



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

**HOUSE OF  
REPRESENTATIVES**

STANDING COMMITTEE ON COMMUNICATIONS

**Reference: Cybercrime**

WEDNESDAY, 25 NOVEMBER 2009

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

THIS TRANSCRIPT HAS BEEN PREPARED BY AN EXTERNAL PROVIDER



## **INTERNET**

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

The internet address is:

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

To search the parliamentary database, go to:

**<http://parlinfo.aph.gov.au>**

**HOUSE OF REPRESENTATIVES**  
**STANDING COMMITTEE ON COMMUNICATIONS**

**Wednesday, 25 November 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:** Mr Billson, Ms Collins, Ms Marino, Ms Neal, and Ms Rishworth

**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**

**BESGROVE, Mr Keith, First Assistant Secretary, Digital Economy Services Division,  
Department of Broadband, Communications and the Digital Economy ..... 1**

**CHIDGEY, Ms Sarah, Assistant Secretary, Criminal Law and Law Enforcement Branch,  
Attorney-General’s Department ..... 1**

**CORDINA, Mr Simon, Assistant Secretary, Cyber-Safety and Trade Branch, Department of  
Broadband, Communications and the Digital Economy ..... 1**

**EVANS, Ms Sheridan, Assistant Secretary, Identity Security Branch, Attorney-General’s  
Department ..... 1**

**HAWKES, Ms Marcella, Acting Assistant Secretary, E-Security Policy and Coordination,  
National Security Resilience Policy Division, Attorney-General’s Department ..... 1**

**MIHALIC, Ms Susan Ann, Principal Legal Officer, Telecommunications and Surveillance Law  
Branch, Attorney-General’s Department ..... 1**

**OBEROI, Ms Sabeena, Assistant Secretary, E-security and APEC Branch, Department of  
Broadband, Communications and the Digital Economy ..... 1**

**ROTHERY, Mr Mike, First Assistant Secretary, National Security Resilience Policy Division,  
Attorney-General’s Department ..... 1**

**SMITH, Ms Catherine, Assistant Secretary, Telecommunications and Surveillance Law Branch,  
Attorney-General’s Department ..... 1**



**Committee met at 12.42 pm**

**CHIDGEY, Ms Sarah, Assistant Secretary, Criminal Law and Law Enforcement Branch, Attorney-General's Department**

**EVANS, Ms Sheridan, Assistant Secretary, Identity Security Branch, Attorney-General's Department**

**HAWKES, Ms Marcella, Acting Assistant Secretary, E-Security Policy and Coordination, National Security Resilience Policy Division, Attorney-General's Department**

**MIHALIC, Ms Susan Ann, Principal Legal Officer, Telecommunications and Surveillance Law Branch, Attorney-General's Department**

**ROTHERY, Mr Mike, First Assistant Secretary, National Security Resilience Policy Division, Attorney-General's Department**

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

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

**CORDINA, Mr Simon, Assistant Secretary, Cyber-Safety and Trade Branch, Department of Broadband, Communications and the Digital Economy**

**OBEROI, Ms Sabeena, Assistant Secretary, E-security and APEC Branch, Department of Broadband, Communications and the Digital Economy**

**CHAIR (Ms Neal)**—Welcome. Would you care to state the function of your branches and divisions and/or any additional responsibilities you may have.

**Mr Rothery**—I chair the Cyber Security Policy and Coordination Committee, which is the senior policy committee in the Australian government for cybersecurity.

**Mr Besgrove**—Amongst other things I am responsible for my department's involvement in the government's cybersecurity strategy, including some of the awareness campaign issues that we have spoken about before.

**Ms Oberoi**—My branch has primary responsibility for cybersecurity issues, in particular awareness raising on cyberspace security.

**Mr Cordina**—In relation to cybersafety, I look after a couple of programs there—the work of the consultative working group on cybersafety, the youth advisory group and also some of the research activities.

**Ms Hawkes**—My branch, as Mr Rothery outlined, provides support to the Cyber Security Policy and Coordination Committee and also has within it the Australian Government Computer Emergency Readiness Team, or GovCERT, and will also house CERT Australia next year.

**Ms Evans**—We do the whole-of-government coordination on responses to identity security, coming out of a COAG agreement in 2007.

**Ms Chidgey**—We have responsibility for the relevant offences in the Criminal Code.

**Ms Smith**—We have responsibility for the lawful access to communications for offences like cybercrime offences.

**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 parliament. Mr Rothery, you have indicated that you are going to give a brief presentation in relation to the cybercrime policy. Please commence with that.

