



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

SELECT COMMITTEE ON INFORMATION TECHNOLOGIES

Reference: e-Privacy

MONDAY, 21 AUGUST 2000

CANBERRA

BY AUTHORITY OF THE SENATE

INTERNET

The Proof and Official Hansard transcripts of Senate committee hearings, some House of Representatives committee hearings and some joint committee hearings are available on the Internet. Some House of Representatives committees and some joint committees make available only Official Hansard transcripts.

The Internet address is: **<http://www.aph.gov.au/hansard>**

To search the parliamentary database, go to: **<http://search.aph.gov.au>**

SENATE
SELECT COMMITTEE ON INFORMATION TECHNOLOGIES

Monday, 21 August 2000

Members: Senator Ferris (*Chair*), Senator Bishop (*Deputy Chair*), Senators Calvert, Harradine, Lundy, McGauran, Stott Despoja and Tierney

Senators in attendance: Senators Calvert, Ferris, Harradine, Lundy, Stott Despoja and Tierney

Terms of reference:

To inquire into and report on:

- (a) the protection of consumer information obtained through electronic transactions, including browsing on the Internet and 'EFTPOS' transactions;
- (b) the privacy and disclosure obligations of organisations that have access to consumer databases; and
- (c) the access by consumers to personal information held in consumer databases.

WITNESSES

AITKEN, Dr Jane Stace, Assistant Director, Information Policy Section, Department of Health and Aged Care 60

AULICH, Mr Terrence Gordon, Managing Director, Aulich and Co.....39

CORONEOS, Mr Peter, Executive Director, Internet Industry Association28

DALE, Mr Thomas, General Manager Regulatory and Access, National Office for the Information Economy 16

DANIELS, Ms Helen Elizabeth, Assistant Secretary, Information Law Branch, Information and Security Law Division, Department of the Attorney-General..... 53

EARLE, Mr Terry Leo, Acting Chief Executive Officer and Business Development Director, Australian Retail Group..... 72

FERRY, Ms Jane Maree, Legal Counsel (Interim), Australian Medical Association 60

FIELD, Mr Tim, Chief General Manager Government Online, Office for Government Online..... 16

GLENN, Mr Richard Alexander, Acting Senior Legal Officer, Information Law Branch, Information and Security Law Division, Department of the Attorney-General..... 53

GRAHAM, Ms Irene Joy, Executive Director, Electronic Frontiers Australia Inc..... 1

HAGAN, Mr Philip John, Assistant Secretary, Information and Research Branch, Department of Health and Aged Care 60

MACKEY, Ms Gabrielle Mary, Acting Principal Legal Officer, Information Law Branch, Information and Security Law Division, Department of the Attorney-General..... 53

NESBITT, Ms Julia Margaret, Senior Policy Adviser, General Practice, Australian Medical Association..... 60

O’LOUGHLIN, Ms Nerida, Acting Chief General Manager, National Office for the Information Economy 16

POWER, Ms Prudence Howard, Director, General Practice, Australian Medical Association 60

PROBERT, Mr Andrew, Senior Consultant, SecureNet Ltd..... 39

QUINLAN, Mr Frank, National Coordinator, General Practice Computing Group 60

TREADWELL, Ms Jane Lesley, Chief Information Officer, Centrelink 16

WOOD, Ms Allison Maree, Acting Senior Legal Officer, Information Law Branch, Information and Security Law Division, Department of the Attorney-General..... 53

WOOLMER, Mr Luke, National Manager, Business and Information Protection, Centrelink..... 16

Committee met at 11.06 a.m.**GRAHAM, Ms Irene Joy, Executive Director, Electronic Frontiers Australia Inc.**

CHAIR—I declare open this public hearing of the Senate Select Committee on Information Technologies and express my regret that the Canberra fog meant that some committee members were unable to be with us for our scheduled 9 o'clock start this morning. I do apologise to those witnesses who have been inconvenienced by our two-hour delay in getting under way.

On behalf of the committee, I welcome all witnesses and members of the public attending this hearing today. This hearing is the first public hearing of the committee's inquiry into e-privacy. There will be a further hearing in Sydney tomorrow. On 25 March 1999, the Senate re-established the Senate Select Committee on Information Technologies to, in part, monitor the personal, social and economic impact of continuing technological change created by industries and services utilising information technologies. Given that consumer databases represent an emerging concern to the privacy of individuals, the committee resolved to inquire into e-privacy in Australia in order to examine the protection of consumer information obtained through electronic transactions, the privacy and disclosure obligations of organisations that have access to consumer databases and the access by consumers to personal information held in consumer databases.

Before we commence with our first witness this morning, the committee has received a further submission numbered 33 from the Australian Securities and Investment Commission. Is it the wish of the committee to receive the submission and authorise its publication? There being no objection, it is so ordered.

I welcome our first witness, Ms Irene Graham. We do appreciate your patience this morning. As you would know, having been a previous witness to this committee, we prefer all evidence to be given in public but you may at any time request that your evidence or even the answer to a question be given in private. Please make that request known to us and we shall consider it. However, I point out that any evidence taken in camera could subsequently be made public as a result of an order of the Senate. I remind witnesses that the giving of false or misleading evidence may constitute a contempt of the parliament. The committee has before it submission No. 23, which has already been published. Are there any alterations or additions that you would like to make?

Ms Graham—No.

CHAIR—I invite you to make an opening statement. At the conclusion of your remarks, my colleagues will have some questions for you.

Ms Graham—Thank you. As we have provided a very detailed written submission, I will not take too much of the committee's time with an opening statement. Firstly, we would like to say that we very much welcome this committee's interest in the matter of electronic privacy. EFA has a particular interest in privacy protection for Internet users and our comments therefore primarily focus on the online area. We recognise that electronic privacy issues pervade many other aspects of life and our online focus should not be taken to indicate a lack of concern about

privacy protection in other areas. Rather, our online focus is a reflection of EFA's charter which is primarily concerned with matters relating to the social political and civil liberties involved in the use of computer based communication systems.

The Internet is, of its very nature, a surveillance enabled technology. Unscrupulous organisations can and do exploit the technology to collect private information and consumer profiles without the knowledge or permission of the user. A number of technology facilitated privacy invasive practices have been described already in our submission. We are pleased that the federal government has introduced the [Privacy Amendment \(Private Sector\) Bill 2000](#). We support in principle the introduction of the core regulatory scheme to provide for the privacy protection of Australians in relation to the activities of the public and private sectors under Australian jurisdictions. Of course, it must be recognised that the Australian government can do little by way of statutory measures to protect consumers using the Internet from privacy invasive practices originating from jurisdictions outside Australia. There is a range of self-defence methods of varying effectiveness available to consumers but one of the problems is that many Internet users are unaware of the tools available. We believe the government should consider further high-level agreements between consumer protection bodies such as that signed in July between the ACCC and the US Federal Trade Commission.

Unfortunately, the EFA is unable to support the private sector bill in its current form because it contains too many exceptions and exemptions and fails to come to grips with the consumer privacy needs in the 21st century. The exception to the privacy principles in the bill in relation to direct marketing is contrary to international developments and effectively legitimises the practice of spamming on the Internet, that is, sending unsolicited email messages. The exemption for small business is unjustified and will introduce a confusing and complex regulatory environment that fails to protect consumers. The confusion that will result from this exemption will hamper attempts by Australian e-commerce vendors to attract customers from both within Australia and overseas.

Another major problem is the exemption for pre-existing data. We believe a transition period should be provided for existing data users to comply with the new legislation. Also, enforcement provisions in the bill at the present time are quite inadequate. Instead of empowering individuals to exercise their right to privacy of personal data, the bill confers on certain business interests the right to invade personal privacy.

We hope that in the course of this inquiry the committee will become fully aware of the inadequacies of the bill and, if you are not already, that you will then endeavour to include your report in the context of the Senate's consideration of the [Privacy Amendment \(Private Sector\) Bill 2000](#). That concludes my initial remarks.

CHAIR—Thank you. At the outset, would you elaborate on the objection that you have made in your submission to exemption for media organisations? What is it exactly that you are concerned about? I see that you are talking about their exemption meaning that they would have access to almost every web site. In another place, you say:

... in cases of complaint, 'media organisations' should be required to demonstrate that publication of personal information was in the public interest.

This committee has actually gone through that issue in a previous reference. I would be interested if you would comment on that.

Ms Graham—Our primary concern is not so much the exemption for the media because we are very much of the view that there needs to be freedom of speech for the media. Getting into restrictions on that becomes very problematic. The basic problem is that in the private sector bill at the moment the definition of journalists or media organisations—one or the other—is very broad. It could effectively mean virtually every Internet web site at the present time. We have a situation where, in the offline world, whereas the media is largely newspapers or television and to a certain extent you can rely on some level of ethics and so forth in what they are going to publish, with the Internet, as I am sure you are all aware, anybody can put up a web site and publish anything they like.

You get into a situation where the question arises: will individuals, small organisations or large organisations—whatever—be able to collect personal information, very privacy intrusive information, publish it and claim that this is part of journalism or that this is media? We see that the definition is too broad but, by the same token, we do not really see how you can narrow it without potentially interfering with legitimate media and journalistic activities. That is really why we have said in the submission—we also said the same thing to the House of Representatives committees—that we believe there needs to be a means by which, if there is gross invasion of privacy—and we are not talking about minor things—an individual can seek recourse.

We would basically see this as being something that should come within the ambit of the Privacy Commissioner so that there is at least an opportunity for recourse for someone who has really had their entire life—everything personal—published without their permission. There needs to be some sort of recourse if it is serious. I am not just saying this about minor things. At the moment there seems to be nothing at all that would enable an individual to do anything if everything were published on a web site somewhere.

CHAIR—You also talk about best practice in countries like New Zealand and Canada, and I think in Hong Kong and the UK.

Ms Graham—Yes.

CHAIR—How do you see our legislation falling short in that way?

Ms Graham—For a start, I have not read each of those pieces of legislation myself—various board members have read various ones. For example, in the Canadian privacy legislation, there is no exemption for media organisations, there is no exemption for political parties and there is no exemption for small business. There is an exemption for journalistic, artistic or literary purposes, but it seems to be somewhat narrower than the very broad thing that we have in ours. One of the major issues that we have at the moment with the existing proposed bill is the exemption for small business. To our knowledge, no other country in the world has proposed to or does, in their existing privacy legislation, exempt small business.

CHAIR—What about the use of cookies? Are they restricted in any of those countries?

Ms Graham—Not that we know of. It is still one of the very new technological issues. A lot of questions get raised and there are claims that they are not really privacy intrusive because a lot of people still believe you cannot link cookie information with an individual's identity. That is no longer true; you can. It is not always the case, but it can be done.

We mention in our submission that in America, for example, at least the federal government has limited the grounds on which government departments can use cookies. They have put out some quite strong wording in recent months about making sure that, if cookies are to be used, there is good reason. I do not think anyone has actually legislated against it, except to the extent that it could be tied with individuals' identities. Some of the existing privacy legislation may well cover it.

Senator LUNDY—In your submission in section 6 you talk about business self-regulation failures, in particular, the sale of databases between different entities. Could you extrapolate a little on legislation that exists in other jurisdictions that covers the sale of data to other entities? Could you also tell us of the terms and conditions under which that sale can take place, given that the sharing of information, by virtue of a sale or partial sale or the entering of a partnership, could be interpreted under some legislation as breaching the privacy conditions?

Ms Graham—Unfortunately, I am not able to answer that because I do not have the detail of any legislation that specifically does that. I am most familiar with the Canadian legislation. To my knowledge, it does not say it in so many words; it is more a case of defining what is personal information and then the legislation in general prevents the sale of it. My understanding is that the sanctions and things are through the Privacy Commissioner. In Canada the Privacy Commissioner has a much more independent role than seems to be the case in Australia. My understanding is that there are financial penalties, but I cannot be absolutely positive. One of the things we have been intending to do is write up some notes on the international legislation, but unfortunately, with a number of things that have been happening lately with inquiries and so forth, we have not quite managed to achieve everything that we would have wanted to achieve.

Senator LUNDY—That is fine. I am not aware of any that go specifically to partnering between companies for the purposes of sharing databases, thereby getting around some of those provisions about sale.

Ms Graham—The ones that we have mentioned in America seem to be under the FTC legislation, which seems to be more to do with deceptive trade practices and so forth. I think they are using the trade practices act there because, as you are probably aware, there is no actual privacy legislation in the United States—although it is starting to look as though it may yet happen.

Senator LUNDY—Are you familiar with the general direction of the safe harbour agreement between the United States and the European Union?

Ms Graham—Not the detail. The last I heard was that it was looking like it was going to go ahead. My understanding is that, unless it has only happened in the last week or so, I do not think the European Union has officially approved the safe harbour agreement yet. It keeps being said that, yes, it is more or less agreed, but as far as I know it has not been finally agreed. The

last time I looked at it—which was not in great depth—it did seem to have some protections in it that the existing proposed bill in Australia does not have. Without having all of that right in front of me, unfortunately I cannot give you the detail, but I am happy to get back to you with it, if you would like.

Senator LUNDY—Yes. Other witnesses might be able to fill us in in more detail there. You mentioned digital signatures, particularly with respect to the ABN database. You cite in your submission concerns which have been expressed and say that the ABN-DSC scheme has similarly failed so far to identify the potential privacy problems. What do you see as the major problems with that particular database as it is currently being developed?

Ms Graham—Did you say the database or the digital signature?

Senator LUNDY—The actual scheme, but in association with the ABN database.

Ms Graham—To me, they are two separate issues. One is the actual storage of data and the fact that it seems to be being sold. It is unclear to us at the moment. One person says that it is not going to be sold any more and then the next person says that it is. It is not quite clear what is happening with the data. One of the issues with the digital signature side of it is that, as far as we have been able to identify, it is unclear what methods are being used to generate the digital signatures and what security there is behind all of that. It seems we have a situation where people are downloading digital signatures that have been created for them by somebody else, and this is supposed to identify them. It is not really clear whether there are backup copies of those signatures being kept. For example, effectively it is someone saying, ‘I will write your signature here and I will give it to you. Then that is your signature. That proves that that is you.’ But if they wrote the signature in the first place, presumably they would have a copy of it. There are these kinds of issues when you start looking at digital signatures identifying people and, so to speak, protecting them—it is not really privacy; it is to identify them so that no-one else can pretend to be them. If you do not know how the keys are being created and what the security issues are, how can you say that it is actually them?

