



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

**HOUSE OF
REPRESENTATIVES**

STANDING COMMITTEE ON COMMUNICATIONS

Reference: Cybercrime

WEDNESDAY, 9 SEPTEMBER 2009

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

TO EXPEDITE DELIVERY, THIS TRANSCRIPT HAS NOT BEEN SUBEDITED

INTERNET

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

The internet address is:

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

To search the parliamentary database, go to:

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

HOUSE OF REPRESENTATIVES
STANDING COMMITTEE ON COMMUNICATIONS

Wednesday, 9 September 2009

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

Members in attendance: Mrs Hull, Mr Billson, Ms Collins, Ms Marino 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

CARTWRIGHT, Dr Jenny, Coordinator, Crime Prevention, Australian Federal Police 1
GAUGHAN, Commander Neil Anthony, National Manager, High Tech Crime Operations,
Australian Federal Police 1

Committee met at 12.46 pm**CARTWRIGHT, Dr Jenny, Coordinator, Crime Prevention, Australian Federal Police****GAUGHAN, Commander Neil Anthony, National Manager, High Tech Crime Operations, Australian Federal Police**

ACTING CHAIR (Mrs Hull)—Welcome. I would like to declare open this public hearing of the House of Representatives Standing Committee on Communications inquiry into cybercrime. This is the second public hearing for the inquiry and the committee will take evidence from the Australian Federal Police. The inquiry into cybercrime will examine, amongst other things, the nature and prevalence of cybercrime and will investigate the adequacy of current measures to prevent and mitigate the impact of cybercrime on consumers.

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. Thank you for making yourself available for this hearing. I invite you to make an opening statement, then we can proceed to questions.

Cmdr Gaughan—If I could make a short opening statement that would be appreciated. The Australian Federal Police welcomes the opportunity to appear before this committee. We particularly welcome efforts on the part of the committee to determine the real impact of cybercrime—or technology-enabled crime, as I like to refer to it—on the Australian public. The AFP appeared before a similar inquiry in 2003 and, whilst the cyberenvironment has changed significantly during that six-year period, unfortunately some of the challenges that law enforcement now faces are the same as we faced in 2003.

Probably one of the most difficult challenges we face is that technology-enabled crime is actually multijurisdictional and does cause us some problems in relation to prosecution and investigation of those particular types of matters. As such, the AFP rely very heavily on our international network. We currently have 35 members posted offshore and we rely on those particular people to leverage off our relationships with law enforcement agencies in other countries.

Obviously, the law enforcement environment has changed markedly since 2003 and the AFP continues to change, with a new commissioner appointed this week. So it is imperative that the AFP as an organisation remains flexible to deal with the dynamic environment that we are currently facing and we need to ensure that we have the capacity and the capability to respond effectively to the next cyber law enforcement challenge which may be an issue—that is, cloud computing.

To position itself to respond to the types of issues that confront us, the AFP established the High Tech Crime Operations portfolio in March 2008. This was after the second Ministerial Council for Police and Emergency Management, or MCPEMP as it is known, in November 2007 endorsed the former Australian High Tech Crime Centre to become a business unit at the AFP. In effect this meeting, which all jurisdictions are represented at, agreed to disband the Australian High Tech Crime Centre and move to a different format. The AFP established the High Tech

Crime Operations to consolidate all its technology related prevention and investigation functions under one umbrella as one way of mitigating the threat of cybercrime. The AFP has coalesced its high-tech investigations arm and high-tech operations support resources into one portfolio. In addition to incorporating the High Tech Crime Centre into the functional areas of the AFP, we have also integrated online child sex exploitation, cybersafety teams, child sex tourism, technology enabled crime and technical operations.

I am the first to admit that to some extent the coordination between state and territory police in relation to this particular issue needs some work. And in fact the Attorney-General's Department-led e-security review in 2000 also recognised that particular issue. We are currently working with the Australia New Zealand Policing Advisory Agency to establish an Australian e-crime investigators management committee which will sit under the ANZPAA Crime Forum. The AFP hopes that this forum will have strong representation from all jurisdictions and will operate in a cooperative manner. The first thing that I have asked that group to do once they are together, from my perspective, is desktop how we actually deal with these types of threats and these types of issues, because I know there is a fair amount of public disquiet out there about how police services in this country are currently dealing with these issues.

The majority of activities that take place on the internet are legitimate, but the convergence in communication provides opportunities for criminals to conduct operational activity more efficiently, securely and economically. This technological change requires law enforcement to develop knowledge and practices for crime types occurring online or facilitated by online technologies. Technology will continue to pose many problems for the AFP. I spoke earlier about the key issue in relation to the AFP having international relationships and I cannot stress the importance of that enough. We work very closely with the FBI, Serious and Organised Crime Agency, Royal Canadian Mounted Police and New Zealand Police through the Strategic Alliance Group as one way of understanding the cyberenvironment a bit better than what we do. We have also got dedicated liaison officers related to high-tech crime currently in London and Washington. The FBI reciprocate this arrangement with an attache from Washington over here in Canberra in relation to child sex offences. Further to that, we have also got an officer currently seconded to the Child Exploitation and Online Protection Centre in London, and her main focus is the protection of children.

The AFP is also a member of the Virtual Global Taskforce, which is a collaboration of countries that look at online threats to children, and the AFP is the designated chair of that group and will take that over in December this year.