**Mr Rothery**—Thank you, Chair. I would like to brief the committee on the launch of the Cyber Security Strategy that the Attorney-General publicly released on Monday, 23 November.

*A PowerPoint presentation was then given—*

The Cyber Security Strategy is the key outcome from the review that was conducted last year. The review looked at all of the current programs, capacities and policies within the Commonwealth government to see whether it was suitable for the current threat environment. Cybersecurity is a national security priority that was recognised by the Prime Minister's National Security Statement to parliament—both in terms of the threat and also the importance of information and communications technology to the economy and the vulnerabilities that unfortunately exist in that complex technology.

We have sought to achieve an integrated whole-of-government approach building on public awareness of the risks. But the important issue is that it is one where there is a need for a shared responsibility, because user behaviour plays a great deal of influence in terms of people's exposure to risk and the way that people actually protect themselves and follow some reasonably basic steps. Next slide, please.

The aim of the policy is the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy. Next slide, please.

Some guiding principles. National leadership. There is a large role for the Commonwealth to take leadership. The internet is international. Many of the threats come from overseas, many of the services that people are seeking to access over the internet come from overseas, and most of the software and computers that people use are manufactured overseas. There is the concept of a shared responsibility in terms of government creating the right legal and policy frameworks, the behaviour of individuals and also the activities of corporate Australia, who are the custodians of much information that belongs to Australian citizens.

Partnerships. One where no one layer can fully manage the problem. There is a need for collaboration.

Active international engagement—for the reasons I have given before.

Risk management, because it is absolutely impossible to ensure the security of the internet. The internet by its very design does have vulnerabilities in it and it is open to everyone, and it is an environment that is extremely difficult to police.

Protecting Australian values. What we are trying to capture there is people's rights to privacy but also people's right to exploit the internet for purposes of doing business and the purposes of sharing their information, their networks, their friends, and building collaborations of interest. Next slide, please.

There are three objectives: firstly, that Australians themselves are aware of the risks of cybersecurity and that they take those basic steps to protect their identity, privacy and finances online; secondly, that Australian businesses operate secure and resilient information and communications technologies, not only to protect their own corporate activities but also because they are the custodians of information of their customers; and, thirdly, that the Australian government itself ensures that its ICT is secure and resilient.

**Ms RISHWORTH**—Would ISPs fit into Australian business or are they a separate category?

**Mr Rothery**—Yes, ISPs we would see in that category. Our strategic priorities going forward include threat awareness and response—we have to know what the problem is. We have to be able to act on it quickly—we have to see new vulnerabilities and new activities by virus writers and other offenders on the internet. On cultural change, there has to be growth in the awareness of the threat and also in the awareness of what individuals can do to actually protect themselves. Business-government partnership is an area where the primary delivery of services to consumers will have to be through business. It is through business, such as the ISPs, that every individual internet user has a relationship, but it is one where government can play a facilitative role, can bring about greater information sharing and can encourage various market players, including the ISPs, to take a greater responsibility for what happens on their networks.

International engagement, for the reasons we have identified earlier, is clearly an area where the Australian government will be taking a lead. Legal and law enforcement: because of both the international aspect and the particular criminal offences around telecommunications, there is a role for the Australian government to lead in the legal and law enforcement elements. Knowledge, skills and innovation: as the Attorney said on Monday, a small number of tech-savvy people are making life difficult for all internet users. We need to make sure that we have tech-savvy people who are fighting for our interests.

CERT Australia: the Attorney announced on Monday that the Australian government would become responsible for the national CERT function beginning in January 2010. CERT Australia will be the initial point of contact between government and the internet industry. That includes vendors, the ISPs and also the international community. Most developed economies have a national CERT and we need to make sure that we get the greatest leverage but that we also contribute to the overall knowledge bank that is held by like-minded governments on this issue.

We need to be able to coordinate through CERT Australia our response to serious incidents between government and the private sector. It is not just about how the government responds to protecting its own networks but what can we actually do to assist the private sector? It may be that if an attack is coming from overseas the Australian government needs to make representation to another government to get assistance.

Lastly, there are the international issues. Importantly, I would like to dwell on the ISP code of practice. This was announced by ministers at the end of 2008 and is currently being drafted by the Internet Industry Association with government support. It is very important to understand that the ISPs are in a unique position of influence. They are the only party that can identify an individual user to the technical computer address that that user is actually using for that particular transaction. The way that computers appear is by their IP address—their internet protocol address. The only party that can correlate an IP address to a particular user is the ISP. Therefore, when we are looking at ways of identifying computers that may have viruses or behaviour that may either be creating a risk to another internet user or an indicator that that machine itself has been infected, the only party that can put that information together is the ISP if it is small users or the network owner if it is a large corporate. Therefore, getting the ISPs into the picture is essential. The ISPs are the parties that have the commercial relationship with every internet user. The ability of organisations like CERT Australia to be able to deliver a benefit for the majority of internet users will be through a partnership with, and cooperation by, the ISPs.

