



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

**HOUSE OF
REPRESENTATIVES**

STANDING COMMITTEE ON COMMUNICATIONS

Reference: Cybercrime

WEDNESDAY, 18 NOVEMBER 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://parlinfo.aph.gov.au>

HOUSE OF REPRESENTATIVES
STANDING COMMITTEE ON COMMUNICATIONS

Wednesday, 18 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, Mrs Hull, 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

**GREGSON, Mr Scott, Group General Manager, Enforcement Operations, Australian
Competition and Consumer Commission 1**

**RIDGWAY, Mr Nigel, Group General Manager, Compliance, Research, Outreach and Product
Safety, Australian Competition and Consumer Commission..... 1**

Committee met at 12.38 pm**GREGSON, Mr Scott, Group General Manager, Enforcement Operations, Australian Competition and Consumer Commission****RIDGWAY, Mr Nigel, Group General Manager, Compliance, Research, Outreach and Product Safety, Australian Competition and Consumer Commission**

CHAIR (Ms Neal)—I declare this public hearing of the House of Representatives Standing Committee on Communications into cybercrime open. We are taking evidence from the Australian Competition and Consumer Commission. Thank you for coming to give evidence today. 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 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. Would either or both of you like to make an opening statement before we ask questions?

Mr Gregson—Thank you, Chair. I will make a short statement and hopefully not cover too much of the submissions we have made to the committee. First of all we would like to thank the committee members for the opportunity to attend today. As a general comment, we would note that cybercrime is obviously a broad descriptor that can cover a broad range of conduct. The ACCC's interaction with cybercrime is primarily related to our very broad role in relation to prohibiting misleading and deceptive conduct or false representations under the Trade Practices Act. That covers most activities in Australia relating to trade or commerce.

The increased internet trade has brought the ACCC into regular contact with online conduct that might be considered to be a subset of cybercrime. Primarily we are talking about online or internet facilitated scams. That is a key area of contact with what you might describe as a subset of cybercrime. Many of these originated overseas.

The type of scams that we are familiar with and see quite often include advance fee frauds or money transfer scams, where you lure upfront payments with the promise of a bigger return down the track. These include things such as inheritance scams or the exiled leaders having a pot of money to share with those outside the country. We also look at a number of phishing scams, where approaches through the internet seek personal information for subsequent use in drawing money down from accounts. It is often passing off as either the consumer's bank or a business that they have an ongoing dealing with. We see quite a few of those. There are lottery and sweepstakes scams—again upfront payments with the promise of returns through a promised prizes. There are false ticketing product scams, an increasing number of dating scams and also a number of online scams directed specifically at business—very often small business, but not in isolation.

We have noted—and I am sure a few other witnesses have commented on—the ABS report of a couple of years ago, which was very helpful in identifying the extent of scams in Australia. It is not just internet or cyber based on scams, but a large proportion of it is. They found that one in 20 Australians were touched by scams, leading to about \$1 billion worth of loss over the course of the year.

In regard to the ACCC's experience over the period 2008-09, we received about 18,000 scam related complaints. That is out of about 77,000 complaints we receive more generally. So roughly about one-quarter of our complaints relate to scam related conduct. Of that 18,000, about 12,000 appear to be related to online scams. I say 'appear' in that it is not always possible for databases to determine which exactly is online and which may be using more traditional methods such as mail or indirect contact.

CHAIR—So your databases do not distinguish, is that what you are saying?

Mr Gregson—It can do, and that is where we have tried to draw that. It is not a perfect delineation. As with many databases, it is hard to drag that information out at times. Our activities in scams is focused in three broad areas. They are separate but they are also very much interlinked. First, there is our education and outreach. We believe this is a key. We do a number of activities in this area. One I am sure you are familiar with is our SCAMwatch website. We got about 100,000 visits in the last quarter alone. We have about 10,000 subscribers to that website. In 2009 to date we have had about 32 alerts in relation to scams. We have a broad range of publications—we would be happy to leave copies of those—directed both that consumers but also at businesses. We engage in a wide range of outreach activities, whether they be presentations, media releases or media appearances to try to educate consumers and make them aware. One of the key issues we really want to make consumers aware of is just to be sceptical about approaches you get proactively in the marketplace, but particularly the online marketplace, so that you have got that scepticism in your mind when you are looking at approaches. We also engage in a number of activities such as the Consumer Fraud Fortnight. We do that through a forum, which Mr Ridgway can talk to you about. We are also involved in a number of international activities, such as the ICPEN—the International Consumer Protection and Enforcement Network—internet sweep days.

The second key area we focus on is disruption activity. This is emerging as a very important technique for dealing with scams. We try to look at ways to interfere with the delivery of money from scams, the platforms they use, whether they be online or otherwise, and other delivery methods of communications, whether it be mail or other traditional means of communication.

