back to you.

CHAIR—I am interested in whether it is possible and what the downsides to it are—if it is a problem, why it is a problem.

Mr Shaw—We will provide some further advice on that.

CHAIR—I am a bit concerned. People generally are rushing round using a computer. They open the box and there are these bits of paper saying things. They throw it over their shoulder, plug the thing in and get going.

Mr Shaw—You have been into my house.

CHAIR—What I am thinking about is trying to build something into the process so that the issue of security is dealt with, rather than it being an add-on extra. People these days are busy enough doing the absolutely necessary essentials and do not really seem to have the time for those add-on extra bits that they can avoid if they would like to.

Mr Shaw—We will have a look at that and come back to you.

Ms REA—Following up on the road safety analogy, the issue that we are trying to grapple with is about education campaigns and ultimately getting the end user to be responsible for their own security. While we would all like that to happen, we also acknowledge that that is probably the most difficult part of the equation. We had a discussion earlier this morning with one of our presenters around whether there is in fact any cost benefit to you as a company that depends upon an enormous number of online transactions to contribute in some way—not just technically but financially—to that end user security. I would be interested in hearing your view on that.

I would imagine that, when it comes to identify theft and when it comes to people being the victims of some form of crime, they are instantly going to move away from online use. Do ISPs and companies like yourself, which would I imagine increasingly deal with online transactions, see a financial benefit to fund some of that security so that you can keep people in a secure environment and therefore keep business online rather than going for more expensive options?

Mr Shaw—I think the answer to that is in two parts. The first part is that the online economy is so embedded across the entire economy that cybercrime does not just touch ISP; it also touches the banks.

Ms REA—That is right; exactly.

Mr Shaw—In a sense we would argue that improving cybersafety and cybersecurity is a public good and therefore is something that is worthy of funding from government. At the moment we make significant investment in this area through a whole range of activities, not just the cost of running parts of the business like Mr Chisholm's where we invest heavily in expert staff and in network equipment and the like in order to provide a safe environment. Mr Kane's area provides a lot of support for educational activities and the like and through the Telstra Foundation does a lot of work. It might be useful for Mr Kane to outline some of that work in a minute. The point is that we are doing a lot now in recognising that this is an important issue for us as a business, but we would argue that, given the embedded nature of the online economy across the entire economy, safety becomes a public good. Mr Kane can talk a little bit more about some of our initiatives.

Mr Kane—We are investing heavily in this area. We see it as a brand and reputation issue for us as well as a responsibility to our users. We feel that every user associated with Telstra, be it a customer, a shareholder or a member of our staff, should be entitled to access to all the information and expertise they need to get real value from their online experience. That is the aim of our internet trust and safety working committee, which is a cross-company committee reporting up through to senior group managing directors in five of our front-house back-of-house areas.

The Telstra Foundation has committed \$6 million since 2007 to cybersafety particularly targeting children and young adults. That will push out to 2012. We have just announced a scholarship of \$15,000 to leading senior police officers at the Australian Institute of Police Management in Manly to take that scholarship overseas to learn more about the online environment of cybercrime and business management using technology. We have an area, which I now run as the internet trust and safety officer, where we are working diligently with the government particularly, law enforcement agencies and national security agencies to push out this message of cybersafety and the need to be secure online.

I will pick up on your point about the analogy of driving. The problem that we all face—and that is government and other presenters to your inquiry—will be the need to actually make sure that the messages that we send out resonate with the different user groups we are targeting. With your traffic and automobile safety you are targeting 16- and 17-year-olds and those older, namely those people who drive a car. We call them the 'very young' in our Telstra clock face. We have identified 12 different user groups. With 'sponges' at two or 2½ all the way through to the 'look at mes' who are using the social networking sites at 16 and 17, to 'tail enders' who are people who are finishing off their career but do not want to leave behind their knowledge of technology because they are going to use that to communicate and conduct commerce.

We have to target messaging that actually looks at the 'forever youngs' and looks and the 'spongers' and then looks at the people who are shuffling through early adulthood. That is the real challenge; to make sure that what we are pushing out is bang for our bucks. We are prepared to spend money and we are spending money. What we have to do is make sure it is targeted and that it resonates with the groups.

Ms REA—I am wondering if you are aware of the legislation that has been mentioned that is before the House around identity theft. I imagine that that would be a real issue for Telstra when you are talking about people's phone numbers and all sorts of other information you need to

ensure security for that customer online. I am just wondering if you have some views about the effectiveness of that legislation and what we can do about identity theft.

Mr Shaw—The people at this table have not been involved in considering that particular piece of legislation.

Ms REA—Okay, that is fine.

Mr Shaw—But we can go back into the company and see if there is a view that we could usefully put before you. Yes, the issue of identify theft is one of the most visible outcomes of cybercrime because people live in fear of it. They hear these horror stories of people losing their identify on line and having all their assets stripped and then recovering it. It is one thing to lose it and get your money back. It is another to recover your identity given all the problems that that can create going forward. It is clearly something that we need to deal with in an effective way if we are going to have that level of confidence in the online environment which is necessary in order to get the benefits that it can provide.

Mr Kane—I would also add that age verification and identity verification online is one of the largest issues that we all recognise exist. We work hand in glove with law enforcement and national security agencies on a daily basis. Our corporate security and investigations area, which I am responsible for, does significant work in that space. So we understand those issues and we are working effectively with law enforcement to try to manage those.

Ms REA—Thank you, Mr Kane.

CHAIR—You said you spent \$6 million on cybersecurity issues; was that what you said?

Mr Shaw—Cybersafety initiatives.

CHAIR—What did you actually spend it on?

Mr Kane—It is through the Telstra Foundation, which is a philanthropic arm of the organisation. We felt that it was really important to ensure that the grants that we offered under the funding were targeting areas that impacted on the corporation itself. So we have targeted cybersafety as a spotlight. We initially offered seven, in \$3 million of funding, for grant recipients who could promote programs and initiatives targeted at cybersafety for children under 24, children and young adults. We actually exhausted that funding. One of the seed funding matters we promoted was the Alannah and Madeline Foundation, who have best-practice initiatives going out into primary schools, through the CEO, Judith Slocum, and I.

CHAIR—So you have provided \$3 million through grants for outside organisations?

Mr Kane—That is correct.

CHAIR—Can we get a list of what those organisations were and what programs were being funded?

Mr Kane—Absolutely. We have just opened another round of funding with a further \$3 million, pushing out to 2012, targeting the same spotlight.

CHAIR—And the other \$3 million?

Mr Kane—The first \$3 million was exhausted.

CHAIR—You said that you spent \$6 million.

Mr Shaw—We have allocated \$6 million. There was \$3 million and then we have topped it up with another \$3 million.

CHAIR—I see.

Mr Shaw—So we have gone out for another round.

CHAIR—I understand.

Ms REA—How big or small are they? What is the range of those grants?

Mr Kane—I will have to take that on notice. I will provide that to you. As I do recall, anything between \$50,000 and \$250,000. SuperClubsPLUS is one that comes to mind, which is a walled garden or a secure digital environment for children to learn better web practices on line.

Mr Shaw—We gave just over a million dollars to the SuperClubsPLUS initiative.

Ms MARINO—The government has announced it will take over the role of AusCERT but in your recommendations you have actually said that you would like AusCERT to be recognised as the national computer emergency response team. I wonder if you could explain why you would prefer AusCERT in that role.

Mr Shaw—Our recommendation was based on our assessments of the capabilities of AusCERT and the desire to see in place an entity that had that knowledge and expertise. That is where, in our view, it rests at the time. If the government chooses to go down another path, then that is within the gift of government. Our overriding concern would be to ensure that the expertise and knowledge continue to exist somewhere.

Ms MARINO—The existing capacity in AusCERT? Is that what you are saying?

Mr Shaw—It is that the knowledge and expertise that exist in AusCERT continue to exist in one way or another. Our primary concern is to ensure that knowledge and expertise is available, as it is at the moment.

Ms MARINO—As a resource?

Mr Shaw—Yes.

Ms MARINO—Given that you have extensive experience in managing a national network with the proposed NBN, what sorts of additional challenges would you see relating to high-speed broadband access given some of the cybercrime issues that you are aware of in your organisation?

Mr Shaw—We run an extensive fibre network already, so we have some experience in these sorts of areas. We are reasonably confident that government and its advisers, in making decisions around the NBN and its architecture, will be cognisant of the various engineering standards and requirements that are out there at the moment and will adopt what is necessary to provide a level of protection to users.

Ms MARINO—I am interested in the proposed National Cybercrime Advisory Committee—it was one of the recommendations. Who would you see as part of that particular advisory group?

Mr Shaw—Darren, do we have a particular view? I think it is going to have to be a wide-ranging group because the issue of cybercrime, as Darren has just mentioned, in terms of the user side of it, has a number of different segments. Glenn is on the network side—the people who actually run these networks, provide security, look at what is happening with traffic and try to mitigate threats and deal with them. A lot of technical expertise sits there as well. It is going to have to be a blended group, and it may well be the group has to be organised in different ways to deal with particular issues and make use of expertise. But we did not have particular names in mind.

Ms MARINO—Would you see that type of committee working with the minister? How would you see that operating in a structural sense?

Mr Shaw—We think that there should be a central point within government to deal with cybercrime issues, where people can report incidents, can share intelligence and can seek advice, resources and the like. It would seem to us that an advisory committee could be part of some structure in that way to contribute to the work of that sort of entity within government.

Ms MARINO—Right, but sitting underneath the minister's portfolio? Where would you see it sitting?

Mr Shaw—As an advisory committee I think it should have some degree of independence in order to be 'frank and fearless'. But it should be located within the structure and governed in a way that it is communicating and connected with government, and that means it can operate effectively and efficiently and get that advice into government.

Ms MARINO—The response by government to the recommendations reflects that.

Mr Shaw—Sorry, the response?

Ms MARINO—Basically, they are in a position where the government responds to the recommendations that a committee of that type would make.

Mr Shaw—I would think that it is a matter of good governance that it would be appropriate for government to respond to these sorts of things. But I would not like to see it quite in statutory requirement or anything like that, where a minister was obliged within certain times to do certain things. The nature of the online economy is such that flexibility and nimbleness is important. The ability for people to provide advice and for government to be able to respond as they see fit—quickly, rather than getting caught up in process—would be important for us.

CHAIR—Telstra is obviously involved with the e-security code of conduct—a voluntary code at this stage. Does Telstra have any opposition to that voluntary code becoming compulsory, and if so, why?

Mr Kane—The IIA appeared before you this morning and the e-security voluntary code is a proposal that we currently undertake with the participation of ACMA. Mr Chisholm will be able to speak a little about what we do in that area as he has responsibility for it. We see it as a voluntary code and we already do this in place. We have not got any significant opposition to continuing down the voluntary nature of the code as it is to be drafted. The first draft will be cut and provided to all participants later next week I understand.

At this stage, I think that all ISPs that are currently involved in the voluntary code understand the importance of what is being recommended. It would not be a firm push from the industry to ensure that other ISPs cooperate with the code. I would have to take that outcome on notice but, initially, I think the voluntary nature of it would ensure that we are seen to self-regulate our industry.

CHAIR—I did not really get a response to my question, though. I understand that you may not be in a position to do so; maybe you could take that on notice; whether there is opposition from Telstra to it becoming compulsory and, if so, why? I am genuinely seeking information.

Mr Kane—Yes.

Mr Shaw—We can come back to you on that one.

CHAIR—There is an issue about third party claims for activities that protect networking customers. Is that correct?

Mr Shaw—Claims against us?

CHAIR—Yes; that you are concerned that is potentially possible, and you are seeking legislative protection from that.