The AFP works very hard to foster strong working relationships with industry, including Telstra, Microsoft and the Australian Bankers Association. I am fully aware that those organisations are not always going to agree with the AFP, but certainly we would like to foster those relationships. Working with the ABA, the AFP has established joint investigation banking teams in Sydney and Melbourne. In the near future an AFP officer will be posted to Microsoft in Redmond. This will be the second such AFP officer to undertake that secondment. In June this year the AFP hosted the Australian High Tech Crime Conference with our partners the Australian Institute of Criminology and the University of Technology, Sydney. We see things such as this as a way of sharing information and building relationships to enable the AFP to work more closely with others to tackle the threat of technology enabled crime.

Finally, I think that we see education as the key, particularly in relation to fighting technology enabled crime. From my perspective, every time I get an opportunity to speak in a public forum I say that the end user is the weakest link. Regardless of what banks and telcos and ISPs and the like can put in place to protect the customer, if the customer or the home user does not have a strong internet security process in place in their home, things are going to fall over. To that end, the AFP is involved in education programs. With Microsoft and ACMA we successfully piloted ThinkUKnow, which is an internet safety program that primarily teaches parents and carers. In 2010 we will roll that program out nationally. So, basically, it is about the relationships to enable us to investigate the crime types but more importantly it is about education. If we do not educate the community we are really going to suffer into the future. Thank you.

ACTING CHAIR—Thank you very much. You mentioned in your opening address some of the issues surrounding questions of jurisdiction in those particular areas. What do you see as the gaps in the Commonwealth's current technology related laws? Basically, do you consider that the Commonwealth police powers for technology related crime are on par with their state counterparts?

Cmdr Gaughan—I do. I think that the majority of our offences are covered by computer crimes in part 10.7 of the Criminal Code Act. Those offences are pretty much mirrored in state and territory legislation. So, from my perspective, the legislation is sufficient and the penalties in the legislation are sufficient. I suppose the question that arises is the coordination of the effort of law enforcement agencies, and I think that is where the difficulty currently lies.

Ms RISHWORTH—I appreciate your comments there about the end user being really important. Both Julie and I noticed that in your submission you estimated that 50 per cent of people did not change their behaviour once they had been caught by this. Can you tell me what types of behaviours they perhaps should have changed and what they did not change?

Cmdr Gaughan—It is simple things like not changing passwords. They do not ensure that their antivirus software is up to date. They did not ensure that the antispyware software was up to date. I think people are of the view that it has happened to them once, so it will not happen to them again, and therefore they become complacent. You can use the analogy of burglar-proofing your home. People have that attitude that it will not happen to them, so why worry about the deadlocks, the alarm et cetera? But unfortunately in the cyberworld you have to continually update these things once you have put them in place, because the use-by date is quite quick.

Ms RISHWORTH—How much is preventable? You hear these stories about skimmers—I don't know the technology that well—skimming off your bank details if you send them in an email. Obviously that is difficult to prevent without taking precautions, but how much of this is about updating your virus software and that type of stuff?

Cmdr Gaughan—One of the difficulties we have is actually quantifying the extent of the problem. So, to some extent, that question is a little bit difficult to answer, but again I use the analogy of the house. If I have really good software on my computer at home and everything has been updated sufficiently, in the same way that my alarm system in the physical environment is strong, the crook is not going to break into my house—they are going to break into the house next door. It is the same with the software et cetera that you put in place. You are not going to stop the really motivated criminal from getting into your computer, regardless of what you have

in place, but it is the same with your house. If you have a very, very robust security system in place, if the crook wants to get in, they will get in. They might not get in overtly but they will get in.

Mr BILLSON—I will start with what you have discussed in terms of metrics and your data about community awareness. What is your sense of the percentage of computer users—home or business—that have contemporary, up-to-date, refreshed software protecting their systems?

Cmdr Gaughan—Less than 50 per cent actually have software, and we are saying that probably about 25 to 30 per cent patch things regularly and keep up to date.

Mr BILLSON—Do you have a target in mind? I know McAfee keeps sending me reminder notices—I am very fond of those. But do you have a goal through your discussions and your networks about what is an acceptable level and how to bring about that change in coverage?

Cmdr Gaughan—The acceptable level, I suppose, is zero, but realistically we are never going to achieve that. I would like to see a day come by where we get to 75 or 80 per cent. I think one way to do that is with a really strong public education message. If we look at the messages that have previously been sent by federal governments about things such as health—slip, slop, slap in relation to skin cancer et cetera—they can actually change the culture. That message changed the way the Australian public dealt with sun. They did put on a hat, sunscreen et cetera. You could even go back to the AIDS campaigns that were run many years ago. Again, that changed the culture. What we need to do with the internet environment is to change the culture. We need people to become aware of the fact that they are at risk and we need them to change their behaviour.

Mr BILLSON—What about the extent to which the ISPs are front and centre in that? To change the culture of internet use, someone is using the internet and therefore you have a service provider who is very well placed to deliver advice—wise counsel. Have you had much luck collaborating with ISPs where they make a virtue of protection as a package of services they offer or routinely reminding their clients about this opportunity?

Cmdr Gaughan—It is a regulated industry. To some extent that does occur through the regulation. One of the issues I have is that there are so many internet service providers in this country—I would not even put a figure on it. The larger ones do play an active role. They almost see it as if they have a responsibility to educate their customers. But, still, just because you educate someone does not necessarily mean they are going to change their behaviour. You can lead a horse to water but you can't make it drink—to use an old metaphor.