I understand that these particular keys are going to become more widely used than they are at the moment. There is some scheme coming forward in the next 12 months. I believe that it is potentially going to lead to these keys being used business to business. I am not sure of the minute detail. It is not perhaps these keys so much as the design, that the process being used to create the keys is expected to get wider use. Basically we are concerned that there does not seem to have been enough attention, or there may have been enough attention but from the public’s point of view it is completely unclear what kind of security has been put in place to ensure that, when the keys supposedly belong to somebody, they actually do. I am not saying that there is anything wrong with it; please do not get me wrong. It is just that it appears that there could be because there is not sufficient information put out to assure the public that everything is as it ought to be.

Senator LUNDY—I will be able to pursue that with government departments a little later today. I have a general question about the role of encryption in protecting privacy. Obviously, there have been continued discussions about and changes to the laws around the world relating to encryption. We have seen somewhat of a relaxation in those requirements in some jurisdictions. Can you give the committee an overview of the role of encryption in protecting

people's privacy, both in an institutionalised form—that is, in the databases that are managed—and also from an individual's perspective in their electronic communications?

Ms Graham—Certainly. There are probably two main aspects that encryption gets used for or thought of at the moment. One is for protecting the privacy of, for example, email communications. There have been strong cryptographic packages for a number of years which ordinary individuals can put on their own computer and then create their own keys so that you can scramble a message before they send it to somebody, and the only person who can read it is the person to whom it has been sent. It is very difficult to explain in detail. Effectively, you can encrypt a message so that only two people can open it—the person you are sending it to and the person who has sent it. Cryptography is good for protecting email messages, but it only works if both the sender and the recipient know each other and have each other's keys.

The other way it is used quite a lot is in electronic commerce in transferring data across the World Wide Web. Most of the browsers now have encryption built into them, such as Netscape and Microsoft Internet Explorer. Until very recently though, one of the major problems with electronic commerce and using the web in this way has been that, because of the United States restrictions on export of cryptography, the encryption has been very weak. For example, in America, Netscape was able to sell or distribute their product that had strong encryption in it but, when the copies of Netscape were issued or distributed outside America, they were weakened. I think it went from what they call 128 bits down to 40. A 40-bit encryption was broken into years ago. So that has been relaxed or changed this year and now exported software from America can have a higher encryption strength.

There is still a general government attitude throughout the world that there needs to be controls kept on the strength of encryption because criminals might use it. This is affecting electronic commerce because of consumer concerns about sending credit card numbers and so forth over the Internet—if you do not have strong encryption, your credit card can be intercepted. On the other hand, the very strong encryption packages have been available to any individual in the world who has wanted to get hold of them for years and years. So the whole aim of trying to restrict cryptography which interferes with e-commerce seems to be somewhat pointless because the encryption software is out there.

Senator LUNDY—A further point on encryption specifically in its role in electronic privacy: can you identify any specific changes in Australian law which would enable the wider use of products that can encrypt and decrypt digital content in Australian law? Is there pressure out there to make that change to Australian law? I understand also that it is not just legislation we are talking about but some international agreements which could be preventing the use of high-level encryption in commercial applications and private applications.

Ms Graham—My understanding is that there is no written down Australian law that controls the strength of encryption technologies that can be used or exported from Australia. EFA has tried over a number of years to get to the bottom of the Australian government's policy on the use of encryption. Basically, my understanding is that it is all tied up in Defence Signals Directorate. Trying to get any information as to what the rules are is very difficult. If you go to some of the software vendors who are involved in products that need to use encryption, many of them will not talk to you about what they are allowed to do or not allowed to do because, once again, we get into the issue of national security. Defence Signals Directorate does not seem to

want anybody to know exactly what is allowed. So I cannot tell you exactly what the situation is. From all inquiries, we believe that Australia basically follows along the line of whatever the American government says, but that it is not written down in Australian law.

You may recall the hue and cry a couple of years ago over the Walsh report, which the government tried to suppress. EFA managed to get that under FOI and then, by sheer luck, found the rest of it in a library. The whole point of that exercise was supposed to be to try to find out what the government were proposing to do about cryptography or why they had their existing policy. It seems that intelligence agencies keep all information very close to their chest.

You also asked about international agreements. There is the Wassenaar agreement, which is an international agreement. The last time this committee met in Vienna, basically America tried to restrict relaxation on cryptographic controls. For example, Ireland have a very open policy. They have virtually no restrictions on it. I think Germany is one of the others that does not have as much restriction on the level of cryptographic protocols that can be used. What seems to happen is that America comes along and demands that the restrictions should remain. Then Australia follows that. My understanding at the moment—I would have to look for the minute details of this because it is a very complex area—is that the last time the Wassenaar agreement got changed, which is only about six months ago, there were some aspects of it relaxed, but we do not think Australia has followed that because America has not. Really the whole encryption policy in Australia needs to be opened up to public debate and, whatever the departments are doing, the public ought to know about it. There should be an opportunity to discuss whether the policy is right or wrong.

Senator LUNDY—If a company embarking on some sort of digital endeavour—it might be a commercial offering, it might be a service—had in their product a level of encryption, where do they turn to find out under what conditions they can deliver their product and deploy some sort of crypto within their product?

Ms Graham—I would suggest that you ask the Attorney-General's Department this afternoon. My understanding is that, if it is going to be sold only within Australia, I think they do not have to get any permission. But if it is going to go out of Australia, they have to get customs export approval, and I understand they get that from the Department of Defence Signals Directorate. There is some highly complex procedure where they end up getting approval. My understanding is that it comes under the Attorney-General's Department. I wish you luck in trying to find out the details.

Senator CALVERT—You are quite critical of the legislation in respect of the fact that there are a large number of exemptions, particularly small business and political parties. You are also critical of the fact that an adequate complaints mechanism is needed. If those two areas were amended or changed to reflect a stronger point of view, would that go a long way to satisfying you?

Ms Graham—There are a number of areas obviously involved with the legislation that we have some concerns about.

Senator CALVERT—Do you see those as major areas though?

Ms Graham—For us, the major ones are the small business exemption and what appears to be the lack of enforcement provisions. I am not sure whether we have said a great deal about enforcement provisions in this particular submission, but to the House of Representatives committee we did comment that we find the way the current bill is written is very confusing. It is very hard to come to grips with what, if any, enforcement provisions are in it. To us, there seems to be virtually none. The Privacy Commissioner does not seem to have very much power at all and there do not really seem to be any sanctions. Again, we are not saying there is absolutely none, but we cannot identify them. We think, if you are to have legislation that purports to protect consumers, that they ought to understand it. We do not see anything there.

With small business there are two primary problems. One is the fact that the vast majority of Australian businesses will fall under the \$3 million arbitrary line that has been drawn, but it is also the exemption for small business operators which effectively allows organisations to subdivide themselves into numerous small businesses and then they can virtually completely escape the privacy laws. So you could effectively have a company turning over \$10 million or \$20 million; it could subdivide and be an operator of several small businesses. Then they can collect, use, sell and do all sorts of things with the data. We really feel that the small business exemption is creating a massive loophole. I do not know whether it was realised that it could be used like this when the legislation was drawn up; perhaps it was not. Certainly the small business operator aspect creates a very large hole.

Senator CALVERT—I am interested to note in your submission that you talk about bogus political parties being formed by commercial marketing interests.

Ms Graham—There have been all sorts of things suggested. The thing is that businesses really do want to deal in personal data. There is a massive market for it. If the government brings in strong privacy legislation protecting personal data and businesses still want to do things that the legislation says they cannot, then obviously they will look for any loophole that they can possibly find to go on doing it. One of the suggestions that was put to us was that creating bogus political parties could be one way to get around the legislation. That is not meant to be a criticism of legitimate political parties, legitimate politicians; it was just any way to get around legislation.

Senator CALVERT—Do you have evidence of political parties having amassed large amounts of personal data that could be used?

Ms Graham—No.

Senator CALVERT—Or do you put that in the same category as you do bogus political parties?

Ms Graham—One of the concerns that arose recently was something to do with the sale of the electoral roll. It seems that the electoral roll is being distributed around in a completely different way from the way I and most of EFA's people and a lot of other privacy advocates knew. I understand that it is being distributed in electronic format or something and I am not entirely sure that that was originally intended by the electoral legislation. I just cannot remember the minute detail. But we are not saying that political parties are using any data incorrectly. What we are saying is: why does there need to be an exemption for political parties?

If there are reasons for exemptions for political parties, then can we hear them, please? I am not asking this committee to tell us. If there is a legitimate need, if the public is made aware of this it might completely change our view. At the moment, the only reason we could see for an exemption is the potential for one political party to attack another political party in the middle of an election or something. We could see that there could be potential for claiming rivalry between parties but that kind of thing could be addressed by delaying any investigation by the Privacy Commissioner during the period of an election or whatever. We do not understand why there needs to be an exemption for political parties, unless some political parties are planning to use data without the permission of the owners of the data.

CHAIR—Do you think the general community understands the implications of e-commerce in terms of privacy?

Ms Graham—No, absolutely not.

CHAIR—Whose responsibility do you think it is to make sure that they do understand? Is it the companies themselves or is it government?

Ms Graham—I really think it has to come down to a combination of everybody. There are certainly some very responsible businesses around that have had privacy policies in place for a very long time and really do understand the issues. Those sorts of companies are obviously doing what they can to draw customers' attention to the issues. But it is very difficult to try and expect businesses which want to be in the business of infringing privacy to educate the public about what the problems are. At the end of the day, I really think there needs to be a greater role somewhere within the government. I think we did suggest that perhaps the ACCC, for example, might become more involved in this area because, whilst they are involved with fraud and Trade Practices Act and everything, some of that also comes very close to some of the issues about privacy—in that companies issue privacy policies that say, 'We will do this and we will do that,' and then they proceed to do something entirely different.

CHAIR—So you do not think a code of practice would be strong enough?

Ms Graham—A code of practice for?

CHAIR—If the industry itself came up with a code of practice and said, 'We will self regulate'—

Ms Graham—No. It definitely has to be co-regulatory. There have to be sanctions of some sort. One of the interesting aspects of all of these codes of practice for the industry is that you will hear from ADMA, the Australian Direct Marketing Association, that they have a code of practice and it has been approved by the ACCC and all of the rest of it. But have you ever asked a junk marketing person telephoning you whether they are a member of ADMA? They will say 'Who?' What is the use of a code of practice if the people—

CHAIR—Try asking them where they got your name from.

Ms Graham—Yes.

Senator STOTT DESPOJA—Ms Graham, thank you for your submission. You have pre-exempted most of my questions in relation to the bill. But on that note, there will be a Senate inquiry into that legislation, albeit a brief one, even if it is not to the pleasing of the two old parties. I have two questions on your privacy bill comments. Have you estimated the quantity of the exemption in relation to small business? You said that presumably a majority of small businesses would be exempt. Would you say 80 per cent? Have you calculated a figure?

Ms Graham—I think it was even more than that. There were figures put out by the Attorney-General's Department. It might have been in their submission to the House of Representatives committee. But my recollection is that it was more like 95 per cent. I would need to look that up, but I am sure that they have said that somewhere. It was either in the explanatory memorandum to the bill or it was in a submission to the House.

Senator STOTT DESPOJA—In relation to that particular exemption, you have recommended that it should be abolished. You are not offering in its place a cut-off figure or a certain number of employees?

Ms Graham—No. We see absolutely no benefit whatsoever to exempting small business. We think to exempt small business will actually create a disadvantage to small businesses which wish to come within the legislation and wish to be able to assure consumers that they do care about their privacy. The way the bill is drafted at the moment, even if a small business wishes to be regulated and wishes to be able to say, 'If we do the wrong thing by you, you can have recourse through the code or through the Privacy Commissioner' or whatever, they cannot even do that under the bill because they are just completely exempt.

Someone suggested to us recently that the only way a small business could bring themselves under the legislation would be to purposely start selling personal data so that that would then exempt them from the exemption. That seems a rather privacy-intrusive way to go about enabling a small business which wants to do the right thing to do so within the legislation.

Senator STOTT DESPOJA—I was going to ask you if you had heard some arguments as to why there was an exemption for political parties, but obviously you have not been furnished with those.

Ms Graham—No.

Senator STOTT DESPOJA—Nor have we. I put it to you that, apart from the rationale that you have given for that exemption being abolished, it seems a bit strange that people should be expected to have faith in a regulatory system implemented by politicians that politicians are not prepared to adhere to themselves.

Ms Graham—Exactly. One of the major questions that arises out of it is: if politicians are not willing to comply with it, how on earth can anybody else be expected to?

Senator STOTT DESPOJA—How widespread do you think the surreptitious collection of personal data online is?

Ms Graham—It is really hard to tell. I suspect that, in terms of Australian businesses at this stage, it is not too great largely because there is not too much business of this type. Australia is very young in the e-commerce world. Overseas, particularly around America, there seems to be quite a deal. A lot of the marketing companies are based initially in America. You have DoubleClick, Engage Technologies, and Acxiom that we all heard about here a few months ago. A lot of them are American based. There is more e-commerce in America at this stage than in Australia. It is probably fairly widespread. If you go looking on the web sites of these marketers, not so much just on their web sites but on areas where they talk about wanting partners to join with them, the amount of data they claim to have collected is huge. They are talking about millions and millions—70 million or 120 million profiles and things. It is probably far more widespread than anybody knows but unless you are in the business you have no way of knowing what they have collected.

Senator STOTT DESPOJA—You talk about the inadequacy of current Australian laws in relation to a company changing its policy on privacy and you use the Toysmart.com and DoubleClick example. I respect and understand that conclusion. More generally, are you suggesting that current laws are inadequate in relation to protecting information online?