Mr Shaw—Yes, similar to protections that already exist in the Telecommunications Act around carriage services and all that.

CHAIR—Can you explain why you think that is justified?

Mr Shaw—There are going to be circumstances where we may take action to protect our network which a customer may argue has adversely impacted them, and they may seek to take action against us when in fact the step we took to protect our network was of a greater good and

necessary in order to ensure that the online environment functioned as it should and that threats were removed. Those threats may not only be to us but also to other users, to other corporate customers, and to government, so we think that it is appropriate to have symmetry in the way that these things are dealt with under law and that those sorts of provisions that are in the Telecommunications Act should move across to the online environment.

CHAIR—Which existing legislation are you drawing an analogy with?

Mr Shaw—There is a provision in section 313 (5) of the Telecommunications Act.

CHAIR—How does that operate at the moment?

Mr Shaw—Under section 313 (5) of the Telecommunications Act:

(5) A carrier or carriage service provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith:

(a) in performance of the duty imposed by subsection (1), (2), (3) or (4); or

(b) in compliance with a direction that the ACMA gives in good faith in performance of its duties under section 312.

If we are acting in good faith and in accordance with the legislation then we should be protected from any adverse outcomes that might be brought against us.

CHAIR—I am trying to get a broader understanding of that section. What are the sorts of things that you are complying with that could potentially bring about damages claims against which you are already provided with protection under that section? What sorts of things are they?

Mr Shaw—We might drop a message from our network because we regard it as a threat. We might think that it contains malignant software or malware of some sort and it turns out that, while that might or might not be the case, the consequence of dropping it is that someone thinks they have suffered an adverse consequence and might seek to take action against us. So I suppose it is a form of safe harbour in effect. If we are acting in good faith and in the best interests of protecting the integrity of the network, there should be similar sorts of protections as exist at the moment under section 313.

Ms REA—I want to get your thoughts on a more general view. We are talking here about various laws, initiatives, coordination and advisory groups—a whole range of things. Clearly, prevention is the only way that we are going to be able to deal with this issue because we heard in discussions earlier today that the actual detection and conviction of a cybercriminal is increasingly difficult, particularly given we can have the best laws in the country here, as was pointed out, but the criminal is probably not even in the country and never will be. I am wondering whether you have some views about the level of effort that we should put into the detection and conviction of criminals and what your experience is. What is the view of the other international companies that you deal with on what the global approach would be?

Mr Shaw—We strongly believe that the law enforcement agencies need to be appropriately resourced in this space.

Ms REA—Will that be effective? If they were resourced, could they do it? Do you think they could they find these people and convict them?

Mr Shaw—They do. You see some instances of that, particularly in that really vile part of the internet where you have predatory practices against children and child abuse. The AFP, in collaboration with some of their international partners, have done some good things in that space and we would argue that they are deserving of continued funding at appropriate levels to enable them to continue to do their own work here and to collaborate with international agencies. As to the issue around effectiveness in some of the economic crimes, I noticed there were some comments made earlier about some of these things. I think part of the education around cybercrime needs to extend to the judiciary as well so they understand the importance of sending out clear warnings to those people who are brought before the courts.

In terms of what our overseas contemporaries might think, I am not sure that I or my colleagues are in a position to put words in their mouth, but given the general level of involvement of the major telecommunications carriers, ICT companies and the like, the Microsofts, the Googles and the software providers, everyone recognises that this is an important issue internationally and we need to do everything both domestically and internationally as an industry, as law enforcement bodies, as governments and as consumers to deal with these things. We cannot wish away the issues that are there but we need to realise the importance of the online economy to our ongoing productivity and economic growth and to the social inclusion that it can provide as well. So continued investment in those areas, including in the law enforcement area, we think is important.

Mr Kane—I would add that it needs to be partnered with an effective awareness or education campaign, because just looking after the aspect of the detection, interdiction and prosecution will not be the silver bullet we are looking for. We need to start with an education and awareness program and coordinate it all the way through to the detection, interdiction and prosecution.

Ms MARINO—I will take it one step further. You are providing a network and a service, but in relation to some of the online content issues are you aware of the extent of organised crime and its use of the internet? If so, are you working with government agencies on this type of issue, and what level of requirement at your particular end is being applied to deal with this expanding issue?

Mr Shaw—We have very close links with law enforcement and national security agencies to deal with cybercrime issues. We do that on the technical side and the like with Mr Chisholm's part of the business. Mr Kane's part of the business deals with warrants and other things that are dealt with through the courts and require us to provide information. We have ongoing consultations with the various arms of government that have an interest in this. We recently signed an MOU with the Australian Federal Police around these sorts of matters. We have staff who are in regular contact with the various agencies to discuss ongoing developments in this space, to share information, to share knowledge and to enhance our ability to collaborate from both sides, because these things are only dealt with collaboratively and not in isolation. Our chief executive takes a keen interest in these sorts of things and does talk to senior people in

government about these matters. We are aware that the government can only go so far and will need the assistance of industry, not just us, but anyone who owns network components in Australia has a role to play. We do not doubt the need to continue to collaborate with the right people in government to ensure that we are sharing knowledge, information and expertise and getting the best outcomes in this space.

Ms MARINO—The level of risk that this poses to Telstra as an entity and, without breaching any commercial confidentiality, I suspect that if people were fully aware of the level of risk it may result in changing their habits and the amount of use they made of the internet. What level of risk is there in that particular perception?

Mr Shaw—Clearly there is a risk in the online environment, as there is a risk in any aspect of life. We take a risk when we drive a car or we walk across a busy street. The important thing for us is to address the risk and address the risk properly. Some of the things we have spoken about here are about identifying and managing risk in an appropriate way. Some of that falls to us as a business and some of it, as we have talked about before, we think is a public good and should go beyond just the business side. But we cannot wish away risk. We acknowledge that there are people out there who want to try and use the online environment in malicious ways, either for economic gain or for some of the more vile things that we hear about on the online space. We have to, in partnership with law enforcement, government and consumers, all manage that risk down, the way we manage any risk in our daily economic or social activities.

Mr Kane—I can add that the partnership with law enforcement does exist between Telstra and the national security and law enforcement agencies and has been acknowledged. I have been asked to speak at an international conference in Vancouver last year and was invited to Rome this year by Interpol to speak on the way we manage that relationship. That type of relationship is not replicated or enjoyed in other places in the world. Like I said, that model would fit in those areas. So it has been acknowledged by law enforcement agencies internationally as something they would like to see expanded.

CHAIR—You have talked about a national cybercrime advisory committee. How does Telstra envisage that would be made up and operate and what its role really would be? There are a lot of people who have expertise in the area. We have lots of people coming to us. Why is another committee going to improve things?

Mr Shaw—We would see that committee having a role in conjunction with another recommendation that was in our submission, which is that we think there needs to be a central point in government where this issue is being managed. At the moment it is dealt with in a variety of areas of government. In their best endeavours they collaborate as best they can. A lot of that, though, is ad hoc rather than done in a strategic sense from one point in government with an overall policy strategy agenda. If that arrangement were put in place then an advisory group which brought people together—the practitioners, the users, the people who protect people on the networks, people who protect people through education—would be a point where government could seek the best advice on a whole range of issues within the cybercrime space. It may be that your advisory committee might have to segment itself in some ways. It may have some working groups dealing with particular issues in order to get the best and the brightest in the spaces to provide the best advice possible to government and to inform education campaigns

and to inform an alert the practitioners out there about emerging threats and how to deal with them in their networks. Those sorts of things. I think the two should be taken together.

CHAIR—Who would this advisory committee be?

Mr Shaw—We would see it as being a mix of skills relevant to all of the issues that are in the cybercrime space. There are clearly going to be people with technical expertise who understand networks and how to protect networks. There are going to have to be people that understand society, the kids, the users, the older users, the seniors—whatever else—and how to educate them. There are going to have to be people that understand law enforcement and how to make things work in a way that, at the end of the day, if we catch people we can actually put them before the courts and get them dealt with properly. There is going to be a range of skills in dealing with an issue that is essentially a crime. It is crime prevention, dealing with the crime, detecting what is going on and taking appropriate action in a law enforcement sense and then educating the community about how to avoid the crime. They will all require different skills and all should be represented in that sort of committee.

CHAIR—You are seeing it as a advisory committee to the government or to the minister?

Mr Shaw—We do not have a firm view in that respect. Our desire is to see a central, more coordinated approach from within government and then an advisory committee to contribute and to assist in that work. If the government were to accept that recommendation and set it up and chose to have a reporting to a minister, that is one model. Whether it reports to a bureaucratic process through public servants is another process. We are not particularly wedded, so long as at the end of the day it can achieve what it needs to do, is effective and can operate in an environment where can provide the appropriate advice to government and get that dealt with.

Mr Kane—I might also add that I am a representative of Telstra on the Consultative Working Group for Cybersafety through to Minister Conroy. I see that as an effective forum that is providing some valuable out takes. That may be a model you look at. It may not be the specific model you settle on. We are targeting education messages and what we can do to push those messages out, particularly aimed at children. Whereas this issue may be aimed at the effects of cybercrime.

Mr Shaw—Mr Chisholm quite rightly pointed out that an advisory group of that nature really should have links into the wider economy, particularly in places like banking and finance that depend on the online environment for a lot of their transactions, so that we capture not only the expertise and understanding that they might be able to add but also be able to reinforce messages about how to deal with and prevent some of these crimes.

CHAIR—I think that is becoming more and more obvious when we look at people who are involved in the internet and the provision of services: the way our economy and our society is working, more and more there are major players at the internet stage who are outside that normal area. The finance industry, overwhelmingly, has a big role to play, I think.

Mr Kane—To pick up on that point, the Consultative Working Group for CyberSafety that we spoke of has industry partners such as Google, Microsoft, MySpace and Telstra on board. We also have the Australian Federal Police's High Tech Crime Operations director. We have senior

NGOs like the Alannah and Madeline Foundation and Bravehearts. We have some significant representations across departments and industry. It worked well.

Mr Chisholm—The type of body we are talking about here also assists with the interfaces between these organisations. Banking and finance does in fact have quite a good internal communications mechanism so they can assist each other with information sharing. The issue is that the challenge faced by banking and finance now will be faced by retail in three years time. We need to avoid creating blatant opportunity for cybercriminals by not getting consistency across the board. Having government act as the coordinator can break down some of the barriers between these industries. My colleagues and I in the banking and finance industry are trying to coordinate with retail and schools, but it is not always possible to reach out. As standards come through other governmental regulatory frameworks, particularly, say, in the banking and finance space, their information and security standards are being proposed as a requirement through APRA. If these types of things can be coordinated on a more general basis, and if you can get some consistency, I believe there will be a far more effective framework.

CHAIR—I understand. Any questions?

Ms MARINO—This might be a bit of a left fielder. With the growth in the use of the internet and the potential growth in cybercrime and the losses that the individual consumer assumes as a result, are you aware of where the liability lies where a consumer has effectively lost whatever they have lost? Have there been cases where consumers have attempted to make a case against a network, an ISP or another in relation to where they believe the level of responsibility for their losses might lie?

Mr Shaw—I am not in a position to give you information about where liability might lie in the Australian environment. It is a complex area, and I think there would be a lot of contractual and other arrangements in place. If you would not mind, I would prefer to take that one on notice so that I can give you some advice.

Ms MARINO—Certainly. Thank you. I would appreciate that.

CHAIR—Thank you for that. There are a number of matters that you have taken on notice. We have got to the end of our questions, so I will close the meeting. We do very much appreciate your coming along and spending your time.

Mr Shaw—Thank you, Chair.