Mr BILLSON—You do not work for McAfee!

Cmdr Gaughan—No, I definitely do not. But, to be honest, I spoke about relationships with industry and McAfee are one of those organisations that we are in regular dialogue with. They are obviously trying to sell a product, but they also are trying to sell a product that protects the Australia people, in their view.

Mr BILLSON—I would like to take you into a space that is slightly aligned to what you are saying. We have heard about that level of cooperation, but we have also heard that, let's say, the

DPP and others are not always as responsive to concerns around this aspect of criminality. Is there a requirement for our committee to elevate the importance of decisive action from DPP to support your efforts and those of the policing jurisdictions?

Cmdr Gaughan—I think again it is an education process. To be honest, I do not think it stops at the DPP; it probably goes one step further than that. We see it not only in relation to the number of matters that are actually taken before the court; to some extent we have seen what the penalties are for these particular offences and the sentencing is not quite the same. I will not say anything further on that.

Mr BILLSON—You include a description in your submission of cybercrime or technology enabled crime. I wonder if it is deficient in its reach. I put to you a thesis that the behaviour, the loss and the harm captured in the current criminality definition are deficient in that they do not reach further and talk about protection of people's personal safety and wellbeing. I would have thought that having cybertrespass software on your system but not activated should be a crime. I would have thought that having functionality embedded in your technology that someone else can activate that you have not purchased and do not control should be a crime. Sorry for getting a little evangelical about this, but, if we are about achieving a just and secure society, the personal security issues and the hurt that can come from technology enabled assaults on people's reputation and their personal wellbeing through the broadcast of material, intimidation and these kinds of things should receive a greater focus. I just wonder whether the tool kit is too focused on a definition of harm that has some kind of financial loss or some material impact and we are not focusing on cybertrespass, cybervilification, sim-stalking, damage to reputation, assumption of identity—I have pages of examples.

ACTING CHAIR—We might ask Mr Billson to hand that over to you later if you want to respond at a later time—if he requires that.

Mr BILLSON—I am happy to. It goes to the heart of what the problem is that we are trying to solve. I guess I am putting to you a thesis—dressed up as a question so the chair does not get upset with me—that our description of what criminality is quite nostalgic and there are a whole new lot of what I think are crimes against the person or crimes against the capability that people hold that are not well covered in the current legal framework.

Cmdr Gaughan—I suppose you could argue that we have structured the legislation based on the non-cyber environment and now the cyberenvironment has changed and we may need to consider that the legislation needs to keep up to date with cyber as it moves forward. One of the concerns we have more broadly in relation to the legislation is the fact that every time a new offence is depicted—such as vishing, which is the new thing; it is mobile phone phishing, where basically now people are receiving SMSs—

ACTING CHAIR—What is that?

Cmdr Gaughan—People are receiving SMSs et cetera in relation to disclosing bank account details. The legislation covers it but to some extent we are on the very edges of using that particular type of legislation for these crime types.

Mr BILLSON—It is a number based trawl so the character spread is less—

Cmdr Gaughan—Correct. One of the issues we have, moving forward, is to future proof legislation so that every time something else comes up in this environment we do not have to come back continually to parliament to change the legislation. One thing that we would be keen to work more closely with parliament on is how we could make that happen.

Mr BILLSON—I invite you to come back to us. I am happy to give you this but if our job is to tackle mischief that we want avoided and problems that we want solved I think there is a definition problem and we are not quite—

Cmdr Gaughan—Yes, certainly, we will look at that.

ACTING CHAIR—Maybe we could put together Mr Billson's material as questions on notice and send them to you for response?

Cmdr Gaughan—Yes, certainly.

Ms COLLINS—Do you have any statistics on how many people are affected by cybercrime—I know many people that have been affected that have never reported it—and how you educate people about who they should report it to and how?

Cmdr Gaughan—I think the second part of your question is a real issue. We do not have any statistics. I think I said earlier in response to another question that one of the difficulties we have in quantifying the exact nature of the crime is that we have received a lot of anecdotal information that there is a fairly significant amount that is not reported. It is up to law enforcement as to how we deal with that—hopefully, through this ANZPAA forum that we are trying to establish. It has actually come out with some clear criteria as to who does what in this particular crime type. There have been some models utilised offshore where there has been a one-stop shop where people go and report crime to one particular area. I was having discussions yesterday with a few people who will be appearing before the committee on Friday and it is something that they will be pushing when they get an opportunity to have a chat with you.

Mr BILLSON—Like the Queensland model for the Nigerian and Ghanaian fraud.

Cmdr Gaughan—Yes, a similar sort of thing, but then you get down to the issue of jurisdiction and who is going to investigate et cetera. It is a rather complex issue. They tried it in the UK where it works a little bit easier because they do not have a thing called federation.

Ms COLLINS—I am envisaging your education ad: 'Is somebody invading you in your home via your computer, blah blah blah. If there is, contact who, how, when, why.'

Mr BILLSON—Who are you going to call? Hostbusters rather than Ghostbusters.

Ms COLLINS—Exactly.

Cmdr Gaughan—I think if we are going to go down the path of, maybe, having a public education process that tries to change cultural behaviour then we actually need to have something in there that is a message as to who they contact.