Ms Graham—I am sure they are. There is no privacy law in Australia at all at the moment that covers the private sector. If something like that happened in Australia, I would say at the best maybe something could be done about it within the Trade Practices Act, which is largely what has happened in America over Toysmart.com. But there should be privacy legislation that creates a situation where, when a company promises they will never share your data with a third party, that should be the end of it. That is really why we see the need for privacy legislation, not reliance on some vague clause that might be tucked away somewhere in the Trade Practices Act. You want clear rules that say, ‘If you say you are not going to give out data without permission, then you do not; and if you do, there are sanctions.’ That is how we see it.

Senator STOTT DESPOJA—Do you see the bill that purports to extend privacy laws to the private sector as still inadequate to deal with these issues?

Ms Graham—Absolutely. Again, one of the biggest areas is small business because for a long time Australian e-commerce sites are going to be small business. If defined as \$3 million, I think that they will basically all be exempt. I do not see that it solves anything.

We are very aware that anything the Australian government does is not going to solve the problem with Australians using overseas sites. But one of the things that the government can do in terms of encouraging e-commerce in Australia is to have strong privacy laws applying to Australian companies. We believe that there is such concern about privacy within the public that if there were strong privacy laws that would encourage Australians to use Australian businesses rather than saying, ‘We might as well go to Europe where we have got the EU data protection legislation and at least we know if we use an European company our data is protected.’ Although we cannot control within Australia what happens overseas, we can certainly put in place a situation where if Australians deal with Australians they are protected.

Senator STOTT DESPOJA—You allude to CrimeNet in your submission. I wonder whether you are willing to put on record your views of CrimeNet.

Ms Graham—I do not know whether we have actually put them on record. I think we might have commented in the media. Basically our position is that, rather than trying to close that site down, it would be better to regulate and have clear laws about what can be provided. We believe that a lot of that information that is on that site could be tracked down through the Austlii law site, through the normal court reporting things. We have since been heard in the media that the Victorian government sells criminal records, et cetera. We feel that trying to just close the site down will be counterproductive because, I would say, they will sell the data overseas. I cannot be positive but it seems very likely that they will sell it to an overseas organisation which will put it on an American web site where it is protected by the First Amendment and the data will still be there. So it will be better to keep it in Australia and regulate what is allowed to be on the site and what is not, in terms of during a trial or whatever legislation the Attorney-General's might feel is appropriate. It would be better to at least set out a set of rules about what can and cannot be on the site and regulate it in Australia rather than push it overseas.

Senator HARRADINE—In this major area of public policy, on balance, would you say that the public interest is being subordinated to the commercial interests of business or other interests of media or even politicians?

Ms Graham—With this particular bill at the moment, it appears that that could be the case. It certainly looks like there are too many loopholes there and that the consumer interest is not the first priority.

Senator HARRADINE—Just for the record: in regard to the membership of EFA, is an organisation named the Eros Foundation a member of your organisation?

Ms Graham—EFA does not disclose its members. We believe that that is their private business.

Senator HARRADINE—Really?

Ms Graham—We do not disclose who our members are. Our members join the organisation. They all join because of an altruistic interest in the issues that EFA is involved with and we do not disclose our members' list to anybody. We do not say whether an organisation or an individual is a member or is not a member.

Senator HARRADINE—You say, 'is independent of government and commerce and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties'. They are your words.

Ms Graham—Yes, that is right.

Senator HARRADINE—On that basis then, can I assume that they are not members?

Ms Graham—I am sorry, but I do not believe it is relevant to this inquiry who EFA's members are and, as I said, we promise our members when they join that their membership is private. So we prefer not to say whether any individual organisation is or is not a member. We simply do not disclose who our members are. I do not understand why it is relevant to a privacy commission.

Senator HARRADINE—Can I say why?

Ms Graham—Yes, certainly.

Senator HARRADINE—In respect of your submission, you have just agreed to the proposition that the public interests are most likely being subordinated to the commercial interests of business in this particular area.

Ms Graham—In the area of privacy legislation, yes.

Senator HARRADINE—Yes; but I go to your organisation's going to bat for the hard-core porn industry—Eros's industry.

Ms Graham—EFA does not go to bat for the hard core porn industry. EFA believes that individuals should have the right to read, see and hear what they want. We also believe that they should have the right to privacy in their own homes and privacy of their personal data. We do not go to bat for any industry. We are not part of the pornography industry.

Senator HARRADINE—So you are quite happy to see hard core porn go across the Internet and be read and accessed by young people, without any protection at all. What about their protection?

Ms Graham—Senator, the Australian government cannot do anything about protecting children on the global Internet, as can be seen by the legislation that has been introduced in Australia. It has made absolutely no difference to the amount of pornography on the Internet. Internet service providers are now required to provide, under the Broadcasting Services Act, filtering software to anybody who wants it and some do free of charge. The best thing that parents can do to protect their children is to either supervise their access or use filtering software. I am afraid legislation introduced by national governments is not going to protect children. It simply creates a false sense of security. Parents who do not understand the Internet are left with the impression that it has been fixed. The problem has not been fixed. EFA finds that very concerning.

Senator HARRADINE—Yes, the problem has not been fixed. It certainly was not helped by your organisation in its going to bat for the Eros Foundation.

Senator LUNDY—I am not convinced that this is completely relevant to the issue at hand.

CHAIR—Are you taking a point of order, Senator Lundy?

Senator LUNDY—Yes, I am taking a point of order.

CHAIR—What is your point of order?

Senator LUNDY—That these questions are not relevant to the inquiry currently before us.

CHAIR—Senator Harradine, perhaps you could direct your questions to the terms of reference, following the question that you have started to ask.

Senator HARRADINE—Thank you very much. We are talking about matters of public interest in the area of privacy and the importance that those public interests, including the rights of children, should not be subordinated to the commercial interests such as those of perhaps a member of your organisation. That is where it comes in.

Ms Graham—I am sorry, Senator, I do not understand the question. I would appreciate it if you would rephrase it.

Senator HARRADINE—I am asking you: because you have agreed that the public interest is being subordinated to the commercial interests of business and that problem has not been adequately covered by the legislation—

Ms Graham—Senator, I think the privacy legislation—

Senator HARRADINE—May I just finish my question?

CHAIR—Just a moment, Ms Graham. Senator Harradine, have you finished your question?

Senator HARRADINE—No. I have been asked to explain the situation. I am explaining it to the witness. I am raising the question about the matters that you have referred to: that is to say that the legislation obviously has not fixed the problem, but there is a very important problem and a very important issue there. Do you not see the issue of the rights of persons—adults and young people, particularly young people—to privacy in their own home and not being subjected to the interests of the porn industry to invade that privacy by various means, including the use of web sites which have slightly different wording from very reputable sites? What about that area of privacy?

Ms Graham—Senator, I think you and EFA see the situation with Internet access quite differently. We see the Broadcasting Services Act as interfering in the rights of adults to control what they and their children see on the Internet in the privacy of their own homes. I accept that you see this from a different point of view and you believe the Internet should be restricted. I am sorry; we will not come to any agreement about that because we see the existing legislation as an infringement of adults' rights and adults' privacy in their own home. We believe the government has done all it can in terms of protecting people on the Internet from unsuitable material. We do not believe that the current privacy legislation before this committee is adequate to protect privacy. We are saying that we think the government have done all they can do on the censorship front but we do not think the government have done all they can on the privacy front.

Senator HARRADINE—So you do not think that there is an attack by the porn industry and other industries involved in violent material on the rights of families to their own privacy in their own home by dint of using web page names which are almost identical to the names of others which are quite reputable, therefore ensnaring young people into accessing those web sites?

Ms Graham—I think you might now be talking about a practice known as ‘mouse-trapping’, which EFA has never, ever supported. We do not support things like fraudulent, misleading conduct, et cetera. What you are talking about now is really completely another issue.

Senator HARRADINE—How can we overcome that problem?

Ms Graham—My understanding of the instance that occurred some six months or so ago about which there was a lot of publicity in Australia is that the ACCC and the FTC in America have signed an agreement and they investigated that matter together. There was international cooperation—which was a wonderful thing—and they got to the bottom of it. I am not quite sure what the police ended up doing about it, but it was a matter for the police. My understanding was that the Australian authorities and the American authorities worked together. Certainly, there was a press release put out by the FTC about this. My understanding is that the problem was resolved and is already resolvable under existing law relating to trade practices, fraudulent practice, et cetera. So the fact that those sites were actually pornographic sites is largely irrelevant. The issue is taking somebody else’s name and using it. As I say, my understanding is that that is already covered under the Trade Practices Act in both Australia and overseas.

CHAIR—Senator Harradine, we are 20 minutes over time so perhaps this can be a short question.

Senator HARRADINE—I will not ask anything more of this witness.

CHAIR—Are you sure?

Senator HARRADINE—I will just follow it up.

CHAIR—Thank you very much, Ms Graham. We do appreciate that you waited for several hours this morning to give your evidence.

Ms Graham—That is fine. Thanks very much for listening to us.

[12.05 p.m.]

DALE, Mr Thomas, General Manager Regulatory and Access, National Office for the Information Economy

O'LOUGHLIN, Ms Nerida, Acting Chief General Manager, National Office for the Information Economy

TREADWELL, Ms Jane Lesley, Chief Information Officer, Centrelink

WOOLMER, Mr Luke, National Manager, Business and Information Protection, Centrelink

FIELD, Mr Tim, Chief General Manager Government Online, Office for Government Online

CHAIR—I now welcome the panel who comprise our next two witness groups, Ms Jane Treadwell and Mr Luke Woolmer from Centrelink, Ms Nerida O'Loughlin and Mr Tom Dale from the National Office for the Information Economy and Mr Tim Field from the Office for Government Online. I am sure each of you as senior officers knows that we do prefer all information to be given in public. If at any time any member of the committee asks you a question which you would prefer to answer in private, please indicate that and we will take it into account. However, it subsequently could be made public by an order of the Senate. I also remind you, of course, that giving false or misleading information may constitute contempt of the parliament—not that I imagine I need to draw that to your attention. The committee has before it submission No. 14 from Centrelink and submission No. 27 from NOIE, which have already been published. Are there any alterations that you wanted to make to your submissions at this stage?

Ms Treadwell—No.

CHAIR—I now invite you to make an opening statement and at the conclusion of that we shall have some questions. Given Mr Dale's voice, perhaps another member of the Office for the Information Economy might like to make the presentation.

Ms O'Loughlin—Our submission has outlined in detail the range of measures that have been put in place or can be put in place by government, individual consumers and industry. I do not think we wanted to go much further than that. To clarify roles, obviously the Attorney-General has responsibility for the privacy legislation, the National Office for the Information Economy has a strong interest and provides advice in this area, particularly as it relates to encouraging greater uptake of e-commerce, and our colleagues in the Office for Government Online have responsibilities in terms of the activities of government departments.

Ms Treadwell—Centrelink is very pleased to be able to be here today to participate in these proceedings. Centrelink is very aware of its responsibilities in handling data on millions of our customers and safeguards the privacy aspects of those transactions and of the individuals by

imposing rigorous security controls and privacy standards within our organisation. In order to protect the privacy rights of individuals, we have in place strict policies, protocols and processes that we enforce. The development of e-commerce, e-business and open electronic architectures between organisations, governments and individuals has created wonderful opportunities for speeding up and transforming the experiences of citizens and organisations. Equally, it has created serious implications in terms of the protection of individual data. As such, Centrelink is approaching these opportunities with extreme caution. I understand that we are invited to these proceedings to outline our practices and policies, and welcome any questions in regard to them.

CHAIR—Probably your agency is the one which is regarded as being crucial to the privacy of more than six million Australians. It might be useful for the committee if you could outline the principal processes that you implement to ensure the privacy of those individuals. Could you comment on the use of cookies and tell us a little about how you go about ensuring that people are not able to access your database.

Ms Treadwell—I will start very generally and then hand over to Luke Woolmer. In regard to Internet interactivity, we have a very basic Internet site. As I mentioned before, our approach to interactions of an electronic nature across the Internet is very basic. We do not enable access by our customers to data in a general sense. In that regard, the use of cookies is fairly immature in terms of our use. We have had two pilots and, in them, essentially the use of cookies has not been actually to collect any data on the individuals themselves; it has been more to continue to keep track of the session to ensure that the person who is connected is that person. On the more general approach to privacy controls, I will hand over to Luke.

CHAIR—Mr Woolmer, could you just indicate to us whether there has ever been an attempt to hack into your database and, if so, how you managed that? Are there any public reporting requirements if such an attempt were to be made? Could you cover those questions in your response.

Mr Woolmer—In terms of intrusion, we would call it detection and intrusion. In terms of people ‘hacking’ into our databases, to the best of our knowledge there has never been a successful attack. To the best of our knowledge, most attempts are just one-offs trying to breach the firewall. Nothing has ever gotten through. We test those things on a regular basis from a risk point of view, using outside agencies and the private sector accounting firms—the big six accounting firms and such—just to try to see if they can penetrate. They have not been successful in the past. Recently, we did one in December and it was certainly not successful in any way, shape or form.

Just finishing off the point on the use of cookies, we as an organisation have, as the CIO alluded to, two small projects where we have used cookies, but only for the authentication or the tracking of where a person is on our site. We make it very clear that we do not retain any personal information whatsoever on the individual. We do it in accordance with the Attorney-General’s published guidelines, which are on their web site, on the use of cookies by government agencies. As my techos explained to me, there are some very good reasons to use cookies from a design and architectural sense—from a computing sense—but we are very cognisant of the privacy aspects of that and make sure we do not collect any information at all. In both of those two small pilots, we advised the individuals that we actually do use cookies in

there but we only use if they are still online basically. If they are not online in any sense, after 20 minutes if there has been no interaction they will be logged out immediately. That is about it.

Senator LUNDY—As a government agency, you work to the provisions of the Privacy Act 1988; is that right?

Ms Treadwell—That is right.