Mr Chisholm—Thanks, Chair.

Proceedings suspended from 12.18 pm to 1.34 pm

SINKOWITSCH, Mr Michael Anthony, Business Development Manager, Fujitsu Australia Ltd

CHAIR—Welcome. Although the committee does not require you to give evidence on oath, this is a legal proceeding of 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. I invite you to make an opening statement.

Mr Sinkowitsch—Thank you for the opportunity to appear before the inquiry today. It is greatly appreciated. Fujitsu's aim in providing a submission to the inquiry was to highlight the extent of cybercriminal activities in Australia. It is assumed that other organisations and individuals presenting to the inquiry will discuss the potential financial and other ramifications of these activities as well as any perceived current legislative amendments necessary. While some of this was also outlined in Fujitsu's inquiry submission, we will leave this for others to discuss in detail during their inquiry appearances. The aim of this statement, therefore, is to focus on how industry, in partnership with government, can assist in implementing mitigating strategies and timely responses to cybercrime activities.

It is noted in the Fujitsu submission that a 2008 survey by security vendor AVG showed that Australia has a very high incidence of cybercrime, the highest of any of the other countries surveyed, which included the US, France, Germany, Italy, Spain, Sweden, Brazil and the Czech Republic. The results showed that around 39 per cent of Australians had been the victim of some form of cybercrime. Broad categories of cybercrimes that impact Australian citizens and government include, but are not limited to, hacking, denial of service, data theft, defacement, espionage and robbery. The perpetrators of these crimes may include hacker unions or crews, both domestic and foreign; organised crime; foreign intelligence services; botnet operators; random individuals looking to take advantage of readily available black or underground technologies; and special interest groups, as we have seen during the past week.

The nature of internet crime is transnational. It is engaged in by both novices and professionals and feeds an underground economy that has its own language, trade craft, assets and resources. Perpetrators of these crimes are not bound by national boundaries. Attacks against Australian organisations and citizens can and do originate from servers based anywhere in the world, even within our own country. Attributing attacks to specific individuals operating under the cover of proxy servers and internet aliases requires deep and consistent monitoring and penetration of black hat or criminal hacker forums, chat rooms, websites and other hidden communities and communications mediums. Naturally, much of this is in languages other than English, further complicating the matters and making them more difficult to target.

The technology utilised by cybercriminals is flexible and advances at such a rapid pace that identifying, understanding and defeating the emerging threats is one of the biggest issues. It is highly likely that right now somewhere in the US, Europe or elsewhere in the world there are a couple of smart people coming up with the next social web concept to change the way we interact across the web. It is also certain that right now there are equally smart or smarter people coming up with the next high-tech scam, SQL injection, botnet protocol, malware product or

hacking tool that will assist criminal elements to gain illicit wealth via the web. It is in the defeating of these new and emerging threats that I will now concentrate.

In order to defeat a problem you must first understand it. The challenge is that we are faced with agile and adaptive adversaries who operate behind the anonymity of cyberspace. The only way to meet this challenge is to be equally agile and adaptive and by employing all means available in a coordinated and concerted government and industry joint effort. Fujitsu believes the government has a good technology and personnel skills base with which to address the issues. However, Fujitsu also believes that government alone does not have, in total, the necessary resources to meet and neutralise these threats. It is Fujitsu's view that a combined approach by government and industry is necessary if effective countermeasures for new and emerging threats are to be quickly identified, developed and implemented. There needs to be a partnership between government and industry, leveraging the relative strengths of each and providing effective mechanisms to defeat these threats.

There are already a number of examples where government and industry have effectively engaged in partnerships to address societal and cybercrime activities. An example is BRIDGE, a US intelligence community initiative to provide a virtual connection for interaction between intelligence analysts and private industry experts. BRIDGE provides an environment for analytic outreach. It is a place where intelligence community analysts can reach out to expertise elsewhere in federal, state and local government, in academia and in industry. New communities of interest can form quickly in BRIDGE through the 'web of trust' access control mode, providing access to minds outside the intelligence community and creating an analytic force multiplier.

There are other examples globally where these types of organisations are being established. The result has been the advent of what are collectively titled security trust networks. Security trust networks, depending on their ultimate aim and purpose, are expert affiliations of interested organisations and individuals that can investigate and mitigate cybercrime threats. Security trust networks are proving to be a necessary and effective model for combating cybercrime activities of all types and motivations. As I mentioned, the challenge is that we are faced with agile and adaptive adversaries who operate behind the anonymity of cyberspace. Security trust networks provide the agile and adaptive environments to defeat, or at the very least limit the damage of, the adversaries.

There have been some recent noted successes by security trust networks in establishing the source and methods of cybercrime activities. These have included the Project Grey Goose investigations into the cyberattacks on Georgia during its recent military conflict with Russia. Project Grey Goose is a loose consortium of individuals, private and government—including, I believe, some within Australia. In their own time they use industry donated analytical tools to determine the source of the attacks using material available on that web, or what is known as open source intelligence. Another example is Canada's privately funded Citizen Lab, which recently discovered and investigated the intricate global cyberinfiltration of the Dalai Lama's network using similar people, tools and capabilities. It is the ability to bring together like-minded organisations and individuals with a common aim, as well as the outcomes of their activities, that is important.

Doubtless you are aware of the attacks on the Prime Minister's website, as well as other government websites, on Wednesday this week by a group calling themselves Anonymous. This provides an outstanding example of government and industry cooperation in defeating, or at least limiting the effects of, an attack against government agencies. Given the advance warning, government agencies were able to notify industry and seek assistance from industry, including Fujitsu, in limiting the effects of the attack. Measures were quickly devised and implemented by government with industry support to negate the effects of the attack, the result being only a minimal disruption despite a concerted effort by the group Anonymous.

Whilst advance warning may be rare, it may also become an increasingly common method of splinter organisations or special interest groups with an axe to grind to gain publicity for their cause, their capabilities and the perceived limitations and technology soft spots of agencies. It demonstrates that a small number of people with only moderate skills can attempt to bring down networks to meet their own aims—criminal, protest or otherwise. However, it also demonstrates the clear ability of government and industry to respond quickly to meet and defeat threats when engaged in a partnership.

Given all this, Fujitsu believes there is a very real need for formal, close engagement between government and industry on an ongoing basis to meet and defeat cybercrime threats. There are examples of this in cybercrime already, such as the AFP's High Tech Crime Centre having embedded financial institution staff. However, the model needs to go further.

Fujitsu believes the government should sponsor the establishment of specific cybercrime government and industry organisations based on security trust networks or another suitable model, empowered to identify and defeat cybercrime activities. The establishment of these organisations with government backing would provide the necessary impetus and capability for the engagement of experts in the various domains of cybercrime across government agencies and industry large and small. The right people—and, at times more importantly, the right interested and invested people—would be quickly brought together to meet threats as they emerge and implement strategies.

In conclusion, the challenge is significant and will continue to evolve. Cybercrime will not go away. As long as there are ways and means of making illicit gains from activities in cyberspace there will always be an underground element, some of whom are possibly state backed, willing to take advantage of that means. Cybercriminals will continue to seek new methods of exploiting weak spots, be they technological or human, in an attempt to defeat implemented countertechnologies and strategies. This will prove particularly so as technology itself evolves.

It is impossible and impractical to believe that all cybercrime activities can be detected and defeated. Declaring that the problem is too vast, however, is not an option as the damaging effects and implications of cybercrime will be felt across the social, security, financial and political aspects of life. Fujitsu believes that government must closely interact with industry—particularly service providers, security experts and technology vendors—at all levels to collaboratively determine effective policies and strategies as well as to drive antic cybercrime technology that will assist in thwarting cybercrime. This will require a commitment of resources and funding on an ongoing basis, as well as continual vigilance, backed by sound and up-to-date legislation, to meet evolving cybercrime threats. Thank you again for the opportunity to appear before the inquiry.

CHAIR—Thank you. You used the term ‘security trust network’. Can you explain exactly what that means?

Mr Sinkowitsch—It is almost a collective noun—a collective term—for a group of likeminded individuals, organisations, government agencies, private individuals, academics or technology vendors, who combine to, in some cases, investigate specific elements of cybercrime or specific activities around cybercrime. Cybercrime, of course, has a very broad definition. I use the example of Project Grey Goose, as a security trust network. They have come together as an organisation using some borrowed tools from interested companies to investigate specific attacks on Georgia by elements within Russia. The security trust network is really an amalgam of interested people—and, on some occasions, invested people—to look at an emerging threat or treatment for a threat, or to determine the origin of a threat, for example.

CHAIR—So is it set up by government?

Mr Sinkowitsch—No, not necessarily.

CHAIR—Are they self appointed?

Mr Sinkowitsch—Many of these are self-appointed interested groups. Some of them have an academic institution behind them, such as the Citizen Lab organisation, which investigated the infiltration of the Dalai Lama’s network. Essentially, they can stem from pretty much any interest group. The flip side is that their interest is specifically in defeating these threats—in determining where these threats originate and how they came about. They commit some investigative and intelligence resources into finding out where these threats are emanating from.

Ms REA—Did they succeed?

Mr Sinkowitsch—There is not much they can do about stopping the threats but they can highlight where they are coming from—who is doing them. They try to determine whether they are state backed or have tacit state backing or whether they are coming from a particular criminal element. They can look at patterns of attack. They investigate through pretty much any means. There are reports available that these organisations have put out on the web.

Ms REA—So that we can understand it, can you explain to us—using whichever one is easier, the Grey Goose Project or the Citizen Lab example—how these things work?

Mr Sinkowitsch—Sure. Okay. In, I think, 2007, there was the Russia-Georgia conflict. I do not know who to believe about which country invaded the other. I am not here to talk about that.

Ms REA—Sure.

Mr Sinkowitsch—There were some attacks on some specific Georgian government websites—denial of service attacks, defacements and so on—by persons unknown. So Project Grey Goose determined to investigate this and find out where these attacks came from by using various experts from around the world, people who were interested and some donated analytical tools. It brought all that information together and then to wrote some reports on the findings. Essentially, they were probing the internet and looking at the traffic that was causing the denial

of service on particular government websites and so on and tracing it back to the various originating elements and then running it through analytical tools to determine where it was coming from. It was essentially determined that, through various servers around the world, the attacks were emanating from Russia.

Through internet chat forums there was chatter around what to attack now, who to attack, how to do it, how to do SQL injections and various things along those lines. So it was really instrumental and it really showed the capability that is out there by interested people with no funding, essentially, to have a look at these attacks, to try to determine the source of them and to bring it to bear and bring it to light.

Ms REA—Did they expose people who were perpetrating these attacks?

Mr Sinkowitsch—What they have done is expose the aliases of the people as opposed to the actual people. With more detailed capability—and if you think about it, that is perhaps where the government side of it could come in with some more powerful rigour and capability—we would be able to potentially find out who these people were sitting behind those aliases.

CHAIR—You talked in your submission about compulsory reporting of breaches. Can you talk a bit more about why you think it is important that it is compulsory?

Mr Sinkowitsch—I think it should be compulsory because if you really want to understand the extent of a problem you need to be fully to grips with it, to have all of the available data to hand. For example, if a financial institution does not wish to publish attacks on it because it wants to protect its underlying corporate viability and so on, perhaps that is a disservice in itself. If government, for example, does not have all the information to hand that it needs, how is it going to implement the correct strategies in order to meet those threats, new and emerging, as they arise? I would note that taking part on census night is not an option, and voting is not an option; you have to do these things, for good reason.

CHAIR—So essentially what you are saying is that there is a lack of reporting at the moment.