ACTING CHAIR—I am running a forum myself in November in Wagga Wagga. The problem that we have is trying to engage with people, because a lot of people who think they are bulletproof have been brought up on the internet. They think that they know all about it and that the type of education that I am providing is for those people who do not know how to use the internet. They feel that they are bulletproof and they know it all, but they are the exact people who are getting caught. I think it is really difficult to educate and engage the community members to come out to talk about these issues. My forum is just a pilot to see how it goes, but the problem that I am having is getting people interested enough to come along and listen to the presentations. I will move on to Nola.

Ms MARINO—I am really interested in the organised crime side of your submission. I would be really interested to hear from you. What evidence do you have on the operation of these particular networks?

Cmdr Gaughan—Our focus, the focus of the government and that of the Attorney-General's Department is now on that organised crime space. Organised crime groups and the number of people involved, who operate in Australia, utilising the internet to commit crimes are quite limited. The majority of people involved in organised crime are coming out of Russia. That is not a new thing, it has been happening for a number of years. We are working very closely, with the FBI, particularly, and the US Secret Service, who have good relationships over there to try to mitigate some of that threat. Over the last couple of months, somewhat surprisingly, I suppose, there has been a renewed effort on behalf of the Russian authorities to assist us with some of these matters to the extent that we are starting to get some leverage with a couple of current investigations. We have done some mapping in relation to money laundering and issues such as that. We use the internet to map where these sites have gone and most of them are going back to Eastern Europe. When you have the difficulty of jurisdictional type discussions—

Ms MARINO—That is the next question. That is the issue we are dealing with.

Cmdr Gaughan—The UK was successful some years ago in a prosecution for a cyberattack where someone DDoS-ed a number of online betting agencies. I think that was the subject of a *Four Corners* program a couple of weeks ago. They were successful in that particular activity because of certain pressure that the English government put on the Russian authorities, and a number of people were arrested and charged. It is a matter of engaging them, I think. Obviously, this is where we have to leverage off our relationships with the FBI and the Secret Service, to actually get in there and get them to do our bidding for us.

As to the extent of the problem in Australia, again, it is very hard to quantify that because there is a lot of underreporting. But, at the moment, most of the crime is coming out of particularly Europe and America. I suppose the one thing we have also got to remember is that we have only got 20 million people in this country. To some extent the larger organised crime groups will target the larger population bases, based on the fact that they are going to have a better success rate. They are only interested in the money. We are even seeing instances where organised crime groups are involved in hosting pay-to-view child exploitation material. And that is only because they are interested in the money. They are not interested in child sex; they just want money.

Ms MARINO—Turnover.

Cmdr Gaughan—Correct. They do not care how it is as long as they keep making money.

Mr BILLSON—Going on further from Nola's point, that is the criminal issue. What about the service providers that enable the criminality—the botnet hosts and all those fee-for-service people that are in that space but might argue they are not actually doing it? What are the key challenges to suffocate that capability from getting into the hands of people who want to exploit it in the way you have described?

Cmdr Gaughan—We are having a lot of luck with that—well, not luck—because a lot of hard work is being done by ACMA, and others, with their relationships they have with offshore organisations to shut down those sites. But, to be honest, they will have 30 or 40 different web pages and they will just keep moving them around. As soon as we shut one down another one opens up. It is very cheap to set up these websites, and particularly when there is a lot of money involved they will continue to move around. It is frustrating, but we do get some successes.

Ms RISHWORTH—I am just following on from Kay's point of view, to get a bit of an idea of the public awareness. You see these emails come through, saying, 'Send us your money and we'll give you this amount of money.' Certainly, I look at it and think, 'Why would anyone do that?' But I have spoken to a number of my constituents that have fallen for it. The issue is: how do you do that education campaign? I just noticed that the Australian Computer Society has suggested that information be passed on when you buy a computer and that sort of thing. It seems very obvious to a lot of people, but it is still having a huge impact. Are you able to elaborate a little bit more on the types of educational processes? Obviously, there is the general public awareness, but are there any that are targeted? I probably should have asked this first, but what is the percentage of people falling for these very obvious, as opposed to the less obvious, scams?

Cmdr Gaughan—Again, the percentage is difficult to quantify, but I will say that the Nigerians and others are continuing to use the same scams because they are successful. They have not changed because they have been successful. If you have been keeping up with the media over the last couple of days the latest one seems to be people going in and taking over Facebook sites. They then send a post, saying, 'I am trapped in England and I need \$12,000,' and people are sending it. That is the scam. The reason why people fall for scams is that, as human beings, we have a tendency to believe what people tell us. The beauty, or the unfortunate thing, of the internet—whichever way you look at it—is that people can be on the other side of that computer and they are not who they say they are. That is one of the vulnerabilities we have as humans.

I think that the issue you raised about an education program is interesting. I was at a meeting here last week of the Consultative Working Group on cybersafety, which Senator Conroy has a lot to do with, through the Department of Broadband, Communications and the Digital Economy. They had a number of kids come in and have a chat with us about what they thought. One of the children there from, I think, Western Australia actually was of the view that, when you buy a computer, you should be on L-plates—that is, once you pass some tests and you actually become literate in how to use it and how you can actually protect your computer, then you get Ps and then, after a little while you actually get a full drivers licence, so to speak. I thought it was not a bad solution, coming from a 16- or 15-year-old kid, but how you educate the millions of people who have already got computers is the problem.

We also leverage off the kids we have got working for us in some of our youth forums to actually educate us. As to how we educate the broader public, I think that is outside my level of expertise. Perhaps what we need to do is speak to those people like those who designed the health campaigns for Slip, Slop, Slap about how they actually change cultural behaviours.