**Mr BILLSON**—Madam Chair, I apologise. We have an occasion going on.

**CHAIR**—We might have to have a quick resolution to form a subcommittee.

**Mr BILLSON**—I move that.

**CHAIR**—The motion is carried. That means we will not lose our quorum and have to fold.

**Mr Rothery**—To give an indication of some of the things that you will see and that perhaps have not been so clear in the public announcements: we will be looking for an international engagement strategy that we will be sharing with the business community. This will identify what our priorities will be in the different international fora. A huge range of international groups are looking at cybersecurity: the International Telecommunication Union, the UN, the OECD, APEC and a number of IT-specific—

**CHAIR**—So you are saying you are implementing a strategy?

**Mr Rothery**—We will be developing a strategy in consultation with the business community.

**Mr Rothery**—We have a number of things underway already. The idea of the strategy is to try to pull those together into something more cohesive.

**CHAIR**—That is an area that I would very much like to hear more about from you.

**Mr Besgrove**—Sure.

**Mr Rothery**—We have a government crisis management plan that is in revision at the moment. What we are looking for is a plan that we can actually share with the business community and with the ISPs such that we have an understanding of each other's expectations in terms of managing a large cybersecurity incident. The third element is exercise Cyber Storm III, which is being led by the US Department of Homeland Security. Australia will be participating in that in October 2010, and that will be an opportunity for us to test the crisis management plan. It will have heavy private-sector engagement, as did Cyber Storm II, and will be a way for us to validate the plan. Thank you very much.

**CHAIR**—Mr Besgrove, would you like to add anything?

**Mr Besgrove**—I also have some opening slides, which I promise I will do in two minutes. I will start talking about them while they are loading. We have previously briefed the committee about some of the awareness-raising strategies. I wanted simply to remind the committee that the work my department does fits within the broad strategy which was announced by the Attorney-General the other day. A couple of key elements of that strategy from our perspective are, first of all, to educate and empower all Australians with the information, confidence and practical tools to protect themselves online; and, second, to partner with business to promote cybersecurity. That is basically what we have on the first slide. Some of the initiatives which were previously mentioned include the awareness week, the alert service, and the schools module which we have developed for both junior and more senior school age children.

The key thing we wanted to convey is that we have a growing number of stakeholders across the community and the economy, including the vendors of the equipment; the ISPs; all of the major banks; a number of retailers; telecommunications user groups; the recently formed Australian Communications Consumer Action Network, which is an umbrella group of consumer bodies relating to communications in Australia; the Seniors Computer Club; the Australasian Consumer Fraud Taskforce, which is chaired by the ACCC; a number of state and territory governments; and many other groups. So that network of collaboration is growing all the time. My colleague Ms Oberoi can talk about the detail of that.

One of the things which have changed since we last briefed the committee is that we were already starting to try to move away from the single awareness week each year towards more of a rolling program. We are currently discussing with some of the banks, retailers and other groups having some sort of initiative in the lead-up to Christmas. We are talking to Harvey Norman about a back-to-school initiative in late January. There is mention of another of couple of other things there as well. The idea is to try to have more of a rolling program of initiatives. We would still focus the majority of our efforts during each security awareness week, but we want to try to keep reinforcing the message and also to take advantage of the efforts of others.

Just to bring you up to date, we believe there are over 9,000 schools in Australia. To date, 1,400 schools have access to our e-security teaching tool online and we have also had more than 800 sent the CDs. We have a couple of people who are engaging full time on a continuing basis with schools. I hope this time next year to be able to say that we have at least doubled those numbers. That is certainly our intention. The idea is to reach all of the schools in Australia over the next two years.

**CHAIR**—Is that done at no charge?

**Mr Besgrove**—There is no charge.

**CHAIR**—If other community groups want to access that module as well, can they do that?

**Mr Besgrove**—We are not placing any real restrictions on accessing any of our material. Basically, it is for whoever is interested. We have certainly supplied some of the schools' information to a number of delegates from other countries at events we have been at in the last couple of months. Recently a representative from Fiji took half a dozen of the CDs away. It is starting to attract some attention. That is the last slide, so I think I got inside my two minutes.

**CHAIR**—Well done. I am very interested in what initiatives Australia is taking internationally to coordinate a strategy for cybersecurity. Very obviously everyone emphasises cybersecurity is not isolated by national boundaries and many of the risks and attacks come from outside Australia.