Mr Sinkowitsch—Very much so, potentially. There is a lack of reporting because you do not have to report, but perhaps there is also a lack of accurate reporting as well. So I think there are two sides to that. In order to implement the policies necessary to be effective, you need all of that data available to you to make those judgement decisions.

CHAIR—Who do you think the best body to report to would be? There is obviously a police investigation unit, but I think there would have to be a question about whether it is really a good use of an investigative body's time to deal with phone calls reporting this or reporting that. Who do you think these reports should be made to? Which body, person or organisation?

Mr Sinkowitsch—An organisation such as AusCERT might be a good one, or another CERT. I believe AusCERT is moving in under the Attorney-General's Department. I could be wrong there.

CHAIR—I heard that today, but I have not had that confirmed

Mr Sinkowitsch—In fact I was listening in earlier. That is where I heard it, too.

CHAIR—That is how rumours start.

Mr Sinkowitsch—You heard it here first! I do not know. I would agree with you that the high-tech crime ops area of the AFP is not really the area, but it is possibly not my place to say that. But somewhere like an AusCERT would be pretty ideal, or even the Institute of Criminology.

CHAIR—What should they actually be reporting? What is the full extent of what should be reported? Is it an actual crime, or should they also be reporting every time an identity is stolen? How far should it go? What should the reporting include? What events?

Mr Sinkowitsch—If it is reporting a crime then there are other ways and means of doing that. I think it is around capturing the data. If it is a crime, for example, then it is a side process that needs to take part in reporting it. I think that things such as attempted attacks, defacements, denials of service and so on—those sorts of things—need to be reported as well, whether they have actually caused financial loss, brought a system down or so on. It is a matter of reporting all of those incidents so that the true picture can be stated and told.

Ms REA—Pardon my ignorance, but what does ‘denial of service’ actually mean? What is it as a crime? Also what does the fourth one you list here mean, ‘the degradation of network performance associated with heavy scanning’? What is the crime involved?

Mr Sinkowitsch—They are actually similar in many respects. In a denial of service—which you will see written as DOS, or DDOS, directed denial of service—essentially they try to do what they did to the Prime Minister’s website a couple of days ago: in laymen’s terms, they try to smash the network, so that anyone else trying to get on to that website or to access any information on there cannot get on and just gets an error message. While attacking government websites and so on has ramifications, when you are talking about the commercial sector, where someone depends for their living on their internet access and on people being able to access their website to purchase things and so on, there are enormous financial ramifications.

Ms REA—I understand. And the other one is fairly similar, is it?

Mr Sinkowitsch—Very similar. So a denial of service attack will traditionally use a bot or a botnet to attack it; a heavy scanning one might just be slamming it with emails or something along those lines, or using some other method of doing that.

Ms REA—I am quite interested in these security trust networks. I know we have talked about them a bit, but what has been emerging, through the submissions we have received and the evidence given today, is that the whole issue around detection and, therefore, conviction of a crime, is probably the most difficult in this area—trying to find these people, and having domestic laws governing this when, in fact, it is an international crime and you may never be able to prosecute the criminal.

It is the first time we have actually heard of some sort of a system which has actually worked to at least be able to detect and find these people in a meaningful way. When you say that a

group of interested parties can come together and achieve this, clearly there must be opportunities there for not just a government but collaboration between governments to be able to deal with this. Would you like to expand a bit on how these networks could actually become more formalised and effectively become detection agencies, if that is what they would be?

Mr Sinkowitsch—As far as government-to-government interaction goes, I think this is a new and emerging field of interaction between various agencies. Undoubtedly, government agencies will already be interacting with their partner agencies in other countries. You see that across other societal issues.

Ms REA—Sure. But would they be setting up similar sorts of things to this to actually do the investigating?

Mr Sinkowitsch—I honestly do not know the answer to that. I suspect they would be but the extent is something that, say, high-tech crime ops or others would be available to answer, I am sure. In terms of industry engagement, though: government has some very real capability and skills and so on, but if you really want that agile and adaptive capability to meet something that comes out, or where it is not within the specific realm of a government agency to take an investigation as far as, say, Grey Goose or Citizen Lab did, then there is a plethora of industry capability out there that is readily able to do that, that is able to do some open-source investigations into these types of things—to run a Grey Goose or a Citizen Lab type investigation. They will be agile and not limited by the means to go out and do a six-month procurement of buying a particular tool to enable them to do it. Industry will band together to provide a common platform to meet these requirements very quickly.

Ms REA—What is coming to my mind, though, is the legal status. I mean, if a group of like-minded citizens decided to catch a robber, they would be called vigilantes. I am not suggesting that that is what we would call these people, but there would have to be some legal status for whatever this network is—it would have to have approval to actually be an investigation and detection agency. Or do they act a bit more like a private investigator than a police force?

Mr Sinkowitsch—I think in its truer sense it is information available to you on the web that you just happen to be bringing together. It is all out there on the web. Nothing that was within either of those two investigations, for example, was proprietary information it was all available. With Grey Goose in particular everything was there on the web, you just had to go looking for it, find it and then do something with it, answer those questions around, ‘We have this information now, what do we do with it?’ You put it through some analytical and investigative processes to find some answers to the questions that you had. In terms of actual legislative requirements I am not entirely sure but my initial answer would be simply that it is all there. You are doing something with the information that exists already.

Ms MARINO—I would like to explore the mandatory reporting side of things a bit further. Does mandatory mean legislated?

Mr Sinkowitsch—Yes.

Ms MARINO—There would have to be a process for doing so and a way of monitoring whether they are or not. How do you see that mandatory reporting process then evolving from a

legislative point of view in how that information is passed on, given that there are a range of commercial issues for companies in that reporting process and what that might or might not do to their businesses? How would you see the process of mandatory reporting? How would the agency responsible for the reporting and its audit process work but also how would the mandatory side of it be monitored?

Mr Sinkowitsch—As far as the specific legislative process and requirements go that is not really for me to discuss. In terms of the sensitivities around the information, clearly, there would be some highly sensitive commercial information that would come in. I would suggest that there are models already in place around that, for example, AUSTRAC in its anti-money-laundering role would have some pretty clear and concise reporting requirements but also barriers around the confidentiality and sensitivity of it all. There is probably a reasonable model there already. I am sure there are other reporting mechanisms that would be similar, ASIC, for example, would have similar sorts of things. Yes, you would have to be very cognisant of the sensitivities of the commercial information in particular but I do not see that as insurmountable. They are already largely in place with different slants.

Ms MARINO—What responsibility do you think that ISPs have in security, scanning their networks and actually dealing with these issues?

Mr Sinkowitsch—There is only so much they can do. In reality you can put as many roadblocks in the way of cybercriminals as you want but they will always evolve to meet and defeat those activities. By definition, a lot of what they have to do is reactive. When a new and evolving threat emerges they will need to react to meet it. We are dealing with some very clever people here. I am sure the ISPs have their own very formalised views on all of this. Mine is simply that to a point they can only be as reactive as they can be.

Ms MARINO—On the liability issue for a user, someone who has a computer and who has got onto the internet, say, they have come across a problem which has cost them money and they are seeking then to hold someone accountable for it. Where do you think, that liability lies for the end consumer, being the person with the computer?

Mr Sinkowitsch—It is the age-old problem of self versus others. It is always somebody else's fault. Again I would say that there are mechanisms in place around the Telecommunications Ombudsman for example. It is a very difficult question for me to answer because it would be totally scenario dependent. There would be times where it would be totally my fault because I did not follow the instructions, my AV software was not up to date and I was looking at sites I should not have been looking at and there would be times when I think I have done everything correctly and followed all the procedures but I still got scammed. Perhaps there is justification there in following that path. It would have to be on a case-by-case basis. I do not know that you could apply some blanket terminology around it.

Ms REA—Is there more that ISPs could do, because there is a lot of discussion about personal responsibility at the end user level? Could ISPs do more to protect their users from that or is it something that you have to deal with at the actual computer?

Mr Sinkowitsch—It is both. If you look at the larger ISPs, they clearly have interests to protect and will go down certain paths to ensure that those interests, their market share and so on are protected. Nobody wants their ISP to be seen as open to cybercrime.

Ms REA—Sure.

Mr Sinkowitsch—The larger ones obviously have that commercial interest, but the smaller garage-driven ISPs, if you like, perhaps do not have the financial backing to implement those measures or perhaps they are not so interested in it. There are other organisations that are far better placed than I am to answer those sorts of questions.

Ms REA—One suggestion this morning, very simplistically, was around a star rating when it came to software or even ISPs, and that people make decisions about products based on a whole range of criteria. For example, instead of an energy rating for a fridge, you could have a security rating and if people want to pay for a cheaper product that offers less security then that is their choice. Is that too simplistic? Could something like that give people the opportunity to have a choice while also being aware that if they are paying for less then they are more at risk individually?

Mr Sinkowitsch—It is a possibility that is worth exploring, but then you get into other issues. If it is a white good, for example, you test it once and know whether it has decent security or not. If it is a piece of AV software it will be updated every day. Was it as effective yesterday, as it is today, as it will be tomorrow and does its star rating change?

Ms REA—Sure, that is a good point.

Mr Sinkowitsch—We have implemented government networks that use more than one AV solution because product A may be very good at a specific type of attack while product B might be better at another specific type of attack, so combined hopefully you are meeting as many of the attack types as you can.

CHAIR—What do you think is the best security currently on the market for individual personal computers?

Mr Sinkowitsch—Me personally?

CHAIR—Yes.

Mr Sinkowitsch—I would rather not comment on that. We implement a number of different types across networks, and often that is driven by a specific requirement of a government department because they already have a commercial arrangement, whether we believe that that is the best or not. We might let them know what our thoughts are around meeting their specific needs, because each need will be different. That comes down to the partnership arrangement as well.

CHAIR—In your submission you talk about making penalties higher. How much higher? How high a level is appropriate, and why do you think that would assist, other than obviously punishing people more severely?

Mr Sinkowitsch—In terms of punishments, the general feeling—and we have had this in discussions with government agencies themselves—is that the legislation as it stands at the moment is not where it could be. Whether that is because it does not address an area specifically or it does not effectively provide enough of a deterrent, I do not know. There are all sorts of ifs, buts and maybes there. In terms of levels of fines, I do not know. You get to the squeak or groan factor, where speeding fines are pretty unhealthy these days and most people do not speed as a result.

CHAIR—I think it is more the points that prevent people from speeding, rather than the fines. That is my personal opinion.

Mr Sinkowitsch—That is entirely possible. It is for others to assess where they believe that groan limit is. When you are dealing with transnational agencies with a business address somewhere in downtown Moscow, I do not know that any deterrent, fine or whatever would be enough. It is a means of implementing other measures to make sure they do not get to Australia to implement the attacks.

Ms MARINO—Michael, you touched on the issue of the potential lack of sharing of information between federal and state agencies—or the silos, if you want to call them that. What would you see as not being shared, and what else do you think needs to happen?

Mr Sinkowitsch—There is always a capability for greater transparency and information sharing between agencies. There is the whole dilemma of ‘need to know’ versus ‘need to share’, and it has continually come across no matter what specifics you are talking about. So I think that, in terms of governments sharing information, there will always be a need to adjust and amend as you go along the path. We need to keep in mind that this is a continually evolving technological threat as well. I am certain that there are liaison groups amongst the three levels of government here in Australia that look at dealing with all of that. I would suggest that there is always scope for improvement of that as well.

CHAIR—I think that is the end of our questions. I very much appreciate you coming in.

Mr Sinkowitsch—My pleasure. Thank you very much for your time.