We obviously follow both those activities up with targeted enforcement actions. We look to address matters where there can be effective remedies across a broad range of consumers and we use that to reinforce education, deterrence and disruption activities. All three of those key areas tie in and feed off each other.

Importantly, and I think it is reflected in some of the evidence the committee has heard to date, those three activities have to be held in an environment of close liaison, coordination and cooperation with both domestic partners—regulators, agencies—and international partners. We have seen ourselves engage in that to a large extent and we are always seeking to find better ways to engage with our colleagues around the country and internationally.

We can provide you with information about some of the areas that we have been involved in. I have already mentioned the ICPEN, the International Consumer Protection and Enforcement Network. That is an international mass marketing fraud working group that involves state police agencies, the ACCC and various international consumer protection agencies. The Australian Consumer Fraud Taskforce is one that we would probably highlight. It is one that the ACCC has

a lead role in and we see domestically as delivering many of the coordination outcomes we need. That involves national regulators, the offices of fair trading, state police and a number of other agencies as well.

We also deal with our state counterparts, whether they be fair trading agencies or ASIC—sorry, ASIC is obviously the Commonwealth—through forums such as FTOAC, SCOCA and MCCA, being the three levels of coordination there. We can provide you with more information about how we actually deal with agencies, and we are happy to take questions on that.

I might just give you an idea about some of the activities we are undertaking to try and refine our work in relation to scams and, in particular, online scams to improve our ability to deal with this important issue. We are trying to find ways to better predict the scam of the day. To give you an example, we saw around the time of the Beijing Olympics some Olympic ticketing scams that came out. Learning from that experience, we are looking at events that are coming up almost monthly to see whether they could generate the same type of activity. Just last week we issued some warnings in the ICPEN context in relation to the World Cup soccer ticketing that is going to come out and put warnings out so that consumers can be alive to any scams come out in that area.

We know we need to entrench our liaison cooperation networks, and we do that by participating heavily in those forums I referred to. We also need to be working on refining our intelligence based identification of scams, looking at data that comes in, not just complaint data but other data that is available to the ACCC and other regulators, and enhancing our disruption techniques, including with both public partners—being other agencies—and, importantly, private partners, whether that be banks or providers of online services that may be used to deliver scams or online cybercrime. We need to have better relationships, and we are currently working on that to make sure that we can disrupt scam activity.

With that general overview, we would be most happy to answer any questions. Just to give you an idea of the split between Mr Ridgway and myself: I am involved in and oversight our enforcement activity in the area, while Mr Ridgway is responsible for a lot of the outreach activity, whether it be SCAMwatch or our participation in forums.

CHAIR—You receive approximately 12,000 complaints about cyberscams a year. Of those, how many do you conclude are potentially criminal matters, and what do you do when you determine they are likely to be criminal matters? Secondly, how many of those have you determined are breaches of the Trade Practices Act, and what action do you take when you make that determination, if any?

Mr Ridgway—I might hazard part of a response. It might be a joint response. A large number of the complaints we receive about scams are multiple complaints about one particular scam at a time. Because of the mass production nature of online scams, a whole range of people will become alerted to or be suspicious about a particular scam at the same time and it will come back to us. In terms of a percentage, we would look at the percentage of the actual scams rather than the pure volume of scams. Both ways, the percentage is relatively low.

We have recently done some joint work with the Queensland police force, for example, in relation to what we call sports arbitrage or horse betting scams, where there was a clear view by

that agency that the fraudulent nature of the scam was well and truly within their jurisdiction as well as there being some misleading or deceptive aspects, of course—so there was an overlap of that. But in each police force's jurisdiction it is really a question of whether they believe something that we would see clearly as misleading or deceptive would fall within what they would consider to be online fraud. We look at those case by case. Practically, when we receive a concern that we think may be something that police forces would have an interest in we use our network of contacts to flag the issue and to share that information and we invite them to consider whether it is something that is already under consideration or whether it is something that they might like to consider nonetheless even though they may not be aware of it.

CHAIR—Over the last 12 months, for example, how many complaints, have you assessed might be criminal and then referred to enforcement? Or is that something that is completely separate? Secondly, for how many have you formed the view that they might breach the Trade Practices Act? What have you done with those types of issues?

Mr Gregson—I will try to address those questions and you may have follow-up questions if I have not quite covered what you require. The Trade Practices Act has parallel civil prohibitions on misleading and deceptive conduct and in relation to false and misleading representations parallel criminal provisions.

CHAIR—Sorry, what I really meant was—

Mr Gregson—Illegal?

CHAIR—criminal activities such as breach of the Spam Act or the Cybercrime Act. When I said 'breach of the Trade Practices Act' I meant both criminal and civil under that act, but I suppose I put them in two categories.

Mr Gregson—Our focus is very much on the provisions of the Trade Practices Act. That is our mandate and jurisdiction.

CHAIR—Do you actually say, 'We think this might be criminal' and refer it to someone? Do you ever do that?