**Mr Besgrove**—That is certainly true. There are a number of longstanding things that have been going on. At the last meeting I mentioned both the OECD and the APEC TEL. I am currently the chair of the OECD's working party on information, security and privacy, so we are in a good position to influence the direction of OECD thinking. We have helped to lead a number of initiatives there, including a few years ago when Australia initiated the setting up of an OECD antispy task force. At the time we did that spam was more of a commercial issue than a security issue but, over the last few years, that has changed. We have also done quite a bit of work relating to the development and spread of malicious software. We are also involved in the APEC telecommunications working party—

**CHAIR**—Just before we move on from the OECD task force, what is the objective of that task force? Is there an intention that there be some sort of international agreement that arises from that task force? What is anticipated will come from that?

**Mr Besgrove**—The OECD is more a policy and research body. In a nutshell, what it attempts to do is get the best information available and promulgate it as widely as possible. So it develops best-practice ideas. It often explores new initiatives. It just recently launched a new project looking at the role of internet intermediaries. The code of practice that Mr Rothery talked about is one of the elements that the OECD is likely to pick up as an example of best practice emerging from Australia. It will also be looking at what other countries are doing in terms of how they engage with their ISPs to try to get them to behave more responsibly with consumers. The OECD has no action-making power. What it does have is a strong research capacity and an ability to promulgate ideas and get them listened to by governments in the Western world. That is one vehicle.

The second one is APEC TEL. In a similar fashion, we have done quite a lot of work in that area over a long period of time. Mr Rothery's department and my department are both active at the moment in the International Telecommunication Union. I do not know where we have got to; he might want to comment on that as well. The ITU moved very strongly into the cybersecurity space about three years ago. The advantage of the ITU is that it is a treaty based organisation that includes something like 190 countries around the world. So if you want to engage in a body where most countries show up and you want to try to take some ideas forward, the ITU has the great advantage that all the players are there. That is also the disadvantage as, with all the players

there, it takes a long time to take things forward. One of the advantages of OECD and APEC TEL is that they are smaller and easier in which to move things forward. You can get things done comparatively quickly.

They are the bodies that we are principally focused on. There are a number of other international bodies. As I indicated earlier, the idea behind international strategy is to take some of those current interactions as well as some of the things which the Attorney-General's department and others are involved in and try to bring them together into a more deliberate strategy. Mike, I do not know if you want to comment from your perspective on this.

**Mr Rothery**—I was just consulting with my colleagues about what is happening at the UN. I understand there are a number of proposals there that we are considering at the moment. The International Telecommunication Union has also entered into a partnership with an organisation called IMPACT in Malaysia. I cannot remember the meaning of the acronym—my colleague might be able to help me.

**Ms Hawkes**—International Multilateral Partnership Against Cyber Threats.

**Mr Rothery**—This is going to be a centre that the ITU is supporting. I think it was originally set up with some financial assistance from the Malaysian government. We have recently had some discussions with them and we have also had discussions with the Indonesian government. We have previously done some regional capacity building under the auspices of APEC. There are a number of proposals under consideration, including one to create a Pacific region CERT and what relationship we might be able to have with such a body alongside the CERT that we are building for Australia. It is a very active international arena. One of the reasons for having a strategy is to try and prioritise where our efforts should go. Almost every international body is looking at this issue, with different degrees of intensity.

**Mr Besgrove**—The other comment I would make is that the reason you need to engage with these bodies is because of the multi-jurisdictional nature of the issues we are confronting. There is no single place you can go. There is no obvious single forum in which you can get involved. One other thing I did mean to mention, which may be of interest to the committee, is that Australia and Japan have co-sponsored a joint project looking at developing best practice approaches to the protection of children online. This is a project which we are progressing in both the APEC TEL and the OECD simultaneously. I have to tell you that trying to get two multilateral bodies to work on the same thing at the same time is not always straightforward. We have enjoyed very strong support from the Japanese government. In fact, the idea originally came from the Japanese and we were very happy to support it. We would expect to see outcomes from that next year.

**CHAIR**—My concern is that, even though on an international level the development of strategies and policies is helpful, the source of much of the malware is from countries where the rule of law is not particularly strong and control of businesses such as ISPs is quite poor.

**Mr Besgrove**—Yes.

**CHAIR**—Bearing that in mind, I am a little concerned that those places that actually need the most control or the most assistance are the ones least likely to implement those strategies and

policies. It would be desirable to have some sort of mechanism in place to make it more compulsory to control that sort of activity. The most common sources of a lot of this malware, although they may have moved on, are some of the former Eastern bloc countries.