Senator LUNDY—In terms of your relationships and your dealings with private sector entities in the delivery of your service, what mechanism do you use to transfer, if at all, the laws that exist under the Privacy Act to those who provide services on behalf of Centrelink?

Ms Treadwell—They are required to observe the same provisions as we are under that act.

Senator LUNDY—How do you enforce that as an agency?

Ms Treadwell—If it is a contract, they are required to sign off on the same provisions as part of the contractual requirements. If they are a member of staff or a contractor, they are required to complete a deed of confidentiality, again complying with those requirements.

Senator LUNDY—In the actual body of the contract, how is that clause structured that binds those private sector providers to the provisions of the Privacy Act 1988?

Ms Treadwell—I will have to take that on notice and provide that information to you in terms of the specifics of our requirements under our contract.

Senator LUNDY—It is certainly an issue now, with respect to a range of private providers that you access. In the light of the forthcoming IT outsourcing for the Centrelink agency, it also is a significant concern. Can you tell the committee what your considerations are to date about sustaining the privacy standards that you as an agency currently have, once you outsource your information technology?

Ms Treadwell—Generally, Centrelink will continue to be responsible for the privacy, and the protocols and arrangements that will safeguard customer privacy. The details are contained within the statement of work and the contract itself.

Mr Woolmer—I will expand a little. When it was preparing for outsourcing, Centrelink made a conscious decision not to outsource the security arrangements. We believe that privacy problems basically manifest themselves as a breach of a process or breach of a security arrangement. We have determined that we shall not outsource the individual security arrangements themselves. Things such as access to the information, access control, authentication, the integrity of the data, the certification of the user are all still being done inside Centrelink, even in an outsourced or potentially outsourced environment. We will set the policies; we will set the standards of access; we will also set the monitoring and the tracing to see who has been into which data sets and for what purposes.

Senator LUNDY—Have you done that because of the lack of legislation in the private sector in relation to privacy?

Ms Treadwell—No; that would be essentially because we consider it to be a Centrelink responsibility. Any outsourcing arrangement does not change the core nature of Centrelink responsibility in terms of protecting the data of our customers.

Senator LUNDY—If it is at all possible, could you provide the committee with the clauses of the contract. I know there are lots of issues; government is keen to claim on commercial-in-confidence. If you could provide as much detail as you can about the way you have structured that privacy regime in the context of IT outsourcing, that would be useful.

Ms Treadwell—Certainly we can provide the underpinning requirements we have. The nature of the contract itself will change in the course of negotiations, I imagine. But certainly we can provide to the committee our requirements of such a contractor.

Senator LUNDY—In terms of the delivery of services in an online environment, you mentioned before that your web site is not currently established to allow any client access to your database for the purposes of facilitating claims or an exchange; is that the case?

Ms Treadwell—In general, that is the case. Essentially, our web site is informational. Whilst there is the ability to email the web master, it is fairly non-interactive. This is essentially because security and privacy are the key issues that we have to be very confident about before we open our databases up. In that regard, we are still constructing that mechanism.

Senator LUNDY—But you intend to move towards a higher level of interactivity, where clients can actually access their own information?

Ms Treadwell—Certainly, we do have the intention to actually provide customer self-servicing. It is in their interests as well as that of the organisation to provide them with the opportunity to provide information to us. That offers an ease of access and convenience for them. Equally, it would be in their interests for them to be able to assess or find out what information we currently hold. The most common type of inquiry relates to what the nature of their last payment was. From our perspective, being able to have the most recent, up-to-date information on their address and other circumstances then enables us to provide a much better service both to government and to those citizens.

We have had a number of pilots. One was relating to call centre automation where people have been able to find out through the equivalent of a telephone banking service how much their recent payment was. We would hope that we would be able to roll that out for all of our customers as and when we are confident of the security and privacy arrangements.

Senator LUNDY—Will that be part of the IT outsourcing contract?

Ms Treadwell—No.

Senator LUNDY—You have kept it separate?

Ms Treadwell—The outsourcing contract deals with business as it currently is. Any developments come on as ‘projects’.

Senator LUNDY—I appreciate this is a bit of speculation. It might link to other areas of other departments. It relates to public key inscription. Are you looking at providing a digital signature to clients of Centrelink as part of where you are going with a higher level of interactive service?

Ms Treadwell—Certainly we are exploring how public key technologies can be applied within Centrelink and we are working with the Office for Government Online in order that that can be done.

Senator LUNDY—Can you give a brief overview as to the current state of the federal government’s public key project?

Mr Field—We have this framework in place, as you know—the Gatekeeper framework. The Taxation Office has done its implementation of public key infrastructure as part of the new tax collection arrangements, which you are aware of—

Senator LUNDY—I have some questions about that but I will come to that.

Mr Field—That has basically been rolled out over the past couple of months. There are a number of agencies which are looking at these issues and use of this technology and approach. But no-one has got to the point of actually rolling out—implementing. The tax office has done it and a range of other agencies are—

Senator LUNDY—Those who have applied for an ABN?

Mr Field—Yes, the tax office is using it for people to put in their business activity statements online.

Senator LUNDY—So there is no other roll-out having taken place as yet?

Mr Field—No. A number of agencies, such as Centrelink, Customs and the Health Insurance Commission, are looking at this—as you would expect them to, given the imperative of getting online.

Senator LUNDY—We had some comments earlier from a witness from the Electronic Frontiers association on public keys. Can you describe for the committee the actual process of creating those public keys and what privacy protections are in place at that point of generation of that public key?

Mr Field—The Gatekeeper framework has a whole list of criteria. Ultimately, those who generate key material and issue digital signatures, and really anyone taking part in that whole process, are covered by them. Physical security—just whether the buildings in which this happens are secure—and staff vetting, the policy frameworks around the actual issue of keys and certificates, and the software that is used are all covered by a whole set of criteria. The

relevant one here is the Privacy Act and the privacy guidelines. A rigorous part of the Gatekeeper evaluation, both before and after actual implementation, is conformance with the privacy principles. To get the Gatekeeper tick, basically, you have been audited right through that process.

Senator LUNDY—Do you engage private providers to provide that technology to you? How is it managed from within the Office for Government Online?

Mr Field—Gatekeeper is a framework that brings together a range of people who do the actual assessment, like Defence Signals Directorate; they have a process where they have contracted to a number of auditors to look at the suitability of certain arrangements.

Senator LUNDY—Do you have a direct relationship with Defence Signals Directorate?

Mr Field—Yes, they do the main part of the security aspects.

Senator LUNDY—Who issues the digital signatures—you or them?

Mr Field—Ultimately, a provider. If I am Centrelink and I want digital signatures issued to my customers, I will engage a certificate authority to do that. Under the Commonwealth's framework, the certificate authority and all those involved in that process—the companies that specialise in that—have to be Gatekeeper accredited.

CHAIR—Senator Lundy, we will try to come back to you. I am just conscious of other people's opportunities to ask questions.

Senator CALVERT—Ms Treadwell said earlier that Centrelink has in place protocols and processes to protect privacy. You probably maintain some of the largest amounts of information that are available and you bring in data matched information from other areas. What sorts of processes do you have in place to protect information that may belong to other departments? Do you have programs where you instruct your staff or teach your staff to protect privacy? What sort of protection measures do you have in place for that? Would you like to comment, too, about the little mistake that was made this week—about the 800,000 numbers on the outside of envelopes? How did that happen?

Ms Treadwell—I will deal with the last one first. It is of enormous regret that this has happened. We have an investigation under way to work out what went wrong. We are aware that, essentially, it is a failure of internal checking—of those procedures and protocols that we have in place that will guarantee privacy. Essentially, what happened was that the mailing list had customer reference numbers on it and unfortunately that was produced on the labels that covered the envelope enclosing a disability magazine that went to over 800,000 Australians. On the basis of the initial understanding of what went wrong, we determined that there was minimal risk in terms of the misuse of that number. We are aware that, as of this week, that information went to the hands of the people who knew their reference number. In addition to that, we have very strong procedures for people when they ring our call centres or appear at our customer service centre: they have to nominate both that number and their name, address, date of birth and a randomly selected additional question. We are seriously regretful that that has

happened. It is a technical breach of privacy. However, there is minimal risk of this being misused.

What we are doing now is investigating how and what went wrong, removing any reason for this to ever occur again and, obviously, tightening any of those procedures or processes that might have been not sufficient to cope with that. We believe that our processes are actually quite good. I will get Luke to actually describe all of the things that we do within Centrelink that cover the issues of the responsibilities of staff and how we actually manage and monitor those processes.

Mr Woolmer—We split it into two aspects—security and privacy. When a privacy incident occurs, it is generally as a result of a failure of a security process somewhere or a human error in the processing. We have a layered approach to our security arrangements. The first and foremost is a general awareness—a high level of awareness that this is important information and we do not wish to disclose it. We use that as a starting point. Everybody, when they join Centrelink, receives privacy induction training. We have a range of materials available, from videos to manuals to pamphlets to posters in our offices. We have a national series of privacy officers around our area offices and their job is to reinforce that message and do any subsequent investigations. Privacy is a cultural thing in our organisation. It is very topical.

I talked about our layered approach. We keep things stored centrally in our mainframe databases. I will just run through some of the issues. We have the information in our database and we use normal security access to those databases. We use large commercial software that is available from international vendors to do what we call ‘access control’. We set standards and restrictions on who can access what parts of that information and for what reasons. Since 1994 we have had full logging and auditing so, when anybody enters the information which they are allowed to enter, we can always go back and see who has gone where and why. That has helped us in a number of situations where we have had inadvertent access, or maybe deliberate misaccess. We can see where any staff person has been for all reasons. We monitor that and we report on that as well.

For access control systems, we have what is colloquially known as the ‘smart brick’. It is a password generating number generator. It was ‘best of breed’ about three years ago in the world. I put my particular number that is only known to me. It matches my number and the physical presence of this piece of equipment with me. The six-digit number it spits out is spat out from that. I have to enter that into a system. It then has a time window to authenticate into our mainframes or into the LAN and can only authenticate into particular areas. We almost have what we call a ‘single sign-on’ environment, where every piece of software is run through this; a couple of very new technologies are being brought in under the banner of access link this year. This at the time was one of the best authentication mechanisms in Australia and/or the world. We believed we were the largest single sign-on site in the world at the time. Over the last three years it has been superseded with for example biometrics in some organisations and things like that. So we have that sort of regime in place.

Then we have the standard arrangements of strong firewalls between our organisations, encryption of data when we move it around—in most situations when it goes outside of our network—the physical security which is on top of that, and a whole heap of fairly tightly put together policies and processes which we try to enforce across the organisation.

Senator CALVERT—Following that last incident, will you be changing the clients' numbers as a result of what happened?

Mr Woolmer—We will need to see the end report before any such determination is made.

Senator HARRADINE—Have you found it necessary to access CrimeNet and, if so, why?

Mr Woolmer—No, to the best of my knowledge.

Senator HARRADINE—So you would see no reason why, in your organisation in its function of determining whether a person is eligible for a particular benefit, CrimeNet should be accessed?

Mr Woolmer—Personally, I would not see any need for that, but I may stand to be corrected by other parts of our organisation. I would see no need for a Centrelink officer to access that to process a piece of information from a work perspective.

Senator HARRADINE—Could I just go to NOIE. One of the functions of NOIE is the encouragement of e-commerce. Could you advise the committee as to what attention you have given, in your encouragement of e-commerce, to this whole question of privacy?

Ms O'Loughlin—We have done quite a range of things, including things like public awareness. I will ask Mr Dale to run through them for you. It is obviously a key concern to us since, if one wants to encourage the greater use and uptake of e-commerce, this is a critical issue for consumers.

Mr Dale—There have been a number of publications, which we have produced jointly with other agencies, to provide basic information for consumers or potential consumers online. They have addressed a number of issues including privacy and also other questions that people ask, such as about credit card security, complaints, payment of customs duties and things like that.

We have also worked very closely with the Attorney-General's Department in their development of the government's privacy legislation for the private sector and have, I think, helped with facilitating discussions with some sectors of industry there. We not only include material on our web site concerning privacy but also respond as much as we can to requests from industry and consumer groups to explain not simply the government's position but current technology developments and so on. On the issue of a barrier or a potential barrier to e-commerce take-up we find that, although privacy is consistently a concern of consumers, in reality security—which I guess is the flip side of privacy—is often the real concern that people have. The issues that have to be addressed there are not so much privacy protection as prosecution of fraud, for example. There are other issues.

Senator HARRADINE—The regular comment you get still is that there is a great reluctance on the part of people to use Visa card or credit cards and so on. That really is a dampener on e-commerce, is it not?

Mr Dale—It is in the area of business-to-consumer e-commerce. Of course, that is only one part of the broader e-commerce take-up across the community. In fact, in the area of business-

to-business e-commerce, the issues are rather different. They are very much more about security than privacy.

Senator HARRADINE—Sure.

Mr Dale—But you are right; it is a concern. But, in regard to basic reassurance or information on issues such as how safe is my credit card, for the time being we can and will continue to work with bodies such as the Australian Computer Society, for example, and various consumer bodies to produce the most up to date and factual information to give people answers to that question. I do not think it is the answer. I think it is how people perceive it, perhaps. It is going to be hard.

Senator HARRADINE—How safe is my credit card, in commerce within Australia and outside Australia, for example?

Mr Dale—Your credit card and mine are at least as safe as when we use our phone to buy things such as flowers and so on over the telephone. It is a fairly common practice. However, the real safeguards around use of credit cards online, which have seen business-to-customer e-commerce grow, lie in the guarantees that the credit card companies themselves provide where people complain. In the vast majority of cases, complaints from credit card users about apparently wrong charges on their credit card are resolved in their favour. The costs of that are borne by the merchant through the charge-back system that the majority of credit card companies apply. There is a system in place there to provide refunds and corrections which are nearly always, as I understand it, in favour of the credit card holder.

Senator HARRADINE—Within Australia?