Mr Gregson—Yes, we will often identify matters that are best pursued by other agencies such as the police force. In certain areas it might be the Communications Media Authority if the matter is spam related. There are a number of partners and we would work out who is best placed to deal with it.

CHAIR—Roughly how many would you refer a year? Is it two or is it 300? I have no idea.

Mr Gregson—We might have to take that on notice for specific numbers. But the types of referrals we might undertake are very specific ones, where we find a matter or a group of complaints that we think are best handled by another agency and formally refer. Other matters we might discuss in those liaison forums, and that can add to the intelligence that each agency has in determining their profiles. So we refer information not necessarily with the expectation of enforcement action.

CHAIR—So you just say, ‘Is this scam going around?’ You are not proposing that they take any specific action about it.

Mr Gregson—That is right. But those referrals sometimes lead to action, particularly where it might supplement the information that those agencies already have on their books. It is hard to provide delineation between matters that might raise concerns under the Trade Practices Act and other provisions such as the Criminal Code or fraudulent conduct, and that is because almost by definition scam behaviour involves misleading and deceptive behaviour.

CHAIR—There may be overlaps.

Mr Gregson—Yes.

CHAIR—I do not mind that. I am just trying to get some idea of how many you deal with under the legislation.

Mr Gregson—We can endeavour to draw out from those statistics the numbers of matters that we either draw to the attention of other agencies or formally refer for action and we can try to put a bit more weight around the numbers of matters that we investigate directly and then ultimately pursue in the court. I have to say that, while we have a pretty good track record in the scam actions in court, they are not very large numbers.

CHAIR—Yes, that was what I was going to ask. How many cases has the ACCC taken up in relation to cybercrime either as a civil breach of the act or a criminal breach?

Mr Gregson—We have actually concluded two matters in 2009 involving what we believe is online scam behaviour.

CHAIR—Civil or criminal?

Mr Gregson—We pursued both of those civilly. We always assess matters case by case as to which forum is best in which to proceed. Sometimes a civil forum can deliver remedies such as quick injunctions, facilitating refunds that we might seek for consumers and, ultimately, the objective of shutting down websites.

CHAIR—So those are the only two this year?

Mr Gregson—They are the two that have been current this year. There have been other cases that have involved elements of internet or online behaviour but they are the two that I would describe as cybercrime or cyberscam type activity.

CHAIR—Why was it that you decided to take action in those two particular cases when obviously there were 11,998 cases where you did not? What was different about them?

Mr Gregson—Like any agency, we endeavour to focus our resources on the matters that will deliver the maximum benefit to consumers more generally. We are often informed by the number of complaints we receive when identifying peaks. We are also often informed by contacts with other agencies that tell us about activity in their jurisdictions. I should say that both those matters

involved referrals from overseas: one from the Fair Trade Commission in the US and the other from Washington state Attorney Generals. Their assistance in providing information about conduct based in Australia affecting consumers more generally was also influential in our decision to pursue matters.

CHAIR—So you are saying it was a scam that originated in Australia and that, as well as affecting Australian consumers, it affected American consumers. Is that essentially what you are saying?

Mr Gregson—Certainly, for one of them there was clear activity within Australia. The other one had a combination of activity in Australia, China and elsewhere. We can provide you details of those two matters.

CHAIR—That would be very interesting.

Mr Gregson—We also obviously have regard to whether participants are within our jurisdiction, either the application of the act's jurisdiction or the ability to enforce remedies we might receive in Australia. We generally should have regard to whether court action we take is actually going to deliver something in terms of fixing the conduct, so we have regard to those issues as well.

Mrs HULL—Basically, IT vendors put product onto the market that may not be secure and that exposes consumers to a variety of infections or malware. Is there an obligation under the Trade Practices Act for IT vendors to ensure their products are safe for consumer use?

Mr Gregson—There are a number of broad provisions within the Trade Practices Act that may be relevant. I have already touched on misleading or deceptive behaviour. You could foresee arguments that if blind disregard to the risks were not taken up that you may—

Mr BILLSON—So that is like a reference characteristic?

Mr Gregson—You could consider those types of things.

CHAIR—I am sorry, we have to go to a division. We will be back as soon as we can.

Proceedings suspended from 12.58 pm to 1.11 pm

Mrs HULL—The question was: is it an obligation under the Trade Practices Act that IT vendors have to ensure their products are safe for consumers' use, because they are putting them on the market and then we find that they expose users to viruses, malware and whatever? That was my question.

Mr Gregson—Let me start again. It is case by case, for every scenario. The Trade Practices Act has quite broad prohibitions—misleading and deceptive conduct, or false representations. If there are misrepresentations about the safety of a product where it is unsafe, we can deal with those.

Mrs HULL—When you say ‘misrepresentations’, is there an obligation for them to prove or to make a statement that their product is safe?