Ms RISHWORTH—As you mentioned, it is under-reported. As has been alluded to already, getting people to report it and to feel that it is an issue that they should report are obviously really important.

Cmdr Gaughan—A lot of people get their cars broken into and they do not report that to police either because they see it as a minor crime and think, ‘Why would I bother telling the police?’ Yet I suppose that if we know that you have had your car broken into, we could do a bit of an intelligence picture about it and maybe target that area. It is the same with cybercrime: if we know the full extent of it, we can actually do some work around mitigating some of those issues.

ACTING CHAIR—You just spoke of scam. It happened to me yesterday; a person that I frequently get emails from sent me an email saying, ‘Sorry I did not tell you that I was going to the UK, but I am here and I have left my passport and wallet in the taxi. Can you send me about \$2,060 or something. You know that I am good for it, because we have been friends for so long.’ Is there an ability to track that back. It came from his site, or from a similar site—there is probably some difference in it that I cannot see: a stroke or something. Is there an ability to track that through?

Cmdr Gaughan—There is, but you get to a certain extent and then you pretty much lose it. So you bounce it off different sorts of boxes, if you like, to an extent that it pretty much drops out. For instance, we know we can get it back to Russia or California and then we may lose it. It would depend on how good the crook is, to be honest. If they are a really sophisticated cybercriminal they will make it almost impossible for us to track them back. But that is no different to the real world. A really good criminal who is undertaking crime—whether it be burglary, rape or whatever else—will backtrack and there will be no physical evidence left.

ACTING CHAIR—How can somebody actually do that?

Cmdr Gaughan—I am not a technologist so it might be better asking someone a little bit more technical.

ACTING CHAIR—You mentioned the *Four Corners* program. In the program the AFP said that they post a warning on a forum—

Cmdr Gaughan—It was probably me, actually, who said that.

ACTING CHAIR—I am not particularly keen to say the name of the message board here—to effectively close down the site. There were some critics who wondered why the AFP did not try to operate the forum and covertly track and apprehend the users. This was pretty much a public statement in the *Sydney Morning Herald* from the Australian Computer Society. Can you explain that operation to the committee and say why the AFP took the decision to post a warning rather than covertly track?

Cmdr Gaughan—I will start at the beginning, but we did track. What actually happened was that there was a referral from the South Australian police—we work very closely with all our law enforcement jurisdictions. They had arrested a guy who owned admin rights to that particular forum, to that particular site. They then asked us to go in on an undercover operation to basically work that site as the administrator, which is what we did. One of our guys went in there as the administrator for a period of months, and we were able to obtain a significant amount of intelligence from that particular site. There were over 2,000 users in there. Some of them were in Australia and some of them have been arrested since that *Four Corners* program and work will continue to bring those people to justice. There were a lot of people on there that, in our view, were probably just hanging out in the forum because they thought it was a pretty cool thing to do.

If you like, it was almost like an education process: we made a decision, after we had gleaned intelligence from that site, to make that posting, basically to let people know that law enforcement was active in those particular sites and to let people know that sooner or later they were going to get caught. The reason we did that is this. I like to look at it as part of the compliance triangle which tax will always quote to you. You have got a certain percentage of the population, the majority of people, who will do the right thing. You have those in the middle who will do the right thing only because they know that law enforcement or the tax office et cetera are policing them and keeping an eye on them. And you have a small percentage at the top who, regardless of what we do, are going to continue to be bad. With that particular activity and that particular decision we were targeting that group in the middle. If we can get that group in the middle to actually move to the bottom and no longer become hackers or cybercriminals, then that will be a win for us.

We know that quite a vast majority of that group probably will, but a small percentage will go to the top of the tree and that is just the way it is. So, for us, it is almost like an education of the underground, if you like, where we are trying to get people to know that we are in there having a bit of a crack at them. It was very interesting meeting and reporting about that, to say the very least. I had some fairly interesting discussions with that particular journalist—

ACTING CHAIR—I bet!

Cmdr Gaughan—I have spoken to that journalist a number of times before and he has been very good, but he just has a way of doing things sometimes.

ACTING CHAIR—You said there have been some charges laid and people have been arrested since the program began. What charge is levelled against these people?

Cmdr Gaughan—It could be possession of credit card numbers in relation to a botnet. It is mainly under part 10.7 of Criminal Code Act relating to possession of malware et cetera. It is actually an offence under that act to possess that type of equipment, so the offences are mainly laid under part 10.7.

ACTING CHAIR—Following on from something that you said about Nigeria, Russia and others, several witnesses have said that Australia should sign on to the EU convention on cybercrime. Does the AFP have a view on whether there are any benefits in Australia signing on to the EU convention?

Cmdr Gaughan—My law enforcement colleagues overseas will tell me there are certain benefits. I really have not formed a view one way or the other, to be honest. It is currently with the Attorney-General's Department for consideration and I know that was the case under the previous government as well.

ACTING CHAIR—There is obviously some contention, otherwise it would happen, wouldn't it?

Cmdr Gaughan—There will need to be some amendments made to the Telecommunications (Interception) Act for us to ratify that. I think that the discussions we are currently having are around how we will reword the TI Act.

Ms RISHWORTH—What changes would have to be made to the act?

Cmdr Gaughan—I think it gets down to sharing information and things such as that—just tightening things up a bit.