Mr Dale—Internationally. The majority of credit cards, such as Visa, Mastercard and Amex, have more or less the same provisions wherever you are using them. I think a lot of online merchants would say that those rules in themselves provide at least as good a system of complaint and redress as any use of your credit card offline. It is not a complete answer by any means, but there is no doubt that if those provisions by companies like Visa and Amex had not been in place the growth of online commerce would have been much less than it is now. There is certainly a role for further work there; that is the work of implementing the legislation that the government is seeking to have passed by the parliament. But, in the meantime, there are guarantees there. We see ourselves as having a continuing role in trying to get more information out to consumers in an understandable form about those guarantees.

Senator STOTT DESPOJA—Ms Treadwell and Mr Woolmer, I am not sure to whom to address this question. It is in relation to data matching, which you have referred to in your submission. I refer specifically to the announcement that was on our radios this morning—that Centrelink will be moving to match records through Centrelink and ASIC and through the Stock Exchange in order to discover hidden assets. I am curious as to whether or not that will entail any changes to current privacy provisions. First of all, I should ask if you are aware of this announcement that I heard Minister Anthony talking very proudly about this morning.

Mr Woolmer—I was not aware of an announcement. If it is being done, under my understanding that would be as part of private companies and trusts changes that were made at the

last budget. There is a large project to manage the legislation differently from Centrelink's perspective—essentially, to reassess the way people are holding assets in those organisational structures. I was not aware of the minister's announcement this morning but I would think it would be in line with that previous piece of legislation. I am not aware that there was a requirement to data match but potentially it would seem a logical position to get that information as well. We have a pretty tight data-matching set of arrangements. It is done under a specific data matching act as well. It was outlined in the submission. We are very cautious about use and re-use of information or any potential use at all. We are also subject to the Privacy Commissioner's inspections.

Senator STOTT DESPOJA—I also heard a figure this morning that suggested that the savings from this measure would be around \$140 million. Is that correct?

Mr Woolmer—I am unaware of any figures. I cannot comment.

Senator STOTT DESPOJA—Perhaps you could take that on notice. I would be curious to know.

Mr Woolmer—Yes.

Senator STOTT DESPOJA—I am wondering what the current Job Network database arrangements are. Could you outline those for me. In particular, I am curious because I know that there has been some talk about the integrated employment system going online—or at least that there are moves afoot to put that online.

Mr Woolmer—The Job Network is part of DEWRSB's portfolio. We have a secure connection with DEWRSB, but I would respectfully suggest you direct to DEWRSB any questions with particular reference to the data and information held by those Job Networks.

Senator STOTT DESPOJA—I am happy to do that. But can I ask again if you are aware that the database is to go online? Are you aware of this process taking place, or that it is supposed to go online?

Mr Woolmer—In what sense do you mean go online? Is it having Job Network members update their own information with IES?

Senator STOTT DESPOJA—I think that is part of it but I thought it was broader than that—that it would be accessed not only through the Job Network agencies but through Centrelink as well.

Ms Treadwell—There is the Job Network database where people can actually interact to find jobs. That is there already. People can gain access to that over the Internet through Centrelink offices and through Job Network providers. There are further developments that the Department of Employment, Workplace Relations and Small Business are obviously wanting to expand on the online side. Those developments are done by that department. The relationship with Centrelink needs to be done in tandem, in terms of what expectations they would have of Centrelink. However, I am not sure exactly what their specific intentions are over the next year.

Senator STOTT DESPOJA—I am quite happy to address those questions to the department, if we can put them on notice.

Senator LUNDY—They are currently not listed to appear before the committee. Chair, I was going to suggest it. I also have some questions which go to the issue of the ABN database, as well as how DEWRSB distribute data from that particular database directly. Could we make some arrangements or discuss it in private meeting?

CHAIR—Are you happy to put those questions on notice or did you want to request the committee to consider requesting them to appear?

Senator STOTT DESPOJA—I am quite happy to place on notice the questions which I currently have, for the benefit of the committee. But, in the short time frame, I am not necessarily suggesting that they have to appear.

CHAIR—Are you happy with that?

Senator LUNDY—I am happy. We are constrained by time. I have a few questions on that issue that I would like to at least attempt to direct to these officers. It relates to the ABN database sale. Is there any officer here that can provide me with information as to the exact status of what the privacy arrangements are for the ABN database, including the sale and distribution of any of that data?

Mr Field—I really think you do have to direct those to the tax office.

Senator LUNDY—Okay. With respect to the Department of Communications, Information Technology and the Arts, we have heard in evidence in previous estimates committees that they certainly have access to part thereof of data collected initially, or compiled, by DEWRSB as part of the ABN database. Are you in a position to answer any questions about how DOCITA uses information as a department when that is handed on or requested from DEWRSB?

Mr Field—I am not aware of the use you are talking of. Is that in terms of communications?

Senator LUNDY—The particular example relates to an IT capabilities database, which sources listings compiled in accordance with the industry that given businesses operate under. That is sourced from the ABN database. Do you have any knowledge of this in DOCITA?

Mr Field—I would have to take that on notice. I do not think that is us.

Senator LUNDY—Could you take it on notice to advise us whether you do source any of that data and manage a service, either in-house or outsourced, relating to, for example, industry capabilities. If you could provide the full details of the management and privacy implications of those databases that would be useful.

CHAIR—Thank you very much for your appearance before us today, Mr Dale, Ms O'Loughlin, Mr Field, Ms Treadwell and Mr Woolmer. Thank you for the way in which you tried to answer our questions frankly. We look forward to some answers to questions on notice.

[12.50 p.m.]

CORONEOS, Mr Peter, Executive Director, Internet Industry Association

CHAIR—I now welcome Mr Peter Coroneos from the Internet Industry Association. Thank you for making yourself available at reasonably short notice, due to some technical difficulties in communication. As you would be aware, this committee does prefer all evidence to be given in public but, if you are at any time asked a question to which you would like to respond in private, please indicate that is the case and we shall consider it. However, any evidence that is taken in that way could be made public by an order of the Senate at some subsequent stage. I understand that you have some documents you want to table this afternoon but that the committee does not have a submission from the Internet Industry Association. Perhaps you could indicate the documents and then we can copy them and circulate them.

Mr Coroneos—That is happening now.

CHAIR—Then you can take us through them.

Mr Coroneos—Thank you, Madam Chair, for the opportunity of giving evidence before this committee today. The issue of privacy particularly in the online context is one that we take very seriously. The three documents which I have tabled today—I apologise for the late notice—are there, I suppose, to testify to the extent to which we have been proactive in pushing for the legislation and also for the co-regulatory format of that legislation.

Perhaps I can begin the points I was going to make by directing the committee to the first document being a letter to the Prime Minister which we sent to him on 30 October 1998. This letter, drafted by me and authorised by the board, sought to encourage the government to review its position which up to that time had been to prefer not to legislate for the private sector on the issue of privacy. In that letter we pointed to three main trends or factors which we believed were relevant to seeking a change in position.

The first was the EU privacy directive which had previously been enacted by the European Commission that potentially had the ability to damage Australia's trading relations with Europeans. We believe that was an issue that needed to be addressed. The second point we made in the letter was the development of what appeared to be the beginning of patchwork, separate legislation from some of the states and we were concerned that we should have a consistent and uniform national approach here and we thought it was appropriate for the Commonwealth to take the lead on that. The third factor—it is one that has been borne out even since that time—is the lack of consumer confidence in dealing with transactions over the Internet and engaging in those transactions. We were urging the Prime Minister to review and to reconsider the government's position on legislation for the private sector. We were delighted when the Attorney-General announced some time after that that the government had reconsidered its position and was prepared to legislate.

Subsequent to that, IIA took part in a business consultative group convened by the Attorney's office. I believe that we made some positive contributions as to the form of legislation and how

we thought it could be implemented. Again, we were delighted when the Attorney decided on a co-regulatory framework as opposed to pure self-regulatory options or indeed to a topdown interventionist legislative model, neither of which we believed were appropriate for the Internet. We believe the co-regulatory framework is well suited to providing consumer protection in the Internet space. We have seen elsewhere, particularly in Europe, much more of an interventionist, topdown, ‘pass a law and try to worry about how you are going to implement it later’ approach. We have serious concerns about the ability of that approach to provide meaningful protection and, indeed, enforceable protection in the Internet space.

On the other hand, we have been quite concerned about developments coming out of the United States by certain, I suppose, bad examples of Internet practice where significant and substantial harm and consumer detriment have occurred through opportunistic use of personal information. We would very much like to see that kind of conduct not occur in Australia. We do not believe we have had any bad examples of that nature or to that extent here yet, but we would like to make sure that did not eventuate. The problem with some of the examples that are occurring, the breaches of privacy in the US, is that tends to impact on consumer confidence in Australia anyway because of the fact that people just simply associate the Internet as being inherently unsafe. That is why we think it is all the more important that Australia has a good, workable regime in place as soon as possible so that we can at least provide protections—as far as Australian businesses operating online—for both Australian consumers and also hopefully for consumers in other countries that choose to do business with Australian businesses.

In the letter to the Prime Minister we actually point to our strategy of wanting to position Australian businesses as, I suppose, more ethical or better regulated than those in other countries. We are hoping to use the regulatory environment as a competitive advantage for Australian businesses seeking to do business in a global context. I guess in the way that you would say Swiss banks perhaps have a good and trusted reputation internationally, we would like to translate that into the Internet context and say that .com.au businesses as a generic term are a safe group of businesses with whom to transact. That is why we pushed very hard for the government to move into this area. It is why we continue to say we want that protection and we want it in place as quickly as possible.

The second document I have tabled is simply a news release dated 1 December 1999 which reiterates why we believe this kind of regulation is appropriate to occur. Also, it averts to the Internet Industry Association code of practice, which has incorporated the national privacy principles and some additional protections about what is done with people’s information. We are very keen to have that code registered by the Privacy Commissioner. Indeed, one of the submissions I will be making today is that we would like that to occur sooner rather than later so that we can overcome this perceptual gap within the market at the moment.

The third document that I have tabled today is a survey that was conducted by the IIA in April this year in conjunction with a magazine called *E-Commerce Today*. That survey asks 13 questions about both the use of spam email or unsolicited commercial email and also the personal information which is collected of customers. I am happy to take the committee through the findings in that survey because I think it illustrates two things: firstly, at least as far as the membership of our association is concerned—which is now about 300 of Australia’s most dynamic and also some of the largest Internet companies—it shows how keen they are to move quickly to protect their customers’ information. Secondly, I think it shows what positive

attitudes they are already employing in respect of customer information, even in the absence of legislation and the code of practice. That is not to say that we should not have the code implemented or we should not have the legislation; but rather we think we are starting from a fairly high base here where compliance generally is very high. That is part of the reason why I think we are going to have a lot less resistance to implementing these kinds of measures within Australia than perhaps might be the case elsewhere.

Those are my introductory comments. I am happy to take questions from the committee. If I could just summarise quickly before you begin questioning: first, we do support the co-regulatory framework to privacy, particularly within the Internet environment. We believe co-regulation offers the best balance between high levels of consumer confidence not only by having the government standing behind with a safety net but also by having the flexibility, through industry administering and creating codes of practice, to move quickly in adapting to changing technologies. The second point is that our members are very keen to commence and to begin implementing our code of practice. We have to see the final form of the legislation really before we can finalise the code. So we are very keen to see this legislation passed. Thirdly, it is our intention to take that to the Privacy Commissioner as soon as possible after that legislation passes to have the code registered.

The fourth point, which I have not made already, is that we think the small business exemption in relation to businesses with a turnover of less than \$3 million should be removed. Indeed, although we have some very large companies, most of our members, the majority, are small companies and they themselves are telling us that they want to be able to engage in high levels of protection. So we are not seeing any resistance from them as small businesses. Indeed we believe some of the more concerning breaches of privacy could occur through small businesses which either do not understand what appropriate levels of consumer protection are and should apply or feel they may be outside the safety net. We think we should cover everyone with this. Finally, on questions like journalistic, health, employment, political party exemptions, the IIA takes no position.

CHAIR—Thank you very much, Mr Coroneos, for taking us through that material.

Senator TIERNEY—Some of the submissions to the committee have stated that Internet organisations feel they have not devoted sufficient resources to security and privacy issues. Do you have a comment on that?

Mr Coroneos—I can only speak on behalf of our members. I think the best way to answer that question is to point to the survey that I tabled here. When you look at it in terms of what they are currently doing with customer information, the majority of them are not abusing that or at least they are not prepared to say so in a survey to us. In terms of resources, security is clearly an ongoing issue. We are certainly very pleased that the Australian Standards Association this year released the new Australian standard for Internet security, the AS/NS4444 standard. That sets a very good benchmark as to what appropriate levels of security are for Australian companies. Whether or not you choose to be certified and accredited under that standard, at least in that standard we have a benchmark for what appropriate levels of security are. I believe that by and large Australian firms offering electronic transactions here are doing so within a secure framework; that is to say, the transactions are occurring within an encrypted environment.

To pick up on the points made by Mr Dale from DOCITA in previous evidence given before this committee, in fact, we believe that transactions occurring over the Internet are more secure than those that are occurring offline. The problem is clearly, we think, one more of perception than of reality. I will relate an anecdote. I was in Sydney airport about two years ago sitting in a waiting area when a person pulled out his mobile phone and proceeded to order a dozen bottles of wine from his wine club. He then gave his credit card information and the home address for delivery. It occurred to me then that people almost without hesitation are prepared to disclose that kind of information over the phone through transactions. Indeed people are prepared to give their credit card in a restaurant or other means like that without really considering the security implications of that. Where you have signed a carbon copy in a restaurant, there is a record of your signature which is pretty much the only fraud protection that we have at the moment from abuse of that information.

Now if I engage in a transaction with you over the Internet and you are the merchant and I am the cardholder and subsequently I dispute the transaction, if you cannot produce a valid signature to authorise that transaction, then under the chargeback arrangements, the risk passes to the merchant and the consumer is not subject to that transaction. My comment as far as the security of credit card information occurs is that it is far more serious an issue at the perceptual level than it is at the level of reality. I would say that, having regard to the encrypted payment technologies which now exist in Australia, the issue is really one of explaining to consumers the measures which you as a merchant are putting in place over the Internet so that you can satisfy them that the transaction is indeed secure.