Mr Gregson—There is no per se obligation. In certain circumstances, you could consider whether the risks were so overwhelming in a way that there might be such an obligation not to mislead by silence. That would be very circumstantial. You need to look at the specifics of the matter. But they are the types of things that we might look at. If we are talking about products themselves, there are also warranty and refund type issues as well, but I do not think that is quite where you are getting to.

Mrs HULL—No.

Mr Gregson—It will always be circumstantial, and the fundamental question will be whether absence of referral to that is potentially misleading and deceptive.

Mrs HULL—So it is a kind of consumer or buyer beware type of thing?

Mr Gregson—There are protections there, but we just need to look at all the facts and circumstances to determine whether the absence of reference to the risks would be misleading and deceptive. We are very keen to look at new ways of dealing with online scams or fraudulent behaviour that might be within our jurisdiction, and they are the types of things that we will be turning our minds to: whether there are obligations on others to ensure that they are not facilitating those practices.

Mr Ridgway—I might also note that in this area particularly the speed with which new forms of attack, new forms of virus and so forth, are developed has really been responded to in part by the growth of the antivirus sort of IT offerings. While something might be, on the face of it, appropriately designed at the time it is sold, it might be that, without too much passing of time, new viral software is developed that is targeted at what was not an apparent vulnerability at the time. I guess that is the issue.

Mrs HULL—So long as it actually covers what it says it was going to cover.

Mr Ridgway—Yes.

Mrs HULL—If they do say they are going to cover something—say an antivirus software is going to prevent you from getting this, this and this—as far as you are concerned, under the Trade Practices Act, it really has to do that or there is an issue that could be prosecuted?

Mr Gregson—Certainly if they are misleading as to the characteristics of the product, the ability of the product to protect people from those issues, they would be issues that we could look at under the ‘misleading and deceptive’ provisions.

Mrs HULL—Has anyone ever asked you to do that?

Mr Gregson—I am not familiar with matters that we have investigated down that path, but we receive, as we pointed out, 77,000 complaints and we would look into matters if there was a concern that producers of those products were misleading consumers.

Mrs HULL—Do you think that there is enough combined information easily accessible for consumers to give them direction or to enable them to protect themselves well enough? Secondly, should consumers bear more responsibility for ensuring that they do more to protect themselves and that they are aware of what is available? How do we educate the consumer? I just held a consumer workshop, or forum, last week. I only had a venue for 250 people, and it was booked out in a couple of days. They were all seeking that sort of information. There is obviously, in my view, something wrong there. Could you comment on that?

Mr Gregson—We do have a large amount of information that not only the ACCC but other regulators in the field provide. We endeavour to provide portals for consumers to get that rather than having to go to every site, so there are links available to provide that information. I have already mentioned our broad outreach activity. In terms of the question of about whether there is enough available for consumers, the fact that consumers continue to be subject to scam activity suggests that there is always a task of making information more available, finding new ways to hit home to new consumers who may not have been exposed to the messages. So that is a constant challenge that regulators like the ACCC have, of making sure their communication efforts are the most effective. We do this on a weekly basis. As I mentioned, we have given 32 alerts just in 2009 about emerging issues. Those alerts will provide, we believe, helpful tips about how you can avoid scam behaviour or what to do if you have been approached by scammers on the internet.

Mrs HULL—Should there be an obligation on a retailer, when people purchase a laptop, desktop, mobile phone—anything that can carry a scam—to provide a source of information that enables people to understand that there are problems associated with this? Should there be something like that?

Mr Gregson—That is certainly consistent with my previous comment that, the more creative and direct ways we can get information to consumers, the better. Whether you have mandated regimes like that is probably not something ACCC can have a view on. It is ultimately a matter for policymakers. The general principle is that, the more ways information can be provided to consumers at the time they are actually focusing their mind on these issues—such as at the purchase of a computer product or when they are doing their banking or when they are exchanging money—the better able consumers are. We have seen some creative approaches from private industry, without their being mandated to do so, where information is provided to consumers where they have identified risks associated with activities that consumers are coming in for.

Ms MARINO—Thank you for being here today. I have a question about the social networking sites and the increased targeting of those by marketing companies. The potential of fraudulent activity, of course, goes with that. From the ACCC's perspective, how would you see yourselves engaging or not engaging with that, and what else needs to be applied through the act or otherwise to be able to manage that particular forum?

Mr Ridgway—I will make a comment. The ACCC is already engaged and working with a number of the leading social-networking sites as well as with some of the large commercial portals for electronic commerce, both for us to identify and alert those responsible for those sites and portals to scams and potential scam activity so that they can put protections and stops in place and also for us to identify ways in which we can alert the users of those sites in a useful

way to some of the risks that they face when they are trading or otherwise in the online environment.

Ms MARINO—I would be interested in what ‘in a useful way’ means—how you communicate that. Also, under the current provisions of the Trade Practices Act, do you have the capacity to manage the risk as you see it from what you have already been looking at on those sites?