[2.14 pm]

MacGIBBON, Mr Alastair, Director, Internet Safety Institute

CHAIR—I now call the representative of the Internet Safety Institute. Thank you for making yourself available; it is much appreciated. Do you have anything to say about the capacity in which you are appearing before the committee?

Mr MacGibbon—I am the founder of the Internet Safety Institute.

CHAIR—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 start with an opening statement? I see you have a presentation for us.

Mr MacGibbon—I have taken the liberty of giving you some copies of it. I have a PowerPoint presentation that we may or may not refer to, depending on how your questioning goes. I am conscious of the fact that it is probably best to respond to questions but I will offer this very briefly. While I am the founder of the Internet Safety Institute—and that is quite recently—I believe I can add value to the committee's inquiry through two of my past employments. The first position was as a federal agent with the Australian Federal Police and the founding director of the Australian High Tech Crime Centre, which has since evolved into Australian Federal Police High Tech Crime Operations.

Ms REA—So you are the person we should have asked all the previous questions of?

Mr MacGibbon—You can feel free to ask them, but we might not have enough time! As for the other position, most recently I was the trust and safety director for eBay Asia-Pacific, therefore I dealt with what happens to consumers in the internet space and I dealt with government from there. The perspective I would like to bring to you today is one of trust and confidence in the internet and a perspective of how government operates, with, as of now, an outsider's view of industry as well.

I believe the most effective way for the committee to look at this is through the eyes of a consumer, because it is when one looks at this issue through the prism of the consumer's perspective that we see that this is neither virtual crime nor cybercrime. This is real crime that happens against real people and it needs to be dealt with through real world solutions. These are the types of solutions that I would like to bring before you today. You now have a choice. It is like pick a box. I can go through with you some of this more structured documentation or you could contact me afterwards to go through it. Otherwise, I can answer questions.

CHAIR—I would not mind if you would actually go through your presentation, because obviously you have a fairly unique perspective that we have not seen.

Ms REA—I agree.

Mr MacGibbon—Absolutely. We will have an electronic presentation.

A PowerPoint presentation was then given—

Mr MacGibbon—You now have material in front of you and up on the screen. There are distinct differences between the online and offline criminal spaces. Perhaps most importantly, from a motivational sense for a criminal, is a presumption of anonymity. I use the word ‘presumption’ very importantly because in many respects people are not anonymous online but there is a strong presumption that they are. Other drivers include the fact that there is indeed a very low likelihood of one being caught as an offender. I ask you to put yourselves in the shoes of the real world criminals that we have all grown up with, so we will take that perspective and then look at that crime through the consumer’s eyes. These things are pretty rational and understandable.

The other thing is of course that online crime is indeed profitable. Many people who have gone before me today have explained and many people who will come after me will explain just how profitable it can be. Very importantly, that profitability comes with scale. It is easy to scale an online attack. It is easy for me to conduct child sex activities in the online space to scale. The internet brings that scale, both good and bad.

The last one is that there is plenty of opportunity for one to commit a crime online in that the machines themselves and the users of those machines are vulnerable, sometimes vulnerable through lack of experience and understanding of the consequences of their actions. Other more basic aspects go to the actual vulnerability of the security of the machine itself, which I think has been adequately covered today.

One of the reasons why there is a low likelihood of both detection of and prosecution of an offender online is given on the bottom layer of that first page of the presentation, which you have. Primarily, the biggest problem we face when we try to find an offender online and prosecute them is that of jurisdiction. A great thing about the internet in a positive sense is that we can all receive information from and indeed do commerce with people all around the world. But the offenders themselves will often reside in a jurisdiction other than the one that we sit in and other than the one that the law enforcement agencies are in. In fact, the evidence may lie somewhere in between those jurisdictions or in many of them.

I come to volume, in this sense. Volume combined with the incremental nature of the offence means that the individual crime that is committed may actually be quite small but it could be spread, as I have said, across many jurisdictions with many hundreds or thousands of victims, all of whom have an incremental loss. It is the volume of reporting that actually becomes problematic for law enforcement agencies, given the fragmentation of the reporting, if indeed it is done, and the inability to aggregate those criminal complaints to see the true picture.

Sadly, the next observation I would make to you is that one of the reasons why we do not actually catch a lot of offenders online is the capacity and the drive of investigating agencies. There is indeed still today unfortunately a mindset that says that these crimes do not necessarily reach the same levels—but the average consumer online who is victimised would think they should be investigated—and often they are prioritised out of investigating agencies’ menu of

work. And, perhaps most important of all, many victims do not indeed know that they are victims.

When I was asked to set up the Australian High Tech Crime Centre in late 2002, this in many respects was an esoteric task. In the seven intervening years, there has been a dramatic uptake of technology—a staggering reliance upon it to a point where these things are no longer acceptable to a society that relies so heavily upon technology.

In my next slide I try to give some sense of the evolution of the crime. It would be fair to say that in 2002 we were looking at the attacks against government and corporate systems. In many respects, online crime was a cottage or handcrafted attack. Someone would very carefully decide to attack a corporate or government system. We were set up in the High Tech Crime Centre to look at those deliberate attacks. Yet in 2009 what we see is that the potential victim base has expanded quite rapidly to anyone who uses technology and is connected to the online space. The attacks themselves are industrialised and scaled, which means also that they are automated and can be perpetrated against anyone online.

The tipping point was really around 2003 with the advent of phishing, a crime which I presume the committee has heard of. While it is not necessarily the most devastating crime, it showed anyone who looked at this crime type that criminals realised that the average consumer at home and small business held information of value to the criminal if only they could work out a way to get to it. It was at that point that the scale and jurisdiction of the threat moved much beyond the capability of agencies to deal with it. Rather than going against a centralised bank system that might have the details of five million account holders, what if the criminal attacked the account holders, who are largely unprotected and do not know how to operate their machines, at home? The criminal can get exactly the same information with a very low likelihood of detection and an even lower likelihood of prosecution.

We have seen that malware, the malicious code that exists online, has proliferated. It combines with social engineering, the ability to get you to make a click that you otherwise would not make, to make it attractive to visit the site that leads to the malware. Often in this debate you will hear about either people's behaviour or the IT security vulnerabilities, but to me they combine to lead to the problem—that is, that the machines we use today, whether the iPhone that sits in your pocket or the machine you use at home, are technically vulnerable by their very nature. My actions can compound that vulnerability to a point where I can almost guarantee that I will become a victim.

It is easy to sit before this committee and talk about the doom and gloom and our inability to act, but I never sat in that space when I was in government and I certainly did not sit in that space when I worked for eBay. I genuinely believe that there is some form of road map or structure which can help us. Again it is for the committee to decide whether or not what I am saying has any credence, but I believe that there are things we as a society can be doing to protect ourselves today, collectively, governmentally, industrially and as individuals. I have made this slide a build because it is a bit complex when you look at it on paper. The first element is building it around the consumer. As I said in my opening comments, this should be looked at through the eyes of a consumer. The consumer obviously needs to provide some form of safety and security for the device that they use. It goes without saying that that IT security product may or may not always function effectively. The consumer obviously needs to have some

understanding of the consequences of their actions, and it is incumbent upon all of us, on- or offline, to take some degree of responsibility.

CHAIR—Is that ‘Act safely’?

Mr MacGibbon—Yes. Then there are online businesses themselves, those that make money online and that we have an arrangement of trust and confidence as we engage with them. Those online businesses can be consumers themselves in the online space, but they can also provide a service. They very clearly have certain responsibilities to actually look after the data that they collect from individuals, financial data in particular. Credit card details, for example, are a regular target of criminals in the online space because they mean money, and criminals online are motivated by money just like they are in the offline space when we deal with this type of crime. They need to also invest in the safety of their customers. If you make money from your customer you should be reinvesting a certain percentage—although I do not know what it is—in the trust and confidence of your client base in the online space. For many years I have said that the internet is a cheap channel not a free channel. You can make lots of money online but you can also lose lots of money online as a business. No business should set itself up in the online space and believe that it should not invest in the security and safety of that space, because they are the same as its responsibilities in the broader community. If the community itself has a malaise and a lack of trust they will not be spending the money in their store, and the same occurs in the online space.

Ms MARINO—From the research that you have done and the information available to you, what percentage of businesses are very aware or engaged in the mitigation of the risk?

Mr MacGibbon—It is generally less than what we would hope as consumers. There is no doubt there are some very responsible companies online. Generally speaking, if you build a legitimate business online—and clearly there are illegitimate businesses online; they tend to flourish—and you have no offline process, you know well the full weight of the challenge that the internet poses. It is both a potential source of great money and an extraordinarily acidic place to do business, so you invest quite heavily.

Perhaps where some of the learnings are yet to be had by businesses are among those that have operated in the offline space and see the internet as a new cheap channel for them to acquire customers and deal with them. I would actually put government in that space as well. The No. 1 way in which Australian citizens now engage with government is online, which is terrific. But government agencies traditionally have used the internet as a way to publish their annual report and the physical location of their offices. Now that we enter into an actual exchange of information with government entities online, they need to invest, for example, very heavily in how to protect the information that the consumers have on their home computers and in that trust relationship between people divulging the information and the government entity holding it. So I would say that there is a gap. This often falls into the realm of the IT security person in a business. To me this is about consumer trust, and that goes well beyond the IT security of the transaction itself.

More broadly, those who provide what I would almost consider the roads of the internet have certain responsibilities, and there are things that can be done. For example, ISPs could require their customers to have a certain level of protection on their computers before they can get on

the internet. Let us think about it from a Parliament House environment. If you were to connect a computer today to the Parliament House systems, it is more than likely that the IT department will say: we can only connect certain types of computers onto this system and, if they are there, they need to be patched and running certain IT security programs before they are allowed to get onto the network. The same could be applied at the household level via ISPs. It may not be a popular proposition, but they could indeed do this and reduce the likelihood of IT security vulnerabilities in homes.

Then we have phishing, for example. I could register a URL today, an internet address, with practically no identification and a stolen credit card. I believe it is time for us to have a 'know your customer' regime on the internet such as that we have forced banks and other financial providers to have. That is, before MacGibbon can register himself a URL, let us identify that it is indeed him as best we can and that he has a right to the name that he wants to use. For example, should I be able to set up a www.bank.com.au account today in Australia? I would say no, unless I was a financial institution. But registrars, the people that actually issue these names that we type into our computers, never ask me if I have the right to register as a bank or maybe as a bank with one letter different. They have no interest in it. What they want is the 59 bucks I will pay them for the year to have that URL. As a consequence, we do not know who it is we are dealing with in the online space.

Ms REA—So there is no screening at all.

Mr MacGibbon—No. Australia has a slightly better regime, so I would hasten to add that we are in a slightly better place, where people, for example, have to give ABN numbers. But I could look that up online today—go to the ASIC website, take down an ABN and then use that as part of my registration process. But Australia is in a much better place, bizarrely, than somewhere like .com, which has more significant issues. There are incremental improvements we can make to the internet, coming from a regulatory and policy environment. I might have heard you laughing when I said that there were more things that government could do than the rest of us!

Ms REA—We always have the most action boxes—it is funny that!

Mr MacGibbon—Yes, that is because I am a big believer in government, having come from that space. Do not be put off by the number of boxes. In fact, there could be a thousand boxes on this page. I have tried to pick up what I think would be the key things. I would happily talk to these but I have actually hand selected three of this circular page on slide 3.

CHAIR—You have prepared three in advance!

Mr MacGibbon—I have prepared three in advance in the hope that the committee would find them interesting. I note, with interest, that most of the witnesses today have suggested that there is a lack of ability for anyone to report matters in the online space. Again, if you put yourself in the shoes of consumers today, it is a horrendously fragmented world. If you were a victim of an internet crime today here in the Australian Capital Territory, probably your first thought would be to go the local federal police office, maybe at Belconnen or Tuggeranong, and it is more than likely that they are going to ask you where the offender resides because it is the jurisdiction of the offender that matters.