Senator TIERNEY—We are sitting here, Mr Coroneos, desperately trying to believe that privacy issues and security are protected. In the evidence to us you have given some other underlying principles of why it should be, you have given us two anecdotes and you have also told us about a survey you conducted. Perhaps you could give us a little more confidence in the results of this survey, because you seem to be saying that you have surveyed them and asked them, ‘Are the measures you have in place taking sufficient regard to security and privacy measures?’ and they have written back and said yes. How do we develop confidence in that sort of survey process? How do you validate that what they have said is right?

Mr Coroneos—I do not think we need to. I think what is more important is that we implement the privacy legislation. Whether or not the survey is valid, the survey is there to illustrate what the attitudes are and the industry’s preparedness to sign to a code of practice under a co-regulatory regime. We are not relying on the survey to tell people that they are safe and therefore the government ought to do no more. What we are saying is that that adds further impetus to our call to pass the legislation, put the systems in place so that we can have the code registered and then badge people according to their preparedness to follow those rules. We are not arguing that the situation is fine now and nothing needs to happen; we are saying that the situation in some respects is more of a perceptual problem at the moment but, to the extent there are real problems out there, we want the legislation in place and the codes registered.

Senator TIERNEY—But you do not have any real way of finding out; you have not put in place any ways of finding out if there are problems out there, have you?

Mr Coroneos—The evidence is largely anecdotal or comes from survey results which member organisations such as www.consult have been performing over the last couple of years

where they ask consumers questions like: what are your concerns in dealing with Internet companies? All I can do is point to the survey results that are out there, the reactions from consumers. The last survey I saw was done in March this year by *www.consult*, which asked 31,400 Internet users: what are your primary concerns in using the Internet?

I have to say that privacy and security of transactions were still major concerns out there. I do not have the percentages available but I could provide those. I think it was in the order of 12 per cent for each of those questions. So 12 per cent of users thought privacy was the No. 1 issue and another 12 per cent thought security of transactions was their No. 1 issue. We think there are perceptual problems out there. We think the good thing about this legislation is that, the sooner we have a regime in there that works both by codes and by safety net provisions, the sooner we can start both providing those protections in a systematic uniform way. It is also sending the message to Internet users that they have protections, whereas before they did not.

Senator TIERNEY—You say on things like privacy that it is a perceptual problem. But in terms of reality and of what is happening with that information, you are walking in a bit of fog, are you not? The consumer does not know and you do not know really either, do you?

Mr Coroneos—No, I do not think the problem is a perceptual problem with privacy; I was talking about security of credit card transactions.

Senator TIERNEY—Just specifically?

Mr Coroneos—Yes. There are real issues. I think part of that is that, for instance, small businesses do not know—because there are no comprehensive guidelines in place, other than the NPPs at the moment—about the dos and don'ts about what should and should not be done with personal information. As I say, the worst examples have been occurring in the US where customer information has been abused in fairly heinous ways.

In Australia I have not seen any examples in my capacity within the association of privacy breaches that have come to our attention, but that is not to say that they are not occurring. Why we think this legislation is important is that, while we can go and develop a code for all the members of the association who it turns out tend to self-select from the good operators out there—I mean, you do not generally get cowboys joining industry associations—so while we are confident that our members are doing the right thing, we are worried about the hundreds perhaps thousands of operators out there that will not join an association and will not sign to a voluntary code of practice. That is why we say you have to have this law.

Senator TIERNEY—Can we turn to your voluntary code of practice. We have dealt with your association in previous years on codes of practice in relation to the Internet and, in particular, issues such as pornography. From that experience, I do not have a lot of confidence, in terms of efficacy of codes and also how long the codes took to put into place. On that last point, you might say this is a chicken and egg question; I realise that. It probably will not be quite the case this time. If, in coregulation, self-regulatory codes are an important part of the partnership, I would like you to build our confidence that we might have a code that has greater efficacy than the ones we have seen from your association in the past.

Mr Coroneos—In fairness, the three content codes that we developed last year in response to the content legislation were registered by the Australian Broadcasting Authority in December. They were registered having regard to the community safeguards that they provided. I can only assume that the ABA subjected those codes to whatever scrutiny they apply to any codes and decided that they were adequate. Indeed, the minister has subsequently gone on the record to say he believes, from his viewpoint, that the issue of content on the Internet is no longer the issue it was because of the fact that we now have codes of practice in place.

If there is a deficiency in the existing codes, I would put it to you that it is probably because under the terms of the legislation those codes are voluntary codes and it is not until the ABA taps someone on the shoulder and says, 'You must start distributing filter software,' that they actually have to do that. I do not think it is a reflection on the code. Rather it is on the context in which that is operating. In the context of privacy codes—

Senator TIERNEY—Before you go off that last point, they were registered in December 1999. I think we were discussing this issue in about 1996. My key point was that perhaps the industry should have been a little more proactive and got it all into place a little sooner.

Mr Coroneos—You can make that point, Senator. We think we were proactive. We started developing the code before the legislation ever was a glimmer in the eye of the government. I think the time delays in this are because of the fragmented nature of the Internet. It is still a very young industry in Australia. It is becoming more mature now and we are pleased to see that, but it is no trivial matter to develop self-regulation in the context of such a rapidly changing environment. I do not think we need to discuss the code.

Senator TIERNEY—No. I want to move on this privacy code.

Mr Coroneos—As far as the privacy code goes, we already have a module within our draft code 5. Subject to whatever changes the Senate might seek to this bill, we believe this privacy module will be one of the first to be taken to the Privacy Commissioner for registration as a code. In a sense, we are all dressed up with nowhere to go at the moment until the Privacy Commissioner has the power to register our code of practice. I guess you just have to see our record on this. We wrote to the Prime Minister and we urged the government to change its position on not legislating for the private sector. We have finished, as far as we can, a draft code of practice. We have participated constructively with the Attorney-General on the detail of the implementation of this coregulatory scheme. So we are waiting for you.

Senator TIERNEY—You have been consulting with the Privacy Commissioner in the process of developing the code. Could you describe that a little further for us in terms of the process?

Mr Coroneos—The Privacy Commissioner is well aware of our code and, in fact, in a recent trip to North America, was using our efforts as an example of proactive industry approach to attempting to provide a set of benchmark rules for a sector of the industry. So not only is the commissioner aware of how far we have come with this but he is actually using the work we have done as an example of the kinds of measures that ought be done elsewhere in countries like America. I do not know what more I can say. He is obviously satisfied with what we have done to date or he would not be using it as an example of best practice.

Senator TIERNEY—How are the privacy practices of your members monitored?

Mr Coroneos—Until the code is registered, there is no monitoring. It will be a complaints based system, as is the content regulation in Australia. It is impossible to monitor the day-to-day practices of hundreds of thousands of businesses. What this law is intending to do, I believe, is provide legal means of redress so that if you as a consumer find that your privacy has been abused then you have remedies and processes by which you can have redress. That is the spirit in which we are approaching this through our membership as well.

Senator TIERNEY—You do not think random sampling could work? In effect that is what the tax office does. It does not look at all people's returns, but the very fact it does random sampling is a major discipline on the system.

Mr Coroneos—Part of the government's approach here—and I understand this is the reason underlying the exemptions for small business—is to not subject small business to compliance costs which are beyond their capacity to meet. If we are going to bring in small businesses, as we hope we can do under this regime, then I think that a complaints based system will be the preferred way to go. As a small business operator, I can imagine that having the Privacy Commissioner knock on your door and ask to go through your entire records is probably going to be something that will be costly. I would rather wait and see how the regime unfolds. Let us see if the evidence is that the principles and indeed the coregulatory legislation are or are not working. There is a review period in here, There is provision for review. Let us wait and see. If it becomes apparent down the track that there is very bad compliance, then we will have to revisit the question that you have raised of periodic and random checks and see whether that can resolve it. But I think we cross that bridge when we come to it.

Senator LUNDY—I am interested in your spam survey. For the committee's benefit, could you also describe the other manifestations of breaches of privacy that can occur in an online environment?

Mr Coroneos—Other than spam?

Senator LUNDY—Other than spam.

Mr Coroneos—One—and again we have not seen this yet in Australia to my knowledge, but it has certainly cropped up in America in recent months—is the situation where a business collecting information over the Internet finds itself in financial trouble and subsequently goes into liquidation, only to find that really its sole remaining asset is the customer information which it holds and therefore is tempted to sell that information to a third party somewhere else in the industry. We think that is an example of the very conduct that consumers will be most frightened of and will further serve to undermine confidence in the net. We think that this legislation would actually make that kind of conduct unlawful because, as you see in the principles, information is only to be used for the purpose for which it is provided. If I provide it to you and you later on-sell it to someone else, then you are clearly going beyond the purpose of that informed consent. That would be a classic case of where we would hope this legislation would cut in.

Senator LUNDY—What about online profiling, where identities are either stored or they are not and it is a silhouette profile for the use of manipulative marketing campaigns either online or offline? How prolific is that practice in Australia?

Mr Coroneos—I am not sure of the extent of that practice. As far as marketing goes on the Internet, it is a bit of a double-edged sword. Part of the attraction of the Internet, particularly for small businesses, is the very low cost and the extent to which they can start reaching much bigger markets than they otherwise could. That is a huge driver of e-commerce. I think that kind of thing, provided it is done within acceptable and ethical limits, is actually quite a healthy part of the new economy. The test is the basis upon which that information is provided to the business and the extent to which the consumer is aware of what that information will be used for.

I have recently returned from Washington where I met with Federal Trade Commissioner Mozelle Thompson. We had an interesting conversation about the change in attitude of the FTC towards privacy in the United States. When he was last in Australia in October last year, he was advocating at that point that they did not believe they needed specific legislation for privacy in the US because they believed they had powers under the FTC legislation and that they could hold people to their privacy statements. When I met him a couple of months ago, he was saying, ‘Well, we actually changed our view on this when it became obvious that the worst offenders were the companies that were not putting privacy statements on their web sites.’ So they were making no representation to which they can be held.

Getting back to the question of what is adequate privacy protection, the discussion that we had basically agreed on the fact that the crucial issue here is the question of informed consent. That should be the touchstone. When we are looking at what are acceptable practices in marketing online versus unacceptable practices online, provided that the consumer is told in advance in clear terms that they can understand what information will be required of them and what it will be used for, and also is given the opportunity to subsequently opt out of that, we believe that is an appropriate way to strike the balance between the innovative use of information for targeted marketing—which can deliver quite substantial benefits to consumers because you are not being hit with ads that you may not be interested in. There are cost savings that translate. Those are the pluses. The minuses are that if you have an abuse of that information then, of course, you undermine the whole point of e-commerce because people are just not using it. At the moment in Australia, according to the ABS we still have less than five per cent of Australians engaging in e-commerce. We believe a large reason for that is basically the lack of confidence.

Senator LUNDY—So in terms of our having what can be loosely described as ‘permission based principles’ for marketing, do you see that those principles should be embodied in legislation?

Mr Coroneos—I think they are already embodied in the national principles and, as I understand it, the legislation will in turn embody those principles as well. When you read the NPPs, you will see that everything is about advising the consumer in advance, disclosing what the information will be used for. I think they do embody permission marketing. What we may need to do—and, indeed, we are quite happy to do within our code of practice—is to in certain circumstances go beyond the minimum requirements set by the national principles and put some addi-

tional provisions in our code that provide added protection for people who wish to deal with our members. We already have a few provisions in there that go a bit further than what the national principles say. If it became obvious that permission marketing needed to be translated into practical points that business could apply in Australia then, whether or not they are in the legislation they could certainly be in the codes.

Senator LUNDY—What about sanctions? One of the issues raised with respect to the Privacy Commissioner's ability to process complaints to allow consumers or citizens some form of redress if they feel their privacy has been breached has been twofold: one, the actual resource level of the Privacy Commissioner to give effect to those laws and, two, the level of sanction that they are subsequently able to apply. Does your organisation have a position on the resourcing of the authority that will dispense justice and also the level of sanctions?

Mr Coroneos—If we look at the purpose of the legislation, if it is there to provide consumers with confidence, then clearly that confidence is going to be only as good as the extent to which they can pursue a complaint—have it heard and acted upon. It goes without saying that you do not bring about legislation like this unless you are prepared to adequately resource the entity that is going to be enforcing and monitoring that. As a general point on that, we would be saying that the Privacy Commissioner will himself presumably have views on what resources he will require to do this. We would be very supportive of his being resourced to that level.

Senator STOTT DESPOJA—I might just pick up that last point of Senator Lundy's. There are submissions to follow yours that argue very strongly that there is inadequate resourcing of security and privacy issues in Australia. I am wondering if you would suggest generally that the government has not committed enough funds, whether to resourcing the Privacy Commissioner or to perhaps implementing, say, public education campaigns in relation to online privacy?

Mr Coroneos—While I cannot give you numbers on how many millions of dollars we think ought to go into this area, what I can say from our viewpoint is that, if you are serious about putting a regime in place—this is legislative infrastructure that underwrites e-commerce—any money that is spent here to raise confidence and make the regime work is actually not an expenditure as much as an investment in the new economy. We believe that whatever level of resources is decided by the Privacy Commissioner, who I think should be in the best position to determine what he needs to provide the minimum level as a protection, should be provided to him. We would be critical if we saw a great law come into place where we could register our codes and everything else only to find at the end of the day that we could not get enforcement because of the lack of resources. We would be calling for more funding to go into it. The government should be looking at the outset about adequately resourcing this and ensuring that happens. If the committee will be making recommendations along these lines, our call to you would be to highlight as a major recommendation that adequate funding go into the scheme.