Mr Ridgway—In our view, the conduct online is often a replication in that environment of conduct that otherwise has historically been in the offline environment. The principled basis of the TPA adapts to all the environments equally, so it is really just a practical question of whether or not we are best able to identify and stop the conduct. In fact, the online environment often will provide us with some degree of access to the identity and location of individuals because of the nature of that environment, so in some ways it can facilitate outcomes. In other ways, of course, there are challenges, as there with any enforcement matter that we pursue.

Mr Gregson—I might just add, in relation to social networks, that there is most definitely behaviour that is not the ACCC’s area of responsibility—the predatory type behaviour on the internet—so, if you are looking at those types of areas, we are very much interested in the misleading and deceptive and the scam type behaviour; there are probably a broader range of other issues that you are turning your minds to as well.

Ms MARINO—There are all sorts. The marketing side is what I was interested in from your point of view.

Mr Ridgway—In a slightly fuller answer to the question of ‘useful ways’, that is a question that we are working through at the moment to identify what an appropriate and the best way is to reach consumers in that environment.

Ms MARINO—Thank you.

CHAIR—Who are the members of the Australian Consumer Fraud Taskforce, how often do they meet, and what does it actually do?

Mr Ridgway—The ACFT has been in place since 2005. There are 20 members. Mostly they are Australian police forces and offices of fair trading. We have the ACCC and ASIC, of course; the ACMA; and the Department of Broadband, Communications and the Digital Economy. We also have the Australian Institute of Criminology, the Australian Bureau of Statistics and the Australian Federal Police force, and we have our consumer protection counterparts in New Zealand who are members. I could probably provide a fuller list on notice.

CHAIR—That would be great.

Mr Ridgway—I do not quite have it at hand. Historically, the fraud task force has had three efforts. One is awareness raising, one is enforcement and disruption and one is research, hence the institute.

CHAIR—Do you mean disruption of internet—

Mr Ridgway—Disruption of scam behaviour. Disruption is a sort of complementary strategy that we use in addition to per se enforcement and stopping and prosecuting individuals. The disruption is about identifying what it is that gives the reward to the scam or to the crook, basically, and how we disrupt that flow of cash et cetera.

CHAIR—So it is like prevention?

Mr Ridgway—Yes, and we have had some successes there. If we can remove the money flow, we remove the incentive. That is basically it. Going back to the task force itself, in recent years we have had a fairly strong focus on what we have called a Fraud Fortnight—this year it was a fraud week—of concerted awareness raising in one particular fortnight—or week—that is coordinated with the international mass-marketing fraud effort by the International Consumer Protection and Enforcement Network. That is in mid-March. We are moving next year to a series of events over the 12 months whereby there will be a number of awareness-raising events that will be hosted by various members of the task force so that we have more frequent opportunities to alert consumers to—

CHAIR—So it is awareness raising for consumers, not the enforcement agencies?

Mr Ridgway—That is right. The agencies are members of the task force, and there is a combined effort by those members to raise consumer awareness. We find all sorts of opportunities to do that. Aligned with that, the task force also has a focus on useful research to identify the costs. The information cited by Scott earlier was that \$1 million flows from research by the Australian Bureau of Statistics, also a member of the fraud task force. The Institute of Criminology is also doing quite a bit of work there. Finally, in relation to the number of meetings, historically the task force has met quite frequently—sometimes fortnightly or monthly—and, as we move forward, we are looking to have a number of discrete functions where substantial efforts come together on either the research or the learnings of enforcement issues between members of the network spread over the 12-month period.

CHAIR—So its main task is just awareness?

Mr Ridgway—No. Sorry if I have given the wrong impression. There are three tasks. The task that most people hear about is awareness raising. The second task—they are equal—is enforcement and disruption. That is not so much in the public domain. It is very much about the police agencies, the fair trading agencies, the ACCC and all the regulators working together to share information and look for joint opportunities to identify and disrupt the conduct. The third effort is the research to get a better handle on the size and shape of the mischief and also how consumers respond to it—how do these scams actually work? That better enables us, the regulators, to explain these scams to consumers in ways that are going to reach them. It also enables us to disrupt the scams once we understand the mechanisms behind the front that you see when it pops up on your screen or in other ways attacks you. So those are the three main areas.

Mr Gregson—Ancillary information sharing between regulators is the sharing of techniques to deal with these problems, whether they be enforcement or disruption techniques. We certainly find that discussing the same problems with our counterpart regulators is one of the best ways to enhance our skills and find new ways of dealing with these matters.

CHAIR—How many people in the ACCC are involved full time on cybercrime?

Mr Gregson—In terms of full-time staff, we have up to about 140 investigators within my purview in the ACCC. They cover the broad range of trade practices matters, many of which will involve scam type behaviour. We have some resources—a team within our Canberra office—that has a special focus on these types of activities. That team ranges between three and four staff working specifically on these types of matters. But that is heavily supplemented. For example, the two matters I referred to today are run by our investigators in our state and regional offices.