You, as the average consumer, are not going to know where the offender resides but: 'I think they might reside in Victoria; that is what they told me as I engaged them online.' They will tell you to go and report the matter to the Victoria Police. They will not know necessarily how to tell you to report the matter to the Victoria Police, but you will go home and Google it, which is what the rest of us do to find out how to do anything online. As a consequence, you will find the contact details for the Victoria Police, who might take your complaint; they may not.

If I thought it were an Australian company that was doing me out of money I would go to the ACCC, and they would do a check to see whether or not it was indeed an Australian registered business. The company told me they were, and I dealt with them assuming they were an Australian registered business, but I find subsequently that they were not. ACCC are no help to me either, nor is any state or territory office of fair trading. I am left in limbo to the point where I cannot actually make a complaint. But if someone were keeping any records of the number of times and places I have had to go to, I probably reported it to five or six places. I am angry, I am upset and I have no recourse before a court and, indeed, if an agency does eventually take my report it is unlikely to be aggregated with all the other victims that are out there to find an offender.

This brings me to the concept of an internet crime reporting centre. There are many ways that we could address these issues, but, as you can see on slide 4, there are certain attributes that I believe any internet crime reporting centre should have. It has to operate 24 hours, seven days a week, just as we expect any other reporting agency these days to operate, particularly an online one. I believe it needs to be a public/private partnership. It may well indeed be hosted by private agencies; in my discussions over the years with corporates, both from a government perspective and a corporate perspective, there are many companies that would like to help in such a regime, but there has never been a lightning rod or focus point for that. I believe government and, particularly, police services would have to learn what large-scale reporting really involves, because we are not talking about incremental numbers here; we are talking about large numbers of incidents that occur in a very fragmented way. There are lessons that government can learn from running contact centres by private industry, whether they are banks or internet service providers or others.

That information then has to be linked to like-minded agencies offshore because it will not be uncommon to find that the trail leads to a jurisdiction outside Australia.

Ms MARINO—Who would you see the crime reporting centre being available to—the average person as well?

Mr MacGibbon—Absolutely.

Ms MARINO—In that instance, if someone has a problem with someone trying to access their bank information, or they believe someone is trying to get at them via their bank details, they could contact this organisation as opposed to their bank—directly, or as well as?

Mr MacGibbon—The devil is in the detail. I would never want to stand between an individual and their money. If the best place to first report the matter was a person's bank, because there was an active draining of a their bank account, then the last thing you would want

in running a centre like this would be the person holding the ball when the music stops and saying, 'You knew about it and you did not refer it to the next institution.'

Ms MARINO—I was just wondering about the process for an individual who has made the call.

Ms REA—But under law you would have to report it to the bank anyway, because a third party could not report your details to the bank, could they?

Mr MacGibbon—I think it would depend on the composition of the entity itself and what agreements are in place between institutions. I do not know the answer to that.

Ms REA—Yes, but you would have to give the details yourself, surely?

Mr MacGibbon—All I know is that it is time for us to discuss this in earnest. Again, there is no way we will solve this in an hour or 10 or 20 hours. But it is now time for us as a nation to start to ask the question: how does the consumer contact government? At the very least, even if this were a crime-reporting centre, the consumer should be able to come to one place and let the government work out the bureaucratic morass at the back end. I am not proposing that this entity be the be-all and end-all of internet crime investigations—that is, that they take the complaint, investigate it and prosecute it. I am saying that there needs to be a front door to which a consumer can come and say, 'I believe something criminal has been conducted against me.'

Ms MARINO—Yes, like a one-stop-shop situation.

Mr MacGibbon—Then they would let government at the back end, with industry, work out where it should go. It might be a civil matter, as many are online. It might be a criminal matter, and it might be a criminal matter that at first glance looks like it is a Victorian matter but as you investigate further and get more complaints you find it is an offshore matter. At the moment we do not have the ability to take enough of that information to actually make a good judgment call. It is at the point where agencies themselves do not take the information because it is worthless. The last thing you want is a criminal complaint on your books that you can do nothing about. Victims have rights, as they should, and I need to keep them abreast of my investigation—and it may be nothing because it may be so small. Then I have to let them know that I am not going to take their matter any further, which is the proper thing to do if I have only one complaint. But how do we know that it is not connected to a much larger crime? Indeed, as I finish off on that particular build, I know there are some very smart bits of software that we could use to help control the volume and the passing out of information in an automated way, but it would need to be staffed.

The outputs are very important for the committee to note. Firstly, any statistic you hear about online crime is going to be dodgy by the simple nature of it, because we cannot collect the stats. At the very least, a centralised place where people can go to complain to government, whether state or federal government, will mean we will have the ability to start measuring this crime type. From there we could have a rational discussion about how heavily we should be funding other aspects of government. It would allow the referral of the crime to the relevant agency for investigation. It would also give us the ability to siphon off strategic intelligence products to feed back into government, and indeed into industry, about how people can protect themselves

against the threats that are occurring against our common consumer base. Very importantly, it could allow for the real-time transfer of the threats to and from private institutions. In the case of credit cards, for example, it might well be that the credit card issuers would have a very strong interest in knowing that a particular batch of credit card numbers had been compromised, because there might be another batch that the government did not know about that was compromised at exactly the same point. Being able to act together with that same information would allow us to reduce victimisation.

Very importantly from a consumer's point of view, it would give a sense of immediate action. It might well be remedial advice. It might well be referral to a site that tells them to download certain antimalware and virus protection because their computer is totally open. It might ask them to at least reduce the likelihood of being victimised next time. Or we might choose to educate the consumer about phishing sites because clearly they have been the victim of a phishing attack. It provides an opportunity to educate a person at a time when they are going to be quite open to that concept.

The committee has heard quite significantly from other witnesses about the concept of a public health style education campaign, and I strongly advocate for such a campaign. That campaign would need to be designed to change basic behaviours. There are probably several hundred things we should all be doing sensibly online today. Having worked in industry, I would be happy if people did two or three of them. I do not necessarily know what they are—patching your system and having antivirus software and a firewall would be a good start, and something about how one behaves online would be sensible as well. But we need to come down to a very small number of behaviours that need to be changed. The changes need to target not just the security of the system but the safety and the behaviour of how one uses those systems. I could have a bulletproof computer and, I guarantee you, I could still get into trouble. Equally, I could drive very carefully on my computer, but if it were vulnerable to IT security issues I could equally end up in trouble. So we need to be addressing both the technical aspects of the computers themselves and, indeed, the way in which we use those computers. The education campaign needs to be sustained, and for years from both inside and outside government I have asked government to have a consistent approach that goes beyond a week or a month to tackle this issue and address the concerns and questions that the public have.

It needs to be built in from the very earliest years, from when one first touches a computer. The best place for that, of course, is the education system because that is where all the children are going to have some form of interaction over time. The people who have probably the closest relationship with consumers are the corporates and many of them are willing to deliver this message free of charge, but they need to have an agreed content. They have a regular dialogue with their customer base and many corporates I have dealt with over the years are more than willing to take a security and safety message out to the people who interact with them.

Importantly, as with any expenditure of public funds, the outcomes need to be measurable. I would urge the committee to think of public health style campaigns. We do not do a Slip, Slop, Slap campaign without measuring, I hope, whether or not people are applying a more and higher SPF sunscreens and wearing hats because we need to measure whether the public expenditure is working. Has it changed the culture of the online space? Indeed, we need to be addressing the low-hanging fruit, as in the most easily addressed issues, in this discussion. My hoped for output would be that it would reduce some of the unnecessary victimisation that occurs online. It is

certain that education in its own right will not solve this problem. What it should do is reduce the likelihood of people being victimised perhaps to a point where law enforcement agencies can then investigate matters that should be investigated rather than the system being clogged up with victims who are victims because we have no system in place to protect them.

The last prepared slide, which I am happy to skip if you are getting bored, is the concept of ISPs enforcing end-point security. It is a contentious one. I am sure I will not be much loved for saying it.

Ms REA—We have been throwing this around all day.

Mr MacGibbon—I think it is important for us to raise as an issue even if it eventually gets knocked out of contention. As I say, in a corporate environment today if I were to plug my laptop into my old employer's network, the system would check whether or not I had patched my laptop to the point that the corporation believed was acceptable. It would check whether I had the latest antivirus signatures uploaded and whether I had a personal firewall in place before it would allow me access to the corporate network. It is one way of reducing the likelihood of my computer, as I connect to that network, being rogue. It does not protect everyone, but it reduces the likelihood of something going wrong.

Again witnesses today have said what a huge social value would arise from a National Broadband Network and I agree. But rogue computers on those networks will cause even greater problems for the rest of us because a computer that is connected to a much larger pipe can cause more damage and it will indeed be a target to criminals elsewhere. What if, as I plugged into the National Broadband Network, the security standards had been set by the NBN administrators to say, 'MacGibbon's computer, as with any other computer connecting to this network today, using network access control type technologies, must have some form of recognised antivirus or firewall on it and his system needs to be patched.' Before I could actually do anything on the network, it would check those things and if I am not patched, it would be the first thing my computer did before I could execute any other activity online.

Today, if I said that people would say, 'You're going to wreck my download speeds and it's going to take five or 10 minutes before I can look at my YouTube videos.' That is true. But with the National Broadband Network of such huge speeds straight to my front door, this would take seconds, if any. So we could build a system with the National Broadband Network that allowed us to have some degree of confidence that end-user computers had protection.

What about the computers in the staggering number of Australian households that have no such protection? There is no real statistic out there. It could be anywhere from 30 to 50 per cent of households that are not actually protected when they are connecting to the online space. What about those people? We do not need to deny access to the National Broadband Network for those people. We could download a temporary program that protected them. We might turn on their firewall for them. A lot of software comes with some type of software firewall that can be flicked on and off. It might be that we provide them with antivirus protection at least for the time that they sit on the National Broadband Network.

Those who are fearful that the government would be leaving some type of software on a person's systems could make sure that that software actually dissolves when they turn

themselves off from the National Broadband Network. Each time they came onto the network, it would reload the required antivirus and other protection and, as they logged off, it would disappear again. Indeed, the user might be prompted to go and buy themselves some form of protection. We might allow them a certain number of accesses before they get kicked off the network. It could be contentious, but it is certainly something I think we need to consider as a modern nation where technology is relied upon so heavily. With that extraordinarily long non-introductory statement—

Ms REA—No, that was very useful.

CHAIR—It certainly covered some issues that I have been thinking about during the day, particularly on what ISPs should do to assist us. I do not know if you were here when we were talking a bit about some of the more basic things. There is obviously a bit of resistance there.

Mr MacGibbon—To be fair to ISPs, there is something you will see on my complex circular chart that is revolving around the consumer. I hope you notice that. As I said, we should look at these. It took me a while at home, as my PowerPoint skills are not great, as many who have worked with me will attest. I do put in there the concept of safe harbour regimes to protect good faith actions. That is what the ISPs were mentioning. I can understand that.

During one of the breaks I was having a discussion. To use eBay as an example—so we will move away from ISPs—if a particular computer did something bad on the eBay network, you would think it was within eBay's rights to say, 'We're not going to allow that computer to have an account with us anymore because that person defrauded another user or committed some form of action that led to loss for a company.' So you might choose to not allow that IP number—that unique number that comes up with my home computer each time—to register an account anymore. So you block it. A person would then contact the company, or contact someone else to make a complaint that the company was not providing a service. On what basis would they make that complaint? The trouble is that that IP number and that computer could be used by a number of people. Why should you punish everyone else in that house for the actions of one individual? So the company might, from time to time, be almost forced to allow someone who they suspect will commit a future wrongdoing back onto a system.