Ms MARINO—I want to ask about the issue of the IT profession itself. In your experience, with the amount of personal information running through some of the IT companies, do you have any evidence of people within those organisations or companies passing that information on?

Cmdr Gaughan—The trusted insider?

Ms MARINO—Yes.

Cmdr Gaughan—Yes, there have been a couple of instances where we have been involved in those investigations. There is one currently before the court in Western Australia relating to that very issue where a trusted insider—an employee—has stolen personal information and tried to sell it. But that happens in all crime types, not just this particular one.

ACTING CHAIR—In that case, how do you keep your officers trained to give them the up-to-date forensic skills? Do you recruit from the private sector? How do you get your forensic skills up to speed so that you can try to match it with some of these criminals?

Cmdr Gaughan—Maybe I am more worried about the private sector stealing our people when we get them to a certain level! That happened to the AFP many years ago, when we lost pretty much all our computer forensic area to another agency. But, to answer your question, it is a bit of both. We do recruit people outside the organisation to upskill us. We get them from both the private sector and some other government agencies. There are some recent examples where we have got people in to train our people. We do a lot of in-house training. We are trying to get our criminal investigators or our federal agents to the stage where they can actually walk into a crime scene where a computer has been utilised and address that crime scene without having to call in the experts. The experts should only be used for the high-end stuff. But we really leverage off the relationships with our international law enforcement colleagues for that particular issue. We send people regularly offshore. I have a guy at the moment who is offshore attending an Interpol conference, where people are going to discuss different ideas about how they can work better on the internet and enhance their computer forensic skills. It is a combination of three

things. We work very, very closely internationally and we spend a significant amount of money ensuring that we keep up to date.

ACTING CHAIR—Say you were undercover in a bikie organisation investigating drug distribution—

Ms MARINO—Organised crime.

ACTING CHAIR—Do you have undercover officers who infiltrate, get involved, become part of it and then learn the system? Do you have that ability?

Cmdr Gaughan—There is. We have internet policing teams in Canberra, primarily, but we also have some staff in Sydney and Melbourne. In fact, most jurisdictions in Australia would have the same capacity—some limited, but the same capacity. The three officers we have working in Canberra are all former real-world undercover operatives. They have worked in that environment and now they are transferring those skills into the online environment. To that extent I am more than happy for the committee to pay a visit to us at some stage and we can walk you through some of those issues relating to what we do in the IPT. We have had the Parliamentarians Against Child Abuse and Neglect out there a couple of times already. But I extend that invitation to the committee and if you want to take us up on it, feel free.

ACTING CHAIR—That would be fabulous.

Mr BILLSON—In your submission there are two things that stood out: one is that you made reference to susceptibility to social engineering. I am not even sure I know what that means.

Cmdr Gaughan—I have sort of already mentioned it.

Mr BILLSON—I thought that may have been, but I read that and I thought that maybe I was misunderstanding it. Do you want to elaborate on it.

Cmdr Gaughan—Basically, it is how people prey on the naivety of people to have them believe who they are and, as such, you share your information when you probably should not.

Mr BILLSON—So, an appetite for that stuff.

Cmdr Gaughan—Yes, an appetite pre-Facebook, perhaps.

Mr BILLSON—You touched on evidence of admissibility as being a potential problem.

Cmdr Gaughan—Evidence of admissibility?

Mr BILLSON—Admissibility of evidence was highlighted as a legal challenge point around these issues.

Cmdr Gaughan—You have touched on the jurisdictional and investigative aspect. The admissibility is based primarily on the fact that we obtain a lot of evidence offshore and we obtain that evidence fairly quickly. We still rely a lot on the old MAR process—the mutual

assistance request process—for prosecutions in this country. To some extent that hampers us, because it is quite slow. So, in a lot of instances we actually go direct police-to-police and we receive information lawfully from those police officers to actually take us through the investigation process. But to some extent there are some problems in relation to us utilising that in a criminal prosecution. We also in many instances reach out directly to people such as Microsoft for the same reason: to get information pretty quickly. We have an investigation going at the moment where I can assure you this parliament certainly would not want us to go through an MAR process to deliver the outcomes.

Mr BILLSON—Is the current legislation before the parliament about international evidence admissibility in the hearsay rule going to make things better or worse?

Cmdr Gaughan—It will make things better. We have had a lot of input in relation to all that legislation through A-GD.

Mr BILLSON—With the nature of the crime, do you have any observations about industrial espionage—the accessing of information for application in another sense rather than for direct immediate financial gain? Also, is the trend to biometric data and the readability of some of those chips another area that we are grappling with?

Cmdr Gaughan—I think the issue of industrial and perhaps even larger espionage is one that we need to be aware of. There have been instances in the recent past where certain large companies in Australia have had their information hacked into, from places outside of our borders, for the purpose of financial advantage only. With the impending rollout of the National Broadband Network we need to ensure that the security and the resilience of that particular process is very strong. The AFP is engaging quite heavily with the other national security agencies and intelligence agencies to ensure that we are engaged very early in that particular process. Could you repeat the second part of your question?

Mr BILLSON—It was about the biometrics trend. I was involved with the stand up of the new biometric passport and see commercial applications of that technology popping up. In terms of identity theft I was wondering about the metrics that surround biometrics.

Cmdr Gaughan—I could provide you with a link into an Eastern European country and you could get an Australian passport and you would not know the difference.

ACTING CHAIR—My goodness.