Mr BILLSON—Your explanation about the interagency coordination is helpful, because it is terribly confusing for us, and I hate to think what it is like for someone who does not spend days talking about it—it is rather tough. Is there an argument that there should be a central hub, a focal point, for intelligence sharing and responsive and timely action where there is a problem coordinating some enforcement activity? That has been put to us by a number of witnesses. Do you have a view about that?

Mr Ridgway—The Australasian Consumer Fraud Taskforce does in effect provide a form of hub—that is, if information or concerns or emerging issues are identified by any members of the fraud task force they come to the rest of the task force.

Mr BILLSON—That is great for the in crowd, but Joe average, who is not quite sure what to do, would not even know the acronym.

Mr Ridgway—And the portal that the fraud task force refer to in all of our awareness raising is the SCAMwatch portal that the ACCC has responsibility for maintaining. So no matter whether you hear it from ASIC or from the ACCC or from the ACMA or the state police forces in their scam material, SCAMwatch is the common point of reference. When someone goes to visit SCAMwatch to report some concerns, when they click on ‘Report a scam’ on the front page, that identifies which particular area, which particular agency, has responsibility for that. So if they want to report spam, then the SCAMwatch portal tells them, ‘This is a matter that the ACMA can help you with.’ If you are reporting a financial scam, that will be ASIC. If it is a direct banking scam, we suggest that the individual contact their local bank, because they have quite active security measures in place, of course.

CHAIR—That leads me to the next question. Those in the non-officialdom space have put to us a view that the industry itself has great knowledge and insights that would be beneficial. Some sectors such as the banking industry have an enormous self-interest in being very upfront and cutting-edge, and their preparedness to share insights and information and trends is not always reciprocated. In the case of the AFP and the like, they get a bit of a diluted sense of what they are seeing. Is that because of the arrangements that are in place, or is there a need to recalibrate that partnership so that there is a little more openness?

Mr Ridgway—I think it is a really good question. We have active partnerships with the banks—if not all of them then certainly the majors—as part of the task force awareness-raising aspect of the work we do, as well as with significant online portals such as eBay and so forth. We have partnerships with insurance companies. There are a whole range of private partners. A lot of the work we have done historically with the fraud task force with private partners—and community partners, like the Country Women’s Association and Neighbourhood Watch and so

forth—have been in the awareness-raising aspect, and we are contemplating at the moment whether or not there are other aspects of the scams work that we do that could draw them in a bit more, say, to the research and identification. Certainly the door is not closed. But most of our material going out to our private partners to my recollection is more focused on their capacity to assist in awareness-raising. But we certainly would never dissuade anyone from identifying something to us and raising it. And, practically, if not within the discussions of the fraud task force meetings themselves, certainly a number of the private institutions do come to us to alert us to scams they have privately identified.

Mr BILLSON—So you sense your tool kit is about right? If I could cut to the chase, do you feel you have the tools that you need?

Mr Ridgway—Yes.

Mr BILLSON—On the issue of fit-for-purpose technologies and vendors' responsibilities: if I sold a child-restraint for my car and it was brittle and blistered in the heat, you would be interested.

CHAIR—Would you?

Mr BILLSON—So that goes beyond point-of-sale fit-for-purpose into its more durable use. Is there an argument that you could run that line past some of the vendors of technology and say, 'It is not enough just to have it shipped out of your premises fit-for-purpose; there is a durable-use expectation that accompanies that sale, and we therefore think you should take certain steps,' whether that be information, or loading antispam software, or whether it be something ongoing. I am just throwing that out there as a different way of looking at this product set and whether there is an expectation that we could push a bit harder with the stakeholders and players in the area.

Mr Ridgway—Perhaps I could hazard a partial response. Without wanting to throw too much grey in, I will use an analogy of the motor vehicle area. In purchasing a car, some people will pay a premium for cars with cushion airbags and other advanced technology; others will opt to pay a certain price for a car that will meet the mandatory safety standards but will not have the additional protections offered by a five-star NCAP rating.

Mr BILLSON—But a loaded software might be sold with a discount which is just good for now and you have not bought a service that updates it routinely. That does not mean you do not meet any safety standards—just picking up on that analogy. There would be that calibration. If you want fortnightly online updates of antispam software, fine, that is this package—but at least when it is shipped out it has got that 'best of breed', arguably, of what is around at the time it is purchased.

Mr Gregson—The fit for purpose issue actually does come back to the warranty and refund issue that we touched on but then moved away from with a slightly different focus. The Trade Practices Act provides statutory warranties for consumer products in Australia, as does other fair trading legislation. One of the issues they provide for is that consumers are entitled to products that are fit for purpose and free of defects. What that means in any one circumstance will depend on the circumstance, but you could foresee situations where a product did not match its description, where it potentially was not fit for its purpose because it could never do what it was

said to be able to do. They may well be addressed under the warranty and refund provisions, which provide rights to consumers to take their own actions in relation to that. Those provisions are also the subject of government review at present, about whether they provide sufficient capacity for consumers to enforce their rights. We are happy to provide you with information about that review to see whether it links into some of the issues you are raising.