I can understand why ISPs would say: 'Wait. If you are telling us we should be taking down websites that have malware on them, that is all well and good, but what about if the business does not care—they are running a legitimate business but have just taken no IT security protection into account—and they are making money on that website and we, as an ISP, take that website down?' They are somewhat at a financial loss. While I as an ISP am taking that down to try to protect other users of my network, the music has stopped and I am holding the parcel. So I can understand why they would ask for safe harbour type provisions. If they act in good faith, either at the request of government or because they have detected someone acting anomalously—and there need to be some definitions around; people more technical than I would have to define them—then they should be protected legally for taking that action to protect the rest of us. What that threshold is, again, is for smarter people than I, but there should be some provision in place to do that.

I can understand their reticence, because a lot of people blame an ISP because they deliver packets. We have never really asked them to do much before. But I do believe that everyone who

operates in the online space—whether it is e-commerce companies, banks, ISPs or, indeed, householders themselves—has a responsibility, frankly, to lift their game. It was too easy for us in the early 2000s to say, ‘It is really no one’s responsibility,’ but in 2009, when everything we do today—whether it is governmentally, business-wise or privately—has some piece of technology involved, it is incumbent upon us all to understand what our responsibilities are.

CHAIR—It has gone from no-one’s responsibility to everyone’s responsibility.

Mr MacGibbon—Indeed, and part of that is because we did not act when possibly we should have. I think the government really, in the early 2000s, was ahead of the curve. What we have seen in that time is that technology has sprinted so far ahead and our appetite for it is insatiable. As a consequence our social discussions have really lagged behind.

Ms MARINO—With your vast experience, one of the things I would like to know is what the real obstacles are for tracking the real location and identity of an alias in another country. What are the real obstacles for those engaged in that process?

Mr MacGibbon—Part of it comes down to this concept of knowing your customer. It is a fair bet that an Australian internet service provider will know most of the people who are connected to them. There are going to be landlines and other things—mobiles. Part of it has to do with what information is collected at the point of registration and what level of veracity that documentation has. Was it fake credentials that were presented to the person at the time?

It is possible to be anonymous online, but what I would say is criminals make mistakes just like the rest of us do and criminals are creatures of habit. So it is technically possible to commit the perfect anonymous crime online, if you want to do it once and you are really smart at covering your tracks. But the average crook is not that smart online, just as they are not offline—which is why we catch people, offline as well as online. It depends on whether or not Australia has arrangements in place with the jurisdictions where either the evidence lies or the offender resides to exchange that information. Australia is actually very well placed for that. The Australian Federal Police, to its credit, has invested very heavily in international liaison. What it needs to do, of course, is apply that international liaison network to this technology crime question, and I would say it would be pretty hard to hide anywhere. If you truly wanted to find the person, at some point they will be found because they will trip up and make mistakes. I will give you an example and it will sound silly. I have been receiving some really nasty text messages recently—

CHAIR—I get some of those: ‘Send me \$10,000 or will kill you!’

Mr MacGibbon—This person is saying some quite offensive things to me as an individual, so I googled their mobile phone number. That person has actually been selling something online and has the mobile phone number that they are using, so I now know where they live and what their vehicle registration is, for example.

Ms MARINO—How stupid is that!

Mr MacGibbon—If that person was a smarter person operating online they would have a mobile phone number that is not connected to some other thing that they did.

CHAIR—Are they from overseas?

Mr MacGibbon—No. This person resides in a different state, and if they keep sending me text messages of the same ilk I will take some type of action. But the point I was trying to make is that this person thinks that they are anonymous because they are sending me a text message which comes up purely as a however many digit number on my phone but they have used that number somewhere else.

Ms MARINO—They have not even covered their number?

Mr MacGibbon—No. And even if it was a private number I could go to my carrier and say, ‘I am receiving text messages from somebody with a blocked number,’ and they will be able to identify who it is. So this sense of anonymity is as much assumed as it is real, and yet it empowers people to do silly things.

Ms MARINO—But the average consumer like us is not aware that those opportunities are there for us in that situation to take it a step further. For an individual, what constitutes enough of an issue for the AFP to decide that they will take on the case and investigate, because they can, as you say, find who this is? How does the individual know that that is a case or an issue that is sufficient to the AFP to pursue to the nth degree?

Mr MacGibbon—Is an excellent question. Unfortunately there is no answer. I cannot answer for the AFP’s current practices on how it prioritises matters. But what I would say is that I understand why most matters are prioritised out of existence: because there is no centralised gathering of the various victims. It goes down to a bank fraud where there is one victim of \$10 million versus 10 million victims of \$1. The criminal makes off with exactly the same amount of money, but I know which type of crime, if I had the wherewithal to do it, I would prefer to be doing as a criminal. The \$1 victim is going to get laughed away, and in fact it will cost the police more money to even open the matter to investigate if there were indeed other victims.

Ms MARINO—And that is if they actually reported it, because most people would not consider a \$1 crime to be worth pursuing.

Mr MacGibbon—Indeed.

Ms MARINO—You probably would not even notice.

Mr MacGibbon—Yes, does anyone ever check what those various things are? That is no offence to the banks about fees and charges. It is just there on my statement and I do not know what it is. There would need to be one person who comes forward and says, ‘Hey, something has happened,’ and then another one in some other place that would allow some form of: ‘Well, is there something there? Where there’s smoke there’s fire. And we’ve found that it is with the same institution.’ So maybe we have to go back to the institution and say, ‘Hey, have you got lots of these \$1 things occurring?’ This comes down to the fact that you have to get the victims coming in through one front door, because of the concept of jurisdiction and the volume and the incremental nature of most of the offences in the online space. There are always going to be big, large-scale silly things that happen online, and those things attract the attention of law

enforcement agencies, governments and the media. But the incremental gnawing crime that occurs at a very low level is possibly bigger than those big offences.

Ms REA—I suspect that, whilst I can believe that the \$10 million by \$1 crimes occur, the institutions that have the most up-to-date secure systems would be financial institutions. I may be wrong, but I would assume that they are the ones who have the most vested interest in protecting their online database and transactions. But getting back to that first slide—and I noted down that you said that cybercrime is profitable—it seems to me, from what has been emerging over the period of this inquiry, that the profit is not so much in the person who actually takes the money out of somebody's bank account; it is actually in the sale of the information.

Mr MacGibbon—It is actually an economy.

Ms REA—Yes. You are not going into a bank to defraud someone's account, because you would imagine that a bank has probably got the biggest security system, but through all sorts of other, less secure websites, through phishing, emails, scams or whatever you can at least gather enough information from a large volume of people that you would then onsell to somebody who actually does want to perpetrate a fraud.

Mr MacGibbon—It is actually a combination. There are indeed people who are going to commit the crime directly themselves and then there is a very active trade in information that could be worth something. Ultimately, what a criminal wants to do is convert something of notional value into actual dollars. One thing I neglected to say to the committee, which I should have, is that criminals have been extraordinarily efficient at the front end of their criminal enterprise. We need to presume that our information is compromised, that our credit cards, email addresses and other things are compromised. It is fair to make that assumption. Where we as a community have been protected is by the inefficiency in them converting that information into real cash.

As an example, I will use the recent arrest in the US of a guy called Gonzales, who is now being held responsible for the compromises of the Heartland credit card processing facility, and of Hannaford's, which is a retail chain, and a few others. He has been pinned to all of these crimes as the guy who compromised all these hundreds of millions of credit card details. The guy is not a multibillionaire. He earned more money than the average person. But he is not a multibillionaire because he could not convert those hundreds of millions of credit cards into real cash because he still had to work out ways of how to perhaps onsell them en masse, to perhaps break them up into bits to sell to a gang which wants to run those credit cards through one system or sell them to a Russian group. They do not make pure money. It is actually at the back end of their criminal enterprises where they have been less efficient, which is good for us. My fear is if they get more efficient at the back end they will be able to use all this information. Whether or not we like it, even if we just raised all the walls today and fixed the problem, there is enough information out there and stockpiled to last a fair while. That is where my real fear lies: if criminals get better at the back end and convert that potential money into real money.

CHAIR—Thank you, Mr MacGibbon. That was very interesting. Thank you for the diagrams you have given us. They have given us a lot of help towards where we might be going. Before I call the next witness, is it the wish of the committee that this document be incorporated as an exhibit in our inquiry? There being no objection, it is so ordered.

[2.58 pm]

HAMILTON, Mr Christopher John, Chief Executive Officer, Australian Payments Clearing Association Ltd

PEARCE, Ms Caroline, Head of Fraud, Risk and Compliance, Australian Payments Clearing Association Ltd

CHAIR—Welcome. I thank you for making yourself available and, in particular, for coming a little bit earlier at fairly short notice. It is very 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 should be treated with the same respect as proceedings in the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. I invite you to make an opening statement.

Mr Hamilton—I have a brief opening statement, Madam Chair, but perhaps first a very brief introduction about APCA. APCA is the payments industry self-regulatory body, not as highly visible as the Australian Bankers Association, perhaps, but concerned directly with payments activity in Australia. It is the primary vehicle for payments industry collaboration in Australia, and its core purpose is to continuously improve the payments system. Our major activities are self-regulation of standards, industry-wide change management and industry policy development and advocacy. Our interest in cybercrime comes from our desire to minimise fraud while maximising the efficiency and utility of the payments system. We have a role in collecting and publishing industry statistics on cheque, credit card and debit card fraud, as well as facilitating industry coordination on fraud prevention.

Like all areas of economic activity, payments are increasingly carried out online, hence the nexus with cybercrime. A relevant distinction that often arises in our work is between the payment itself and the underlying economic activity or transaction to which the payment relates. In cybercrime, we are vitally interested in fraud risks in the payment but are not tasked or resourced to deal with the broader fraud risks of the economic activity, and sometimes that distinction can be hard to draw. To take a straightforward example where I think it is relatively easy, if you were to buy a case of wine online using your credit card then our statistics and programs and our interest lie in addressing the risk that the use of the credit card might be unauthorised or that the payment data might be misappropriated in the course of that transaction and subsequently misused. We are not at all concerned—but others, of course, are vitally concerned—with whether the wine offer is a scam or indeed whether the wine is poisonous or any other aspect of the underlying activity.

Obviously, we fit into a matrix of many people who are combating cybercrime in this area. Financial institutions, card schemes, regulators and law enforcement agencies all have a role to play, and we take very much a layered approach to minimising payments fraud. Obviously, consumers and merchants are also important parts in that total picture.

Let me size the online payments fraud challenge by quoting briefly from our published statistics. In the 12 months ending December 2008, Australia's total payment card fraud rate was

around 32c in every thousand dollars, which is low by world standards. As a comparator—and not all countries publish this data, but the United Kingdom does—the United Kingdom is at the rate of around \$1.12 per thousand dollars, or £1.12 per thousand pounds, if you prefer. The statistics also show, though, that what we call ‘card not present’ fraud—that is the industry term which covers online payments fraud; it also includes other things like telephone and mail order activity, but the great bulk of it is going to be online—has proportionately grown significantly in the last two years. In 2008, it represented just under half of all credit card fraud, and that has grown in the last few years.

Sophisticated attacks by organised cybercriminals clearly target the financial sector. There is some limited data to support this. Verizon, a data security company, publish a data breaches report. In 2009, they indicated that the financial industry accounted for 93 per cent of the 285 million compromises of records that they found in their report. It is very hard to compute those numbers, isn't it, but clearly this is where the bang for buck is potentially for cybercriminals. Credit card information is the most common data targeted, representing around 12 per cent of all data breaches in 2008. That is according to another data security company, Symantec. Both of those reports are public, by the way. They may be relevant to the inquiry.