Senator STOTT DESPOJA—Senator Lundy asked you about different manifestations of breaches of privacy or use of people's information apart from spamming. I think you were alluding to the cases that we heard about or read about in the submission from the EFA this morning—the Toysmart.com and DoubleClick cases—and I think you said something like that you would hope that this is something where the legislation would step in or pick up these cases. From your assessment and reading of the Privacy Bill, do you believe that it does? Do you think it provides adequate protection for consumers from that kind of sale of assets or

where—as in the case of DoubleClick, I think—organisations radically change their policy in relation to the protection of privacy of individuals' information? Will the legislation pick it up or do we need to strengthen it in some way?

Mr Coroneos—The principles are very broadly cast. Part of the answer here is not only to stipulate what adequate levels of protection there ought be but also to have an informed market out there that understands what their rights are so that the complaints regime can work properly. We think it is better to leave the principles as general as they are. Sure, the codes can raise the bar here and there, as we are attempting to do. But ultimately once people understand what is fair play here, then they will develop a better sense of what is not fair play as well. Provided the provision is not so broadly cast that you could not pursue a remedy, then we believe that those remedies will be available. I see nothing in what DoubleClick or some of these other cases have done that would not come within the ambit of the principles.

Take the first principle, that says that information should only be used for the purpose for which it is provided—I think that is No. 1. That is a very broad statement. If you as a consumer believe that the information you have provided that company has been used for purposes other than for which you provided it, to the extent that that principle is entrenched in law you have your avenue for action. I do not think we need to go down to levels of particularity. The danger is that the more specific the legislation is the more likely it is that you will be excluding certain practices, as the technology, particularly in our industry, is developing. We would rather keep it general to catch as much of the wrongful conduct as possible rather than attempt levels of particularity. The codes can address that particularity. That is why we say the coregulatory framework is so efficacious here. It gives you the ability to refine and adapt the codes and keep the legislation as the basic underlying foundation.

Senator STOTT DESPOJA—I acknowledge the work that you have done in developing the code and also in being part of the push to get the government to implement its 1996 election promise. You will no doubt remember the Democrats with our own private member's bill were keen to ensure this happened sooner rather than later. But you talk about raising the bar within your own code, for example. Should there be other limitations? For example, should there be limitations on the use of cookies? That is something that the committee is interested in.

Mr Coroneos—Cookies are a really interesting case. Again, it is an example of a specific technology which is in widespread use now. It underlies the performance of certain online shopping experiences where, if you are putting things that you are buying into a virtual shopping cart and then going from one page to the next, you actually need to have the cookies there so the site remembers what you put in the cart from one page to the next. So I do not think you can actually outlaw the practice of cookies without severely limiting what can be legitimately done.

But to come back to the question: the touchstone here is the issue of informed consent. That is the key. So against any example that you can find, you ask the question: is the consumer adequately informed? Have they consented? If the answer is yes, I think the technology should be allowed to develop without feeling that you have raise specific hurdles for each possible abuse before it has occurred.

Senator STOTT DESPOJA—I acknowledge in your opening remarks that you said the organisation did not have a view on the exemptions for political parties, and I think you referred to medical and media—

Mr Coroneos—And employment records.

Senator STOTT DESPOJA—Was that because you could not agree on a position or did you just consider that inappropriate or out of your sphere of interest?

Mr Coroneos—It is outside the ambit of the issues that we think we ought to be addressing here. We do not have a view as to the adequacy or otherwise of the exemptions that are in place there. All we are saying is that from our viewpoint, having regard to the concerns our members have raised and to what has been evident in the research of the concerns of the consumers in their online experience, those are questions that we do not turn our minds to because they are not key issues for us.

CHAIR—I think that brings to an end our questions. Thank you very much indeed, Mr Coroneos. We do appreciate your bringing along those documents.

[1.35 p.m.]

AULICH, Mr Terrence Gordon, Managing Director, Aulich and Co.

PROBERT, Mr Andrew, Senior Consultant, SecureNet Ltd

CHAIR—Welcome. You would have heard me indicate to the previous witnesses that we prefer all questions to be answered on the public record. But if there is a question asked of you that you would prefer to answer in private please indicate that you would like to do so and we will consider your request. The committee has before it submission No. 13 from SecureNet and No. 18 from Aulich and Co., which have both already been published. Are there any alterations or additions you would like to make at this stage?

Mr Aulich—No.

Mr Probert—No.

CHAIR—I now invite each of you to make an opening statement and perhaps summarise the main points from your submissions. Then we shall have some questions for you.

Mr Aulich—Thank you, Madam Chair. My submission primarily tries to cover a number of areas ranging from what you do with legislation through to how you can change the culture of government and the private sector, in relation to the protection of privacy and the maintenance of security in our IT industry. I suppose the major point I want to bring up front today, given the time we have, is the question: who owns the data in practice, both of companies in Australia and also of the individual citizens who will be affected by how that data is used.

Outsourcing is one of the main issues that you need to address in some way or another. Although you may not be able to do it in legislative terms, you will probably have that opportunity to do it in terms of advising the government as to how it could administer the tender process. I would make the point here that we are not just talking about outsourcing of government because, in essence, the industry will be controlled by those who are most successful at getting both government business and managing it and also getting the business that spins from that, which is the management of the financial institutions such as banks and insurance companies, et cetera. So it is pretty likely, for example, that the major players in the outsourcing of federal government data and assets will, in fact, be the winners also in the private sector. This means that across the board, essentially, so far, foreign based companies and foreign owned companies will be running the data of Australian companies and individual citizens.

For the most part, Australians are employed in those companies. But, ultimately, the responsibility for the direction of those companies and what is done with the data is in the hands of the administrators or legislators here and, possibly at the end of the day, their head offices in Germany, England, France or, in particular, the United States.

So I have made one suggestion in my paper that might help a little to clarify the responsibilities of the major companies, which are likely to be multinationals, towards the small

and medium enterprises, the subcontractors who are handling their IT contracts. For example, security and privacy protection is very likely to be done by smaller, very focused companies as part of an overall consortium. They are not likely to be done by a major prime using its own direct employees.

I suppose the key issue is: how do you make sure that Australian companies are upskilled to take part in that process so that they, in fact, grow as part of the outsourcing process, so that we start to own and control the data that belongs to our individual citizens and the companies that exist or are registered in the various government data bases? I made the suggestion that, for example, whenever the government examines a tender—and let us say you get to the final two bidders in a tender process for outsourcing—any SME that has had a business relationship with those major primes be asked or invited along to give their views about the history of their relationship with that major outsourcer.

I will just give an example. Let us say it was EDS or IBM. We would want to know how IBM or EDS had dealt with the SMEs over the last three or four years both in their government contracting and in the contracting, say, of a bank or any other major organisation in which there has been an outsourcing project. The SMEs would be invited to come along and say, 'We've had a good relationship, we've grown as a company as a result of that relationship and our skills in privacy and security protection have increased as a result of our relationship,'—including the number of employees, particularly those at that smart end of the IT industry.

Currently, a major outsourcer is free to win a bid and then, at the end of winning the bid, simply to say to the SME, 'I'm sorry, you're in the bid with us, you helped us to win the bid but you're no longer needed because your price isn't right,' or 'you couldn't adjust it downwards when we needed to cut costs.' Alternatively they say, 'I'm sorry, the payment cycles are going to be a little slower than normal.' Alternatively, the penalty system for non-performance will be pretty much against you. In fact, in some cases, I understand that some of the major outsourcers make money out of non-performance by their subcontractors. I will not go into details as to how that occurs. But, essentially, if you have an open forum in the tender process, you are able to see how SMEs have enjoyed or grown from the outsourcing arrangement that they have come to with the major outsourcers. That is the first thing.

The second thing is that there is a certain tendency in the industry and you need to watch for this very carefully—and I guess this is by way of warning to the senators, who probably know far more than I do about the technicalities of the technology of the IT industry. This goes to the way the industry actually works; in other words, it goes to understanding how it makes its money. If there is no money in security and privacy protection, then literally that will not be where the major companies go; that will not be where they put their resources. They will bring in other people on a cost effective or even very cheap basis to provide security and privacy protection in their bid. It does not matter whether they are going for a bank or a government agency, they will simply look for the cheapest solution, and they will beat the SMEs down in order to get that cheap solution. In contrast, however, as we have all seen in e-commerce, the major inhibitor to the growth of e-commerce and business online for government, and therefore cost-cutting and extra service provision for government, is the fact that the consumers do not trust the way that organisations—that is, government and outsourcers—are protecting their personal information.

I can say that, of the 18 or so employees and subconsultants in our organisation, I cannot think of one who would conduct e-commerce. That is because they are in the industry and they know what can go on and they know that there is at the moment a less than perfect record for the industry in protection of privacy and the provision of security. That is mainly because security rates at the end of the line when it comes to major bids. I invite you to have a look at some of the tender documents that have come out from OASITO and other organisations, either in government or the private sector. You will see that security rates, from the ones I have seen, from between one page to four pages in documents that are anything up to 400 to 500 pages long—and it is usually stuck somewhere back in the rest of the thick paperwork. So there are a number of areas where I think you need to look pretty carefully at the way the industry is going and to understand how the industry works.

I know, as a politician in the past, I had very little idea how new industries operated, where they made their profits and why they would move in one particular direction and not concentrate on other services. The answer, I guess, is that they work out where they make their money and where they protect their corporate reputation. They are the most important issues for them, plus share price. When you are dealing with an immature industry like the IT industry, essentially, share price is the key. Every third month they will do extraordinary things in order to improve their profitability or their sales—and I would put it this way, ‘their nominal sales’. There is a difference between ‘real sales’ and ‘nominal sales’, as many of you will know. In this industry that is very important because the share price is absolutely vital, given that the industry rewards its key executives for the most part with share or stock options. Therefore, governments have to be aware that that is what drives industry, and security and privacy protection will not be at the forefront of most companies’ agenda unless it is forced on them.

In short, I do agree with the notion that has been mentioned here this morning that you do need a rather strong privacy legislation regime. I do not think it has to be absolutely draconian. But I think you have to be aware of how the industry operates and, certainly, you need to look very closely at the codes of practice that the industry is bringing to you or that will be brought to the Privacy Commissioner.

Secondly, I think you need to assume that, unless you—being governments, parliaments, financial institutions and major companies—can convince us, the consumers, that we are going to be protected, the cost savings that governments, for example, can gain out of doing business online and the enormous benefits they can get in terms of service provision will just not appear in the way that we have calculated. If you are doing forward planning for budgets for a government and you are saying, ‘We are going to have a take-up of online business of this per cent by this year and this per cent by the next year,’ and you are hoping for savings on that basis, you are going to have to be pretty tight about the way you handle the rules and regulations in relation to the growth of that industry and the way it should perform.

So the industry, in a sense, is now saying, ‘Please regulate us; please give us the legislation which is strong enough to enable us to compete in the OECD area and the European Union to fit in with their directives.’ They are saying also, ‘We want to be able to assure consumers that their personal data and financial transactions are, in fact, secure and safe.’ At the moment, they are not convinced of that.

CHAIR—Mr Aulich, Senator Calvert has an appointment at 2 o'clock and he is quite keen to ask you a question. Could we get that question in now? Other questions will follow perhaps after Mr Probert's presentation, thank you.

Mr Aulich—Fine, Madam Chair.

Senator CALVERT—In your submission, I note that you refer to the incidence of hacking. As you know, I have a farming background. In my industry, crackers are old sheep. Here you are talking about hackers and crackers. I am just wondering whether you are talking about young people who hack into business and crackers being the older people? All jokes aside, I think you make a very good point that it is a young person's game, virtually. You raise a situation of hacking and cracking and whatever. Do you believe there should be a strengthening of penalties for hacking because of the large amount of it that seems to be occurring?

Mr Aulich—Yes, I have two responses there. The crackers are those who are basically doing it with criminal intent or intent to do real damage. Hackers are generally conceded to be people who, for curiosity and ego reasons, just want to prove that they can get into systems. They probably are not doing anything illegal but they probably are just on the edge. The crackers are the ones you would be watching and they are the ones who, for example, for personal gain want to commit fraud or want to bring a system down, literally. They do not like a government organisation and they want to bring it down, or they do not like a sponsor of the Olympics and they want to bring their system down—those who have actually committed a crime. That is essentially the difference between the two.

Yes, I think the first thing is to have enough educated police to deal with them. Looking around states, I would say that they are just not resourced adequately to deal with the enormous number of hacking and cracking incidents that occur. In fact, if you rang them, they would say, 'Thanks, we'll get back to you.' That would not be all of the police forces, but some are very, very thinly resourced—inadequately so.

CHAIR—As Senator Lundy has a couple of questions for you, Mr Aulich, perhaps we will go to her at this point.

Senator LUNDY—Just reflecting back on your comments about the IT outsourcing program, I do not know whether you were present when I was asking Centrelink about the methodology by which they extended the provisions of the Privacy Act 1988 to private contractors. It seemed very clear that they had not only attempted to hang on to formal responsibility of privacy and security issues but also hived off those aspects of that work within their current request for tender documentation. In fact, that is close; I think it is actually tender documentation in negotiation now. Do you think that the hiving off of all matters relating to privacy and security in management of government databases would go some way to addressing what I think is a very real concern: the loss of control and ownership, in some respects, of information gathered by government to facilitate a public service?

Mr Aulich—It is a question of risk. Under the current legislation, you have to contract the obligations for the outsourcer. The outsourcer has to agree to meet certain criteria, and you hold them to it legally. Otherwise, it automatically comes back to you. If IBM were running a particular group of agencies, it would not be IBM's responsibility ultimately to protect privacy

and security. That would automatically go back to the agency, unless the agency had specifically set out the criteria that needed to be met. I believe that should be done more clearly. As people get more expert at handling outsourcing contracts and understanding the role that security and privacy plays in outsourcing, I think they will start to write those much more securely. But, currently, I think we are in an in-between world where nobody knows who actually really controls it at the end of the day. That is why you are getting a lot of breakdowns at the moment in the government system in what I call fairly basic privacy protection.

Senator LUNDY—How critical is the underlying technology architecture of a given agency or department in establishing an environment in which privacy and data security can be adequately maintained? What is the relationship between the policy and the hardware?