Mr BILLSON—Coming back the other way, when I buy a coffee from Maccas, just in case I was not sure it says, ‘Caution: hot contents in cup’. Obviously there is a whole lot of litigation that sits behind that and that is all gripping stuff, but they are trying to guard against harm and risk. Is there an argument that—

CHAIR—Liability is what they are guarding against, rather than harm and risk.

Mr BILLSON—I am a reservoir of goodwill, so I am hoping it is for more virtuous reasons, but you are absolutely right! But going to the next step: why is that not a reasonable expectation of somebody’s technology, where even in its boot-up screen and things like that it might say, ‘Be aware: this technology may be vulnerable to scamming, malware,’ et cetera? I am just wondering, thinking about that awareness building, why we do not look at those opportunities as well.

CHAIR—I have an example of that. One issue that has been raised with us is the risk involved in routers that do not have a proper password put in. At the moment, if people do not put in a password, it can be very easily misused. Not only may the router not work effectively but it would basically compromise the whole computer system. The manufacturer could very easily set it up so that, when you turn it on, you have to put in a password before you can utilise it, therefore safeguarding your whole system. The cost involved in that would be, I would have thought, pretty small.

Mr BILLSON—And it is a known risk too, which I think is the point we are getting at.

CHAIR—A quite well-known risk.

Mr BILLSON—With newer technology, we have known risks associated with it.

CHAIR—Is it that the legislation does not allow you to enforce that, or is it that you just do not do it?

Mr Gregson—We are entering into areas that relate to the law of tort of negligence.

CHAIR—It is not tort. It is a contractual relationship, as there is with any sale of product. Basically you are selling a product which actually is not fit for use. You are buying it for a particular purpose—to make your computer system work better—and the way it is set up means that it actually does the opposite or potentially does the opposite.

Mr Gregson—Certainly, and we have dealt with the warranty and refund issues which provide consumers with products that are fit for the purpose that they are sold for. If there are arguments—and it would depend on the circumstance—that those products simply are not fit for their purpose or they have got some defect and they do not deal with what they say they will,

then they are matters that may afford consumers rights in those contractual relationships. The extent to which those warranty and refund rights are effective for consumers is subject to the current review before government. The ACCC does not have a role in enforcing those private rights. We can provide information—

CHAIR—But is it a breach, anyway? What we are asking you is: does the legislation deal with that sort of issue where the product itself can compromise the cyber security of the computer system it is meant to be part of by failings in the way it operates?

Mr Ridgway—I think the framework of warranty rights currently under the TPA looks at whether or not there are inherent defects or faults in a product. At the moment, we are grappling with a product that, stand-alone, absent some malicious external sort of impact, will function as it is intended to function. It is perhaps more or less vulnerable to an external attack. We do look at these issues on a case by case basis but, in the hypothetical, something that functions quite well or quite appropriately, absent that malicious attack by a third party, is not, I would think, going to fall foul of the warranty provisions.

CHAIR—Can I put it to you another way and maybe ask more in the positive: bearing in mind the cyber environment in which we now live, with the high number of attacks—and we have a parliamentary system, which I think is reasonably good, with firewalls and I get probably 20 or 30 scam email attacks, all sorts of things, a day—should amendments be made to the Trade Practices Act that allow consumers to be protected from software or hardware being sold that makes them susceptible to attack without their knowledge?

Mrs HULL—Who is responsible for consumer protection in these circumstances?

CHAIR—Hang on, I want to get an answer to the question. Do you think that there needs to be amendments to the act in order to protect consumers in those circumstances? Essentially, what you seem to be saying is that the present legislation does not cover that situation. You may wish to take this on notice, because I understand it is a difficult question.

Mr Gregson—I am happy to see if there is more information we can provide on notice. I do not want to sound evasive or appear difficult on the question, but the Trade Practices Act has a broad range of general prohibitions. They may apply to certain circumstances, depending on what it is. We have warranties and refunds, we have misleading and deceptive conduct and, in the extreme, we have unconscionable behaviour. They may touch on some of the issues you raise, but they do not provide a specific requirement that you are referring to to ensure that the products sold will cover every contingency.

CHAIR—Hang on, you are not actually answering the question I am asking you. My question is: would the Trade Practices Act need to be amended to protect consumers from being sold hardware or software, the manufacturers knowingly selling it to them, knowing it would make them susceptible to cyber attacks? Would the legislation need to be amended? I think the answer is yes from what you said before.

Mr Gregson—To have a specific prohibition it would. I do want to answer. I am not being difficult at all, but there are a broad range of general prohibitions that may apply in certain circumstances.

Mrs HULL—So the act does not prevent that happening now?

Mr Ridgway—No.