**Mr Besgrove**—That is correct in many cases. If I could touch briefly on the approach that my portfolio and its predecessors took to spam, which was more of a commercial problem when we were addressing it, we were confronted, in essence, with the same situation. We did a range of things. First of all, we made sure that there was appropriate legislation and enforcement in Australia; secondly, that there was appropriate awareness raising in Australia and overseas; and thirdly, that we pursued international engagements and, in particular, where we could we encouraged countries to implement legislation. Australia actually used some of its development funding to help some countries in this region to develop their own anti-spam legislation, for example.

That is one approach where you are actually trying to address the four or five different elements of the problems simultaneously and accepting that one of the things you are going to have to do is encourage other jurisdictions to think about their own legal basis. I know that AGD has been quite active in the development of model laws in the past, for example. They are frequently used globally to try and raise the basis of the regulatory regimes across the planet on particular issues.

**CHAIR**—Do you want to add anything to that?

**Mr Rothery**—One of the techniques that are used to identify suspicious behaviour is, for example, when you normally do your internet banking from either your home or office and all of a sudden your bank account is being accessed by a computer in eastern Europe. That is quite often a trigger for the bank to launch an investigation, and that is when an individual might get a phone call from their bank saying, ‘Is this really you?’

One of the things that lead to is that the criminal syndicates then seek to actually relay their attacks through third countries. Whilst it may be very difficult to really clamp down on the sources of the organised crime syndicates through international agreement setting, we can actually make it much more difficult for them. We can make it more difficult for them to use innocent third parties in other countries as a way of either controlling their networks or relaying their spam, which quite often deliver the viruses and so forth. If you can get the like minded governments to agree, you actually make it much more difficult for them and you make it easier for us to put technical barriers and security devices in place because you can see where the suspicious patterns are.

That is only an interim measure; in the long-term, obviously, we would prefer to see a uniform approach internationally to deal with cybercrime. But there are things that we can achieve just by getting the like minded nations to collaborate.

**Mr Besgrove**—I would certainly reinforce that. One of the other things that we have used quite a lot is just informal collaborations between enforcement agencies—these can often be remarkably effective.

**Ms RISHWORTH**—I have a couple of questions about the code of conduct for the ISPs. Firstly, I notice that it is a voluntary code of conduct—is there any particular reason why it would not be a mandatory code of conduct? Is it because you are trying to get them on side and do not want to use a stick, or is there a particular reason why it is not mandatory? How far away are a lot of the ISPs out there from actually behaving in line with this code of conduct?

**Mr Besgrove**—The original motivation for moving to the code was because we had for some three or four years operated through an Australian Communications and Media Authority program called the Australian Internet Security Initiative, AISI, that seeks to identify compromised computers in Australia. We have enjoyed very high levels of collaboration. We have about 53 ISPs involved—do you remember how many?

**Ms Oberoi**—I think it is close to 70.

**Mr Besgrove**—It is close to 70 now, and they are the largest ones. They cover well over 90 per cent of the market. There are something like 400 ISPs in Australia, but many of them are very small. We have already got very active engagement in this particular initiative—that is all voluntary and we have had that engagement for quite some time.

What we do not have is consistency of practice. When a customer is identified, the ISPs do different things. We know that some of them work much more effectively than others, so our motivation was to say, ‘Can we find a way to, first of all, make them aware of what we regard as best practice and then, secondly, get them to sign on to that?’ We went down the voluntary route because we already had high levels of collaboration and we were confident that we could get the industry on side. The industry and the association were more than happy to come on board and help us with this.

Our approach is: if you can do something through a voluntary code that is much faster than trying to do it through a regulatory process, particularly if the industry and others start to try and resist it. We have always said that if this does not work then government will have to consider firmer options because this is really serious stuff. This is damn dangerous and we have got to do something about it. But so far we have had very high levels of collaboration from the industry. We believe we are only a couple of weeks away from being able to launch this particular initiative with a date of effect during next year. We have also always said that our intention is to review it after a year. If we believe it is working, fantastic. If not, we will try and improve it and if it has not worked then we will look to other alternatives. We are not going to leave this alone: we cannot.

**Ms RISHWORTH**—I see it as quite a serious point because, while we have heard a lot of evidence about the end user being the most important to sign up, there is not a driving lesson, as we have heard before, when you buy a computer. People are not always sure. The ISPs are very important to get on side. What do you see this code will be? I do not know whether you can tell us. What is the best practice if an ISP identifies a computer as being compromised?