Payments institutions have a strong focus on detecting and preventing card and other online fraud. Industry codes and commercial practice, importantly, mean that cardholders are rarely out of pocket for fraudulent transactions. They suffer the inconvenience and the distress, if you like, but usually not the financial loss. Generally, online merchants and financial institutions pick up the tab, but then of course that is reticulated back through the system, so the total cost ends up going up. The rise of online retailing and the costs of fraud in that area to the community make this one of the major fraud challenges in the industry.

Financial institutions employ increasingly sophisticated techniques to identify and prevent fraudulent transactions. It is a sort of an arms race, as I am sure you have heard from many people previously. International card schemes develop techniques to reduce card-not-present fraud, including the use of additional methods for authenticating cardholders. There is a very widespread practice called CVC2—the additional numbers that you see on your credit cards—and there are online authentication mechanisms, such as Verified by Visa and MasterCard's SecureCode. They are both mechanisms for adding a layer of authentication to the online transaction.

More generally, there needs to be an ongoing balancing of costs and benefits in fraud prevention. The internet is fostering a vibrant and growing retailing channel. Fraud prevention techniques will continuously improve; but so will the fraud techniques, unfortunately. There is an unavoidable element of trade-off between security, cost efficiency and customer utility. Finding the optimal trade-off and ensuring the proper allocation of incentives amongst the parties involved in a payment is what drives efficiency, competition and innovation and also optimal fraud prevention. This is an ongoing effort, requiring solid data, effective collaboration and, above all, flexibility in the face of a fast-changing environment. Broadly speaking, our view is that the Australian payment system strikes that balance reasonably well at the moment, but the environment constantly changes so it requires reassessment. I am happy to answer any questions.

CHAIR—One thing that has been mentioned by a few other witnesses and that has occurred to me is the constant adding of additional layers of information to check the security of

payments, particularly credit cards. There are additional numbers; they ask for the name of your mother before marriage. The more that is disclosed, the more that is available and the more there is that can be used. Is it really effective as a protection to seek more and more information?

Mr Hamilton—It is a dilemma, absolutely. I think your previous witness indicated the lack of ability to rely on the card number itself because of the widespread context in which it is used. There is a very big focus in the industry on trying to minimise the risk of compromise of that card number through things like requiring encryption at each step in the cycle and preventing the storage of the card number unless it absolutely has to be stored. Those things all minimise the risk, but you cannot rely solely on those. It is necessary to have another layer of security to get the added comfort. That said, there are various techniques for minimising that risk. One-time passwords and things like that are all possibilities. A number of the financial institutions now use SMS based authentications. That is a one-time password system. That is not widespread in the credit card world but certainly is becoming much more common in other types of financial transactions. It is a constant battle but in fact continuous upgrading of security is another measure which reduces the effectiveness of fraudsters.

CHAIR—A lot of laptops these days—and I think I have seen it this actually used—have the capacity to have your fingerprint.

Mr Hamilton—Yes. I use a fingerprint based system on my laptop.

CHAIR—Wouldn't it be the absolutely foolproof method of preventing fraud online if, when you were making credit card payments, you had to use your fingerprint? I have no idea technically how you would do it.

Mr Hamilton—Neither do I, I must say.

Ms REA—Could you scan fingerprints?

CHAIR—It might be that you would have to have your fingerprint in the credit card and that, before you did a transaction online, the credit card you put in would have to match.

Mr Hamilton—I am not enough of a technical expert to be able to comment on the fingerprint part of it.

CHAIR—If you did that, unless you actually were doctoring your fingerprint—

Ms Pearce—A few years ago that there was a lot of talk about using fingerprints for authentication and it was widely believed that it was a really hard thing to forge. Then somebody came up with an incredibly cheap method of creating one. It was like a bit of rubber with a false fingerprint that you just put over it. It completely fooled all the systems.

Mr Hamilton—Perhaps they could be made better as well.

Ms Pearce—We keep thinking that technology will provide a really good solution and so many times there are problems. There is no foolproof solution. That is basically the problem.

Mr Hamilton—This is why we say there is an element of trade-off here. We would like to think there is an answer that does not impinge on cost or convenience and is permanent, but so far no-one has found that. I think it is unlikely that that will be easily found. These things are always a matter of getting the next step ahead of whatever the latest scam is. A new scam emerges and then you respond to that. It is a matter of keeping a lid on it.

Ms MARINO—I will go to your issue of the one-off number. Is that in any way responsible for the fact that, in spite of the increase in your statistics in the amount of online fraud, we have not had an even greater increase compared to, say, the UK? Has that been successful and is it worth doing elsewhere?

Mr Hamilton—I do not think that is primarily responsible for the statistical phenomenon that you are observing.

Ms MARINO—So what is?

Mr Hamilton—There are a range of factors there. One is sheer geography and economics in that we are a relatively small country that is a relatively long way away. That helps in terms of organised crime looking for the next target.

Ms MARINO—So they would operate from a centre like the UK where there are a lot of people in a small geographical area?

Mr Hamilton—Absolutely. We know for example that the UK has a very major problem with Eastern European organised crime, where there is a very systematised method of first of all compromising the card data and then taking and using that card data relatively effectively. Australia benefits because it is a little bit harder to get here. That said, it is happening and will happen to us as well. However, then you need to move to other means of reducing those risks.

One of the things which Australia has been quite successful at is minimising the possibility of moving that type of fraud into other areas. For example, we have a very widely used EFTPOS debit card system in Australia. You cannot use that online and there has been a lot of complaint about that over the years. You can use your ordinary ATM card in the shops to buy nearly anything these days but you cannot use that card online. That is a significant reduction in convenience but it makes that card a great deal safer and more secure and indeed all the fraud stats indicate that. What you have is a quarantining of the fraud, if you like, in an area where people are at least aware of the risk. That is a very material point because financial institutions, for example, put a lot of resources into detection programs and sophisticated ways of pattern recognition and checking to see whether a credit card transaction looks unusual. They spend the money on that because that is a way of minimising card fraud and do not spend it on EFTPOS debit cards because they do not need to.

Ms REA—You can use that account to pay for things online though. Those account details are accessible and you can pay bills. Indeed, there are some organisations or businesses that will not actually let you use a credit card online. You have to use your savings account rather than your credit account. So those details are there, but they are not associated with a PIN.

Mr Hamilton—That is right, so then you fall back on the ability of the fraudster to actually access the account having the account details.

CHAIR—You said that your organisation is undertaking strategies to reduce fraud, what strategies have you found most effective or are you not able to say?

Mr Hamilton—I think the key way to answer this is to talk about the layering of fraud prevention techniques. No one strategy by itself is a silver bullet. What you need to be doing is looking at each step in the transaction and trying to minimise the risk at each point. In card transactions, for example, there are minimum standards around the terminals that are used for cards and the storage and encryption of data. At the same time, the card schemes have frameworks for online authentication. You need to do customer education for consumers to be aware of and minimise fraud risk.

CHAIR—When you say customers, do you mean the banks or the customers of the banks?

Mr Hamilton—Sorry, consumers who are customers of the banks. There is a great deal that each individual person can do to minimise their own exposure and risk and so there is an education opportunity, if you like, there. There are also merchants as well, so a lot of fraud arises because the data is passing through a merchant and there needs to be some way of minimising that. Probably the most damaging card fraud problems that have occurred globally in recent times—I think they were mentioned by the last speaker—tend to be the large-scale compromise of large numbers of card details.

CHAIR—That does not happen when someone goes online and buys something, obviously they are getting the numbers from the source.

Mr Hamilton—Right, and generally one of two places—either a large merchant that has stored the data or a third-party processor working for a number of merchants who have stored the data. So, instead of getting a few card numbers or sitting there all day and getting a few hundred, you can get literally millions in one go if you can hack that system. The response to that and the way to shut that down is to have much stronger focus on encryption of relevant data in transmission and also preventing storage where it does not need to happen, and the global card schemes have a very big focus on doing that. Action on that is one of the things that have made a big difference.

Ms Pearce—It is quite a hard question to answer in some ways because if you have never had the fraud it might be hard to identify what it is that you are doing that stops the fraud happening. But maybe the thing that we could point to is protection of the PIN. We and our members go to a lot of effort to make sure that those PINs, when they are used, are secure. One way of doing that is not to allow them to be used over the internet.

CHAIR—But that is only ATMs.

Mr Hamilton—And EFTPOS.

CHAIR—Yes, some credit cards, but a lot of credit cards still have signatures.

Ms Pearce—That is true, but one of our rules is that you do not use the PIN in insecure devices—that is, you do not use your pin in internet transactions. We are aware that you use them in ATMs and in EFTPOS devices. We go to a lot of effort to make sure that when PINs are used there they are protected. Sometimes the information is transmitted over IP links, but it is strongly encrypted when that is done so that if there was a potential for a fraudster to be tapping the line they would not get those PIN details, and that is because of the standards that we use and the expense that our members go to to make sure that it is secure. The PIN is seen as absolutely fundamental to protecting people's money and is probably one of the things that have been most effective.

Mr Hamilton—Yes. Extending that into the cybercrime world, I think it is fairly likely that nearly all cards of all description, credit and debit, will rely mainly on a PIN rather than a signature at some stage in the future. For credit cards it is essentially optional now as to whether you use a PIN or signature, but at least one of the major credit card companies has already indicated that it is moving to full PIN.

CHAIR—Isn't there a greater risk for the consumer in using a PIN rather than a signature?

Mr Hamilton—That is the point I am coming to. I think it is very unlikely at that point that the industry will be comfortable with using those PINs online, for the same kinds of reasons that the EFTPOS system does not allow them to be used online. It is too easy for them to become compromised in that environment. For that reason you need an alternative authentication mechanism which is segregated from that PIN so as to reduce the overall fraud risk of that product. Something like the Verified by Visa or SecureCode type of product, which gives you a separate registration with a separate PIN, is probably what is needed. Again, the trade-off comes into play here. Those products struggle a little bit because of the inconvenience of having to register separately and get a new online passcode, so merchants tend not to want to offer them on their websites because it slows down the sale and increases the risk that the customer will lose interest at some point in the sale process and go away. Customers need to go through the process of registering, having their passcode and remembering it, which is another inconvenience. There does not seem to be a silver bullet for that problem.

Ms MARINO—You touched on the eastern European issue as far as the UK is concerned. Have you any knowledge, information or evidence of that sort of activity in Australia in relation to cards?

Mr Hamilton—Anecdotally, and in limited news reports, it seems reasonably clear that there has been some imported organised crime activity in relation to card fraud. Not online, to my knowledge—I do not know that I have seen that reported—

Ms Pearce—I have not seen it reported.

Mr Hamilton—but certainly in relation to physical cards. Skimming is the term we use for taking it off the card.

CHAIR—There was a group arrested in New South Wales recently where they were skimming the numbers and then a crew was coming over physically and using them to take money out of ATMs.

Mr Hamilton—That is right. Just to reinforce that point, we try very hard to protect the PIN and keep it away from the online environment because it is the way that people access their actual bank balances through an ATM. That kind of scam is quite separate from the cybercrime world, but it also needs to be rigorously detected.

CHAIR—As there are no further questions, thank you very much for coming. I appreciate the effort you made, particularly on a Friday afternoon. If you do not mind, if anything further occurs to the committee we might contact you for clarification.

Mr Hamilton—Of course. Thank you.

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 3.20 pm