CHAIR—That is what I am saying. You have just answered saying that, at the moment, as long as the product itself works, it does the job, even if the manufacturer knows that, unless you take further steps, it makes you vulnerable to attack, there is no breach?

Mr Gregson—I think I have been quite specific on two occasions now. The act has a number of broad- ranging prohibitions that may apply in certain circumstances. It does not have a specific prohibition requiring what you have referred to. If policymakers felt that such a specific prohibition was required to catch all circumstances then yes, you would need to look at either the Trade Practices Act or at some other mechanism for doing so. I do not want to be difficult, but we pride ourselves on trying to be a creative and effective regulator and, where we can, we will use the broad range of provisions available to us to address the issue of consumer harm. So there may well be circumstances where the behaviour of manufacturers or marketers can be addressed under those broad prohibitions.

CHAIR—Could you go away and come back to us on that. Within the legislation you operate under, is there any remedy or action that the ACCC could take?

Mr Ridgway—I have a complementary comment. I think I understand the thrust of what is in the committee's mind—that is, that perhaps some information is required to be provided to consumers so that they are alerted to the fact that there is a hazard out there and they need to take caution.

Mr BILLSON—Risk and vulnerability.

Mr Ridgway—The closest analogy I can think of is some of our information standards. There is an information standard regime already under the Trade Practices Act. For example, it is used in relation to care labels on garments so that, when people have their garments laundered, drycleaners and other professional service people can identify the nature of the fabric and avoid the harm that would be caused by using the wrong chemical. It is similar where a policy case is made through the regulatory impact assessment process and there is therefore a capacity to develop an information standard that would be fairly useful in this space. I would note, though—and again we do not want to sound too cautious—that there are already a number of commercial offerings of virus protection, alerts and so forth. So I suspect that the consideration of whether an information standard would be necessary would be in light of what is already out there in the marketplace.

CHAIR—The point Mr Billson made was probably slightly different from that. I do not think it is just a matter of alerting people that there is a risk.

Mr BILLSON—I am just calibrating the different things. The chair is quite right—you should go further than that but, as a minimum, people should be alerted to the risk that they are exposed to if they do not invest in the optional extra of a protective package of software that is updated and all those kinds of things. Quickly moving on, the Spam Act has been well received. The Cyberspace Law and Policy Centre in Sydney says the malware potential opened up by

spamming is not adequately addressed. Do you have a view on that? If a spamming episode draws people to a site that activates malware and drags you into a botnet or something like that, that is far more substantial than the nuisance—if I can use that term—of the abatement objective of the Spam Act. There is another layer of harm, so should another layer of penalty be introduced?

Mr Gregson—Certainly regulators look for the most effective way of addressing a problem, and sometimes spam legislation may deal with it. If it gets more into the field of consumer fraud then either the police forces or us would look at that subsequent conduct. I should note that there is currently a series of reforms to the Australian consumer law which will provide additional remedies to both the ACCC and other regulators, including civil pecuniary penalties, which is further armoury for us to deal with some of these issues in the consumer protection field.

Mr BILLSON—‘Fit for purpose’ is a great concept, but what if you have got something that is beyond the purpose for which you purchased it? You have got embedded functionality that you did not buy, that you do not want and that you did not consent to. It is either at a software level to allow someone to draw data out of your technology or it is like the British Telecom case with its broadband spend. In that case there was a concern that some of the technology people bought did a whole lot of other things that gave some remote operability and functionality to their hardware. It was not what they bought; it was alleged that it was there for other purposes. Where do we stand on that and do you have adequate tools to deal with that? There is no question that it does what you want it to do, but there is all this other stuff that you did not want and did not consent to that is not under your control and may in fact be detrimental to your interest. It may not have been activated, but it sits there. Do you have a view about whether you are equipped to deal with that kind of circumstance?

Mr Gregson—Again, there would be no specific prohibition to deal with that scenario. We would look at the circumstance to see if it was misleading and deceptive, which we do across the broad range of all our complaints.

Mr BILLSON—But they make no representation—and I have got a PC at home and some peanut is monitoring every application and use and the data that is on it. I did not ask for that. I did not know it was there. No-one said it was or was not there; it is just there. I feel that that is a real—

Mr Gregson—An important part of that is misleading conduct—

CHAIR—We really have to close up because we are about to run into question time. Can I ask you to take Mr Billson’s question on notice. Also, we have a number of further questions that we did not have the opportunity to get to. Would you mind if we provide you with those questions and seek responses in writing?

Mr Gregson—That would be wonderful. On the issue that we do not quite resolve, we will endeavour to provide more information about the broad provisions of the Trade Practices Act.

CHAIR—Thank you very much for attending. I am sorry that our time was a bit squeezed by other activities, but it was very much appreciated.

Resolved (on motion by **Mrs Hull**):

That this committee authorises publication, including publication on the parliamentary database, of the transcript of the evidence given before it at public hearing this day.

Committee adjourned at 1.50 pm