Ms RISHWORTH—My question takes a step back to something that Bruce alluded to. Obviously, cyberbullying is something that schools are desperately tackling with—I know of schools in my area—whether it is through the phone, the internet, Facebook and all of these areas. I guess it probably might not sit with the AFP, but how do you get the police involved in that? People I have met probably do not think it is an issue for police involvement, so police have not been involved. But could police come down to the school, for example, and say to some of the young people, ‘This is a very serious crime.’ It might be that the legislation does not cover it. I am not sure what it is, but I would like your comments on how we might look at that as a criminal issue.

Cmdr Gaughan—The legislation, in my view, does cover it. But, to be honest, police will only get involved in a cyberbullying incident if it escalates. The social networking sites have a significant role to play. The AFP does get involved in these, and Jenny’s area actually delivers crime prevention strategies to kids through our ThinkUKnow website. We have mitigation strategies on that as to how people can deal with the issue of cyberbullying. The consultative working group that I spoke about earlier has a subcommittee that deals directly and only with cyberbullying as its key mandate. Senator Conroy has made it quite clear to the CWG that the government’s view is that cyberbullying is a real priority, and from our perspective it is a real priority. Again, it gets down to the communication issue that you touched on earlier, and I think the key message that has come from us is the ability to educate and communicate with people the fact that law enforcement is interested in these issues. When I was growing up in the western suburbs of Sydney, the police officers used to come in regularly and talk to us about different aspects. Now we go into schools and we talk about those same aspects but we include cyber in that as well, particularly the issue of cyberbullying.

Ms MARINO—I have a question which is particularly local. How does the law sit and your position sit in relation to young people who have photos taken of them in all sorts of circumstances that are then used in a way that can compromise them? We have touched on that, but where does the AFP sit within that environment?

Cmdr Gaughan—That is ‘sexting’, as we refer to it, where they take a photo on their mobile phone and send it. It is child abuse material—or child pornography, as it is legislated under the act—so it is a criminal offence. Kids sometimes miss that. If the child is under 18—we will say under 16—and he or she has taken a photo of themselves naked or in an erotic pose, it is child abuse material. There has been one instance in Victoria where they moved forward with a prosecution. Most times, in that particular instance, we would educate.

Ms MARINO—It is very important, because I have had instances in my electorate where I have had an employer, for instance, ringing me quite desperately because he has received—

Mr BILLSON—The families are just beside themselves—

Ms MARINO—some of those types of photographs of employees and he is thinking about where this leaves him.

Cmdr Gaughan—If it is an adult—

Ms MARINO—Yes.

Cmdr Gaughan—that is an interesting one. I do not really have the answer for you there.

Ms MARINO—The person has simply been sent these without requesting them. Whoever it is has just sent a whole raft of people a photograph. The person who has received them without wanting them is then in a very difficult position.

Cmdr Gaughan—Could I take that one on notice.

ACTING CHAIR—Yes.

Cmdr Gaughan—With kids it is clear, but with adults—it is harassment, I suppose, but whether or not there is actually an offence under the Telecommunications Act or similar I am not sure.

Mr BILLSON—Here are five more for you.

Cmdr Gaughan—Five more?

Mr BILLSON—Your job, and the job of all of us, is about securing a just, fair and secure society. The five are as follows: having identities assumed or created, involving new or manipulated images; the distortion of a person's personal interest, reputation or character; the broadcasting of personal data that is inaccurate, offensive, profoundly disturbing or intensely damaging; the use of ICT to bully or intimidate another party, to act in a manner contrary to their will, their free choice or interest; and maliciously and intentionally hurtful campaigns of retribution, of character diminishment with no public interest or freedom of speech value. Just get that into your initial content—it can be really toxic.

ACTING CHAIR—We will provide this to you.

Cmdr Gaughan—I know there was a website in Victoria some months ago that—

Mr BILLSON—Yes, in Geelong.

Cmdr Gaughan—That was referred, I think, to ACMA for a determination as to whether or not it was lawful to maintain that website. It is a really interesting question, Mr Billson, as to where that law enforcement commences and regulation comes into it.

Mr BILLSON—There is a spot in between, though, where people say 'freedom of speech'. There is no freedom of speech virtue in that; it is pure mischief. It is pure harm. There is no freedom of speech in that.

Cmdr Gaughan—It is malicious.

Mr BILLSON—We have the blacklisted content. We have take-down machinery for unlawful content. Maybe the halfway house is that this kind of stuff should be able to be taken down through the ACMA process, and that might be the way, so at least you can get a remedy—even if it is not criminality. The individual can get a remedy to abate the harm and achieve that goal of a just, fair and secure society.

Cmdr Gaughan—We need to make sure we future-proof it so that we move beyond mobile phones to whatever the next thing is.

Mr BILLSON—Yes.

Ms MARINO—Whatever the next thing is.

ACTING CHAIR—About the incidents that have been raised, I read recently where a woman had gone back to her room and had been photographed by a colleague, then that colleague

showed the photographs of the woman; she has taken court action on that person. Then again, that is a civil action, it is not a criminal action, and this was a 33-year-old or something woman and a young colleague, who was said to want to make friends as a result of showing this around and sending it off to others.

I would like to ask about identity theft. Obviously, it is becoming an issue to be dealt with. Is there a real issue with identity theft within Australia? Are people being targeted for identity theft? What is the main vehicle whereby people are accessing the kinds of information—the dog's first name, the birth dates, parents' maiden names et cetera—is it the Facebook type sites and that kind of social communication site? Are they the vehicles that see identity theft becoming more pronounced? Do we really have a problem with identity theft in Australia, or is it more in other countries.