**Mr Besgrove**—Best practice as far as we are concerned is that they identify the customer, that they basically closet them—I am not sure what the term is—reduce their access, engage with the client and provide them with support and advice as to where to go and what to do in order to remove the compromise and then reinstate the privileges that they would normally have. So,

basically, clean up the machine so that it is able to operate effectively in future and make sure that the customer is aware, first of all, that it is compromised, second, knows where to go for help and third is more vigilant in future.

We are concerned that there are many thousands of compromised machines out there in the Australian community and, in many cases, people will be completely unaware of it. All that will happen is that they will curse their ISP because the computer has slowed down. That will be all that they will notice. They will not notice much else because in many cases the compromised machine is being used as part of botnets to do other things—launch spam attacks, denial of service, phishing attacks and a whole range of things—and the individual may not actually be the target at all. They may just be a ship of convenience, if you like—one of many tens of thousands.

**Mr Rothery**—There is some healthy self-interest for the ISPs. When people's machines run slow and they blame the ISP, they ring the ISP. That costs the ISPs money. Also there is the possibility—and I think it is a healthy one—that there could be new markets for ISPs in selling value-add services to help people clean up the machines or in getting a commission from the sale of antivirus products that they recommend. At the point of bundling when they are selling the connection, the modem and the software, they could check that the customer has adequate antivirus products and suggest an additional product at that stage. We think that there is a value proposition here for the ISPs to take a much more active role that should be revenue neutral for them.

**Ms RISHWORTH**—Do you think this is something we can make marketable to the ISPs? Do you think a certified voluntary code of conduct for consumers is an option or an opportunity?

**Mr Besgrove**—I believe so. The strong message we are getting back is that they do see this as very clearly in their interests. Our focus today is on cybersecurity. My department has a very strong focus on consumer service generally and we see this as an integral part of trying to get the telco and ISP sectors to lift their game more generally. That is a very strong message that my minister has been putting forward repeatedly.

**Ms COLLINS**—I wanted to pick up on what you said about protections being available at the bundling point. We have heard before that perhaps they should be available at the purchase point. I would appreciate some views on whether you think security should be sold at the purchase point or at the bundling point and whether or not that could be included in a code of practice or some other form of regulatory manner, voluntary or non-voluntary, so that people actually have the correct security and protection on their PCs.

**Mr Besgrove**—We have not thought too much about regulating at the purchase point. Ms Oberoi can talk about the discussions and the engagement we have with both Dick Smith and Harvey Norman, we certainly have their active support in the awareness-raising activities. What we are looking to do is trying to make sure that people are basically given the material when they buy the box.

**Ms Oberoi**—We have had strong support from Harvey Norman and Dick Smith but what we are also trying to do is engage with them for the pre-Christmas festive season and also back to school. Harvey Norman has showed a very strong interest in partnering with us in back to school

promotions because one of the things they find when people buy the machine—and they have not given us a proportion of how many people do buy antivirus products—is that there is a large proportion of people who spend a significant amount of money on a really high-tech laptop or PC but do not spend the extra \$60 or \$100 to buy the protection they require. So, certainly, they are quite keen and we are engaging with them and also with a lot of online businesses such as eBay that recognise that this is an important issue.

**Ms COLLINS**—From what I am hearing, the preference is to provide the security at purchase point rather than at bundling point when they connect to an ISP.

**Mr Besgrove**—Certainly our view has been to try and provide awareness of the need for security, but, with the work we are doing with other parts of the chain, certainly we are definitely doing as much as we can to increase the ISPs' and the telcos' awareness that they have a good corporate citizen role here. As I indicated earlier, we are sufficiently concerned about the level of compromise that we do not think this is something that government can leave alone. I think we are going to have to continue our efforts in this area, and the minister has certainly indicated a predisposition to do so.

**CHAIR**—Certainly it is a lot bigger issue now than buyer beware. Previously, if you did not look after your computer, your computer was compromised—that was a problem for you. Maybe you did not get the right service. Obviously the situation now is that it is like a nuisance. If you allow your computer to have no protection, not only is it a problem for you but it is a problem for all your computer neighbours, who may become subject to a cyber-attack because you have not taken the initiative. I am interested in your view on whether there is a higher responsibility for the computer owners. Are they answerable to other people if they do not take steps to ensure their computer is protected, if it is a potential liability for the people who are attacked from their computer?

**Mr Besgrove**—As one of the few non-lawyers in the room, I have no idea what the answer to that question is!

**Ms Chidgey**—The answer is no. The liability rests with the individual with the malicious intent—the one who is using the computers as botnets—rather than the individual. The individuals have no awareness that their computer is being misused.

**CHAIR**—A civil case of nuisance? If you have a piece of land and you allow water to run over your land and go onto your neighbours land, there is a liability.