Cmdr Gaughan—There is a problem with it—it certainly occurs. Again, it is one of those issues about how you actually measure it, because people in a lot of instances do not actually report it. To some extent people do not actually know that they have had an identity theft takeover until they go into their local post office to apply for a passport. They then get told, 'You have already got one.'

To some extent, you are right: most of the issues relate to social networking sites where people go in and give out too much information. A lot of that has got to do with the fact that they just share information with everybody and they do not actually lock down their profiles to friends only. One of the other issues, of course, is that malware is getting onto their computer and stealing that information. So it gets down to the original protection of the computer in the first instance. You have got to protect your computer and then you have got to change social behaviours in relation to how much information you actually share with other people.

ACTING CHAIR—Is it a serious enough threat that we should have a strong campaign associated with the kinds of protection that you need to put in place in order to prevent identity theft? If you had a level of, say, one, two, three or four things that would need to have an education campaign—we talk about education all the time in this hearing—what would be the key top education messages that you as the AFP would impart upon the people? Where would you start?

Cmdr Gaughan—By keeping your computer up-to-date, number 1. That actually mitigates a lot of the other issues we have discussed.

ACTING CHAIR—In keeping your computer up-to-date, how would you explain to the consumer why they need to keep their computer up-to-date? What would be the list of things that you would see as a threat to the user?

Cmdr Gaughan—You then need some road crash examples; you need some real, hard-hitting examples that 'X' had their computer taken over and lost their identity, and this was the result. I say 'road crash' intentionally—

Mr BILLSON—Yes—care or consequences.

Cmdr Gaughan—Exactly. There needs to be consequences; you are not going to change social behaviour unless there are consequences.

ACTING CHAIR—Do you have all of those examples?

Cmdr Gaughan—We could provide those examples of what we see has been the top four or five road crash issues to the committee. We will take that on notice and get something back to you.

Mr BILLSON—I suspect that is part of the lack of motive for behavioural change.

Cmdr Gaughan—I agree totally.

Mr BILLSON—Young people think it is a nuisance, it is a pain, ‘Yeah, I’m going to get mucked around a little bit, but my credit card has got a cap on how much I’m vulnerable for, blah, blah, blah,’ so it seems that to outline the horrendous consequences that may occur to motivate a change of behaviour, like those cigarette ads where the cancerous mouth is appalling, is an issue. People think it might be a nuisance, but not as harmful as it potentially is.

Cmdr Gaughan—I think that is 100 per cent correct. We are very fortunate in this country, whereby when people have their identity taken, or they have their bank details stolen, usually the banks will refund the money. It actually does not rest with the consumer, so there is no responsibility because there is nothing at the end of the day. I am sure you will hear from others that maybe that needs to change.

Mr BILLSON—Speaking of hearing from others, could I invite the other ladies to add to the conversation if there is anything we have touched on or they would like to add to the discourse we have had.

Dr Cartwright—My area looks after crime prevention so we are predominantly heavily involved in educating the whole spectrum of the community. We look at education for not only youths, parents, carers and teachers but also for senior members of the community.

ACTING CHAIR—Seniors are important.

Dr Cartwright—We were involved this year in National e-Security Awareness Week, where we went out to a number of locations in regional Queensland, New South Wales and the ACT and did workshops for seniors. We advised them of some of the things that they can put in place to protect themselves online and have a safe online environment. So those are some of the things that we do. The messages are different, depending upon who the audience is. In regard to youth, some of the presentations that we go out to schools and deliver focuses on protecting your online reputation. When we talk about consequences, we talk to them about the fact that if you upload provocative images of yourself to your Facebook or MySpace site this could potentially impact on you later on. If a prospective employer searches online and finds this information about you, is that going to have an impact on you later on? As Commander Gaughan said in regard to ‘sexting’ we also tell the kids that when you are creating these images and sending them to your friends are you aware that you are actually committing an offence? It is self-created child pornography.

It is partly about educating the kids and the parents. We have a campaign called 'ThinkUKnow', which we piloted in the ACT, Victoria and New South Wales, in which we look at talking to parents. So we are focused on the kids and on the seniors but we are also focused on the parents.

Ms MARINO—There is the other level of those who are in receipt, as I said earlier, and they just do not know what to do when it lands on their computer or their mobile phone. Here is this photo that I have not asked for and it could be someone in my workforce and they may or may not be in the age groups. What do I do and how do I deal with it within even my workplace, because it is an issue?

Cmdr Gaughan—You get all the harassment, bullying and all of those other issues.

Ms MARINO—Absolutely, but also then there is the vulnerability of the person who has received it and who did not want it. How do I handle it?

ACTING CHAIR—I think that message is clear. We are going to lose our committee members so I need to finish off here. We will be putting together a report. When you respond to our questions on notice, could you advise us what would be the take-home messages that you would like to see the committee really consider in compiling their report.

Cmdr Gaughan—I think the key issue that I would like the committee to take away and think about is putting forward a public message—a really hard-hitting train crash type scenario—that the message needs to get out there to the consumer, because clearly it is not. It would make all of our jobs a lot easier if it does.

ACTING CHAIR—Thank you for your evidence. If the committee has any further questions for you the committee secretariat will seek further comment from you at a later date.

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

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

Committee adjourned at 1.44 pm