**Ms Chidgey**—I am afraid my specialty extends to criminal law!

**Mr Rothery**—If I could follow up on that very briefly, I understand that the draft code of practice is encouraging ISPs to have a conversation with the customer at the time of connection to the internet and also in the follow-up stage if there is a compromised machine identified. A compromised machine may actually have antivirus software on it but may not have been kept up to date by the customer. The customer may have bought the machine with antivirus software but then declined to pay for the ongoing subscription fee. The code of practice would pick that up because, at the point that the machine was compromised, it is suggesting that the machine would

have its access to the internet limited until such time as it had been cleaned up to the satisfaction of the ISP.

**Ms RISHWORTH**—Are there incidents where the viruses are ahead of the available antivirus software? What happens there? Do you limit the internet until such technology or program is available to clean up the computer?

**Mr Rothery**—Every time that an antivirus product is updated, it is updated because at some time in the previous weeks or months a new virus or piece of malware was identified. There is always a time lag. To the extent to which an individual computer would be identified as being compromised, it would be at approximately the same time that the antivirus products would be updated. Any difference there would be hours or days. So there is very little risk, I think, that a person who is doing the right thing would find themselves in that position, but what I have to be clear on is that there are pieces of malware out there that are not being picked up. There is a gap. The very, very sophisticated pieces, if they are kept in low numbers, are not picked up.

In fact the work that [www.GovCERT.au](http://www.GovCERT.au) has been doing in the Attorney-General's Department has been working in that space—that is, to help business identify those attacks on their systems that will not be picked up by the commercial antivirus products. Because of the activity of the law enforcement and intelligence community, we may be able to give a business additional information on top of what they can get from commercial services, but because we are protecting the intelligence source of that material, we do not publicly release it. We release it to those corporates that we have done a risk assessment on for the national interest and that we believe that we can trust, and we give them that information in advance of it going to the commercial antivirus vendors. It has been a function that my department has been performing for more than three years.

**Ms RISHWORTH**—And who then constructs the technology to clean up that system if the commercial antivirus—do they do it themselves?

**Mr Rothery**—Yes, we do not provide the companies with the clean up tools. We tell them what to look for, particularly the traffic patterns exiting their systems so that they can block any attempt of either a control or data exiting their system. Some 480 Australian companies are registered with us and we provide them with regular updates. The information that we provide them is a pool of information that we get from cooperating governments overseas as well as our own agencies here in Australia.

**CHAIR**—I want to go back to that issue of civil liability. I do not know which of you is best placed to get a response on that.

**Mr Besgrove**—Definitely not me.

**CHAIR**—It is something that could be taken on notice. Does anyone want to volunteer for it? It is certainly something that may become an issue in the future.

**Mr Besgrove**—I have two other quick things I wanted to mention in respect of the code and the related Australian Internet Security Initiative. We know of a number of other countries who have similar things to the Internet Security Initiative. Probably the most advanced are the

Koreans and the Japanese, but we know some Scandinavian countries, including the Fins, also have not dissimilar things. It is our understanding that when the Japanese identify a compromised machine, there is a degree of compulsion in the relationship between the ISP and the customer. I just make the observation that Japan is a very different country.

**CHAIR**—Yes, there is a cultural aspect to this.

**Mr Besgrove**—It is much easier to tell people that they should do something. I might be wrong, but it does seem to us that the ISP compelling a customer could lead to other concerns in Australia.

**Ms RISHWORTH**—So you are saying it is easier to cordon off the computer?

**Mr Besgrove**—We are just trying to work with the culture here.

**CHAIR**—One thing that has become apparent throughout this inquiry is that there is a bit of a gap in low-level collection of information reporting and investigation. For high-level cybercrime in banks, when there are mass incidents, there is an avenue for investigation and prosecution in most cases, either with the state police or the Federal Police. But for those many small level cybercrimes, where it may be less than \$1,000, there really does not seem to be an avenue for people to pursue those. In a lot of cases we do not really collect the information. If someone goes up to their local police station and says, ‘I’ve lost \$200 because I followed this link,’ or whatever, in most of the cases the police are not going to do anything so they do not collect anything. It has been argued to the committee that the creation of a general portal for the purposes of collecting information and reporting, and then referral to other areas if it is considered appropriate, would be quite beneficial. I understand it has been done in other jurisdictions. Is it something that consideration has been given to?

**Mr Besgrove**—There are a couple of observations I would make there. There is already in existence the Telecommunications Industry Ombudsman. And, while the TIO’s purview does not extend as far as some of the issues that this committee is looking at, invariably some of the complaints they get relate to ISPs. I am also aware that offices—

**CHAIR**—But they do not deal with crime?

**Mr Besgrove**—No, they are not crime. I am also aware that state offices of fair trading deal with quite a few reports of this nature. I am aware of that through the Australasian Consumer Fraud Taskforce, which I am a member of and which the ACCC chairs. I guess my first response would be: you don’t think that state offices of fair trading are an appropriate place?

**CHAIR**—Have you dealt with them?

**Mr Besgrove**—Only in committee meetings, not directly.

**Ms COLLINS**—I think what we are trying to say is that most end users, when something happens to them, do not know where to go and report. I think that is where the chair is coming from.

**Mr Besgrove**—Yes.

**Mr Rothery**—One of the recommendations of the review from 2008 was to ask the Australian Federal Police to broker a clearer understanding with state law enforcement about which matters should be referred to which jurisdiction. In other words, if you are a victim in New South Wales of what you think is a vendor in Western Australia, in which jurisdiction do you report that and at which point should something be reported to the AFP versus state law enforcement? An important element of that, particularly in terms of being responsible for what will be CERT Australia in January, is the issue of what matters should be dealt with as criminal matters versus what matters should be dealt with as security incidents. Every case of a virus or malware is, in some way, possibly a crime under the cybercrime provisions of the Criminal Code.

We acknowledge that there is a lack of clarity there and we have asked law enforcement to help us clear that up, partly so that we can give a much clearer message to people as to where they should go. So we acknowledge that there are some areas there. The difficulty is that that conversation is about computer crime offences: the unauthorised access or impairment of computers. When you then start talking about things such as, ‘I have ordered something on eBay and it didn’t turn up,’ or, ‘I have had someone take my intellectual property,’ and all of the other types of crimes that can be facilitated or committed on the internet, the degree of complexity then rapidly escalates because then you have consumer protection issues or fraud issues; you might have defamation and intellectual property theft. I think it would be fair to say that it can be very difficult for the individual to know which jurisdiction and area of law deals with an incident. All I can say is that at the moment we have endeavoured to pursue, through the strategy, greater clarity around computer crime offences. That is one of the goals of the strategy.

**CHAIR**—That might be useful for those who are making inquiries and are prosecuting, but for consumers it still does not necessarily assist them. Do you think there is any benefit to having a general or central portal which takes the complaints and then directs them to the appropriate place?

**Mr Rothery**—My only hesitation with regard to the portal would be that we would be injecting something into the evidentiary chain. In the conversations we have had with law enforcement they are quite reluctant to have a crime reported to anyone other than the police in the first instance. An alternative could be an information resource that could effectively redirect someone to report to the appropriate agency. In other words, rather than actually take the information or evidence about the action and then redirect that inquiry to the most appropriate agency—

**CHAIR**—But that happens now. I have to say that I think it is really a complete furphy if that is considered a problem, because there are cops reporting now when civilians ring up and commit things they think are crimes. If it is considered to be a crime, it is referred on to the police and the police then contact you.

**Mr Rothery**—I can only pass on the view that has been expressed to me—that is, there can be difficulties in the evidentiary chain if additional layers are involved.

**CHAIR**—But you do not actually take evidence. It is not a suggestion that you actually give evidence through it. It is just a matter of saying, ‘These events have happened,’ and then saying,

'If this has happened then you should go to either the police, ACCAN, the Ombudsman or whatever.' I was not proposing that it actually be part of the evidence gathering. I do not think you could possibly do that—

**Mr Rothery**—All I can say is that it has not been looked at as part of this strategy because we have been looking at really only the computer crime offences. We have acknowledged that there is a weakness there and we are working with law enforcement to be clearer.

**CHAIR**—So you are saying there has been no assessment by any part of government as to whether a general portal would be helpful?

**Mr Rothery**—That is correct. There has been no assessment.

**Mr Besgrove**—Not at this stage. It has been raised by some people with us in the past.

**CHAIR**—What sort of people?

**Mr Besgrove**—ACCAN, but ACCAN has been with us only for a short period of time. It is one of the issues they have raised. A few people in the past have suggested that the role of the TIO might be broadened.

**CHAIR**—We might have some further questions. If we were to forward those questions to you, could we receive your response in writing?

**Mr Besgrove**—Yes.

**CHAIR**—We may want to cover off any areas that we did not cover today. Could we also please receive copies of both your PowerPoint presentations?

**Mr Besgrove**—Yes.

**CHAIR**—Thank you very much for attending. I am sorry we did not have as many people here as we might ordinarily. It was certainly useful for us. Hopefully, with a little more interaction between us, we can cover off any issues that are still outstanding. Thank you for your attendance.

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

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

**Subcommittee adjourned at 1.37 pm**