Mr Aulich—Generally speaking, you look at security and privacy protection from four pillars. The three key ones are computer protection, your communications system and, most importantly, your procedures. The procedures pillar—that is, how do you work out who gets access to what data, how is it protected in transmission—is vital. So there is a technical question there. But, really, at the end of the day, the key issue that really counts is how the people are managed within that system. You can have all the technologies under the sun but, if people log on generically in a particular organisation or if you give a free-for-all to people who have very senior administrative rights, all that technology will not prevent inappropriate people gaining access to key data to which they have no right.

You can see this in a couple of cases that have occurred in the federal government with people who would have been very senior and who would probably have responded to a security person with the view that, ‘I’m a very important person, you can trust me and, therefore, I should be allowed to come in and work on a Sunday or from home remotely and get into any database I like.’ If someone says that and is allowed to do that within the organisation, or with very loose controls over them, then you are bound to have trouble sooner or later. I have not been able to find out how much of the \$146 million worth of fraud that, according to the Auditor-General, occurred in the Commonwealth the year before last was committed by senior people in government agencies. But my guess is that that would be the most interesting figure of the lot. That, again, is about the control of personnel and the way you allocate rights to access databases.

Senator LUNDY—So, even if the strategic control of privacy and data security were retained within the agency or department, you say that some risk could still be presented because of it being affected by all these tiers in the way that it is managed.

Mr Aulich—Yes. You have to manage the risk as the owner and, no matter how much you outsource, you have to set tight criteria for performance. From what I have seen, a number of the outsourcers, for example, are not providing all the documentation that I would expect if I were the client. In other words, if you wanted a breakdown of performance indicators on the technological side, sure, they can give you that. But if you were to say, ‘Give me all the patches that you have done or vulnerabilities that you have fixed in an underlying operating platform,’—like NT, for example—you would be lucky to get that provided to you gratis by the outsourcer, unless you specifically write it in. On many occasions, that is not written in and it is not required. So, at the end of the day, the agency owns it and ought to be controlling it, even though it has been outsourced to majors to do.

Senator LUNDY—I have asked this question at a number of Senate estimates committees of particular agencies and departments who have outsourced their IT. The response that continually comes back to me is that they have translated the provisions of the 1988 Privacy Act into a clause in the contract and thereby transferred the law by virtue of that contract to be applied to the vendor. What is your comment on that as an adequate mechanism for the protection of privacy of information held by government departments but now controlled, in effect, by private companies? Is it adequate protection?

Mr Aulich—The agency owns the data, no matter what they do in outsourcing, even if they set tight criteria. It is up to them to make sure that the outsourcer actually protects it. As much as anything else, I would say that the roles of the Privacy Commissioner and the Auditor-General are vital here in that from time to time they need to look at how privacy is protected—and, in the case the Privacy Commissioner, some very detailed audits need to be done about complaints that are coming into that particular agency.

Most people do not bother complaining. I have to say that the breaches of privacy are probably much higher around the country both in government and the private sector than we would recognise because most people do not bother. I can find examples of similar advertising where people are asked to give other people's private emails to a cinema company. Then, suddenly on your screen you have a note which says, 'Your car being of this type may have been stolen. We have seen witnesses. Would you like to call this number?' It is just an advertising gimmick, but it is an example of the sort of culture that prevails out there in many places. You can literally just get this out of vulnerable young people at home on the Internet, and someone's privacy gets invaded. That is, you get an email at work which says, 'We think your car has been stolen.' That is a typical example of the culture.

Senator LUNDY—Are you aware of any private company engaged as an IT outsourcer either in Australia or around the world which has, I guess, a range of business interests that has, for whatever reason, used that public database or information contained within it for commercial purposes not related to the business of the government department?

Mr Aulich—No, I have never been made aware of that. That would be your greatest problem. But I doubt if you would ever know that, especially where the control of that IT outsourcing company is offshore.

Senator LUNDY—Are you aware of how many databases for Commonwealth government agencies are actually housed within hardware offshore?

Mr Aulich—As far as I know, the majority, with the exception of backup and contingency facilities, are in Australia but they would certainly in many cases be out of Canberra. In order to get critical mass, they probably do it out of Sydney or Melbourne. What you would find is that there would be a significant number of agencies and private sector clients all serviced out of one facility, say in Sydney, which, if you are in the Olympics, constitutes a bit of a problem as well.

Senator LUNDY—I hear rumours all the time about large vendors who have, for example, a major private sector client and a major public sector client utilising their mainframe to store their data in such a way that that data coexists on the same mainframe, albeit separated by the formulations through which they access that technology. If in fact that were true, it would be

almost like a technological Chinese Wall that exists between the fields of data in that given database to serve different clients. Are you aware of any relevant laws or structures or do you have any comment on that type of distinction? It is really affected by the contractual arrangements, as these big databases are consolidated within vendors who do have really large public and private sector clients.

Mr Aulich—Certainly they exist. They do bring a number of clients, public and private, into one physical facility. The only way that you can control that is to request during the contractual period that the outsourcer, the service provider, has certain physical controls built in. That is the fourth pillar of security and they have got to be able to guarantee that. There have to be very strong penalties involved for them if they breach that, because sooner or later people talk in the industry. In the industry, the average length of time for senior people to stay in any particular company is about 18 months. As you can imagine, it is a very loose industry in terms of who says what and who is prepared to bag previous bosses. Loyalty to the organisation—and that is in fact a security issue—is pretty limited nowadays, given the way the industry works.

CHAIR—Can I just draw together three threads that you have made in your submission and in your comments today and they are: the public awareness of existing and potential breaches of privacy, the fact that the solution could be found with a better informed public, and the comments you made about older people being less familiar with the technology. How do think that this particular issue of public education could be dealt with? Do you see it as being the responsibility of the providers through the Internet industry associated with some sort of code of practice? Do you think the government should regulate in that way? Who should conduct a public education campaign to make those people better informed, given that, as you say, they are now more aware of the potential for breaches of privacy?

Mr Aulich—I think it is mixture of all of them. The key thing is the media. They are the ones who, primarily through television but occasionally in key articles, ultimately decide the agenda. I have got to say that a lot of the media, since they are relatively young—well, they look young to me nowadays—have been brought up in an IT world and they tend to take for granted what I would regard as relative abuses of privacy. They are not number one on their agenda. They like the notion of the latest, flashest technology because that is what they tend to work with. But I think politicians, on committees like this for example, are the appropriate people to raise the issues and the media will start to pick the issues up sooner or later, particularly if consumers start to complain because of the loss of their own data, data being given to other people or inappropriate people or financial fraud going on. There are a number of issues but, essentially, I think the media is first helped along by committees like this.

Secondly, it is in the vested interests of the service providers themselves to actually make it work. As people know more about how privacy gets abused in this IT age in order to survive in the marketplace they are going to literally lift their game, but at the moment we are a bit slow about the way we handle outsourcing, for example. I am not all that confident that the politicians are going to spend the time or have the experience in understanding how the industry works. At the heart of it is: who makes money and how do you make money? They are the drivers in the IT world. Catching up with what they do and how they abuse privacy is very difficult. It requires a lot of time and you have to talk to a lot of people. This is the start in committees like this.

Senator TIERNEY—You heard Mr Coroneos's evidence from the IT association. Have you any comments on any aspects of that evidence that he presented today?

Mr Aulich—I thought what they said was quite interesting about the way the overseas countries have affected what we do here. Their views appear to have changed over the last three or four years, based on the fact that the Europeans in particular will not do business with our companies unless we have special privacy laws or regimes in place in Australia. Therefore industry has gone from a position where it wanted to be lightly regulated, at best, to one now where it does want some regulation in order to prove its credentials overseas.

Senator TIERNEY—Moving away from the Wild West?

Mr Aulich—Exactly. I think that has to happen, otherwise the Europeans simply will not do business with us.

Senator TIERNEY—Okay. Are there any other aspects?

Mr Aulich—One of the first things we do when we ask our people to go in and do penetration tests in companies or organisations is to ask them to look at the Internet service provider. We always regard that as one of the weak points of any system. We would like to know more about the way in which they actually protect their systems. Some, I think, are like any other business: they are struggling out there in the marketplace and they are not prepared to put the money into protecting their service and the technology that they use to provide that service for you.

Senator TIERNEY—The company or the Internet service provider?

Mr Aulich—The Internet service provider. That is a weak link in many areas and, again, there will be a shakeout in the industry as some suffer some major breaches of privacy and security. They will go out of the market pretty quickly and those that survive are going to be the ones who spend the money and do the work on security.

Senator TIERNEY—That is an interesting point.

Mr Aulich—It is a time consuming process to take one server and fix it to make sure it is secure. You cannot just put in a box and link it up and say it is going to provide the security now with a password.

Senator TIERNEY—You stated in your submission that public awareness of privacy issues is critical, and in response to Senator Ferris you indicated perhaps some ways of improving that privacy. Could you perhaps give us a better feel of what the current level of awareness is with the public in terms of security of information and privacy issues?

Mr Aulich—It is fair to say that the Australian public, which has always shown a degree of commonsense in the way it handles politicians—and I think Bob Hawke once said that, on the whole, the Australian public has always picked the better of the two major parties each election—

Senator TIERNEY—That was when he was winning.

Mr Aulich—Yes, I think so, but he also applied it to the Menzies period as well. In other words, of the two the public tended to go for the one that, at the time, was most ready to be in government. They have a similar view about IT and privacy and they kind of know their rights.

They are aware that there are breaches all around the place, but they just hope that things are going to improve. They will certainly, for reasons of rewards, embrace IT. That is the major motivation for them. If they know they are going to get frequent flyer points, or any sort of reward points, or win a lottery or whatever, they will give away information which ordinarily they would not give away. So they are going to connive in a way, or collaborate, in their own loss of privacy when they move towards the reward system and take part in it because the databases that Amex and others have are extraordinary. It is beyond what any of us can imagine in this room. If you have a look at your Amex application form you might see that you have given them, like most credit card companies, an enormous freedom to do what they like with the information you give them. I presume you get frequent flyer points, so you would be in the same boat.

I would say the Australian public knows there is something wrong; they are not taking up e-commerce in the way that they should. In other words, they are bad consumers, primarily because they think there is something wrong but they are not quite sure what to do about it. They are going to need some leadership somewhere, which is really to tell people how the system works.

Senator HARRADINE—Are there frequent flyer points to Canberra and back?

Mr Aulich—I do not think you parliamentarians get them anymore, do you, you have to give them away.

CHAIR—We get them, but they are actually owned by the government as part of the process to get lower airfares.

Senator HARRADINE—They are unwanted!

Senator TIERNEY—I was quite intrigued, being a customer of American Express, as to what you said about American Express. Perhaps you could elaborate a little further. We know they have a vast database, but just give us a flavour of what you think they might be doing with that database that we customers may not be aware of.

Mr Aulich—If you sign the caveat at the bottom when you make an application for credit with credit card companies, generally speaking you agree to them using your personal data in any way that they see fit, that is, to on-sell it to other people and to amalgamate it in other databases. They have a code of conduct about making sure it does not get out beyond those people who they want to give it to, but it could include your income, your marital status, your children, and, if you are taking up life insurance via one of those credit card companies, it could mean your spouse's, your siblings' and your parents' health records. You start to see some of the implications of that.

To be personal, I think my brother would sooner die than let me know about his medical condition and yet when I fill in forms for credit or for life insurance, and sometimes the two merge, I need to give the full medical history of my immediate family. I am not so sure that I should be asked to do that. Credit card companies can pull all this together because you allow it in order to get rewards, or to take part in the rewards system. Most people will not read that very detailed information that appears on your application form.

Senator TIERNEY—So that explains why these strange things pop up in the mail that we have never requested?

Mr Aulich—Yes, it is why you get the advertisements for Mercedes and so on. Yes, they know your profile very well. I indicated here that one of the fastest growing industries in the United States is the information industry, the data industry, which is essentially the industry that literally provides whoever wants it, whether it is politicians or banks or whatever, with full profiles about people's tastes, lifestyles, spending patterns, and personal views. They are massive. I always work on the basis that if Kerry Packer gets involved then obviously there is a chance for money to be made because he is a very adept businessman in many ways. As soon as he moved into this type of database business I knew that that was coming to Australia, to a PC near you.

Senator TIERNEY—I raised the question with Mr Coroneos about doing random audits, like the tax office does. He says it should be on a complaints basis. That has always worried me—let the crime occur and then we will try and figure out what we are going to do about it. Of course, what the tax office does is random audits. Do you think this area should be subject to random audits?

Mr Aulich—Yes, very definitely.

Senator TIERNEY—Could you explain why.

Mr Aulich—The Privacy Commissioner should be asked to look at databases held and accessed by government agencies, to literally take 500 people at random and then work through—because the audit logs will show all this anyway—who had access to the database, for what purpose it was used and which companies were involved in it. For example, if an outsourcer were running, let us say, Centrelink's database, it is very likely that the outsourcer will use subcontractors for maintenance and support, and maybe for upgrading part of the system. The number of people who were involved could be quite interesting. To see who got access to the administrative rights of the system or just to some of the data would be quite interesting. The Privacy Commissioner would probably find it very fruitful work to go in and look at those on an audit basis at random.

Senator TIERNEY— Mr Coroneos says this would place undue stress on small business by increasing compliance costs. Do you think that is a real concern?

Mr Aulich—I cannot see so. I do not see how random auditing in the tax office has increased compliance costs for small business. We have not experienced that.

CHAIR—Thank you very much, Mr Aulich. Mr Probert, you have been very patient. Would you like to make a couple of opening remarks and then we will see if there are some questions for you.

Mr Probert—Thank you. In our submission we stated our concern at the lack of controls over organisations with regard to implementation of e-privacy. We have presented some research statistics showing that a significant number of senior executives are unaware of their security vulnerabilities and hence privacy vulnerabilities. We noted the apparent lack of security controls and the well-publicised exposure of the GST Start-Up site. We have no doubt that this will follow the course of the famous Australian case in 1995, when Skeeve Stevens was punished under the Crimes Act 1914—suitably amended, I hope—for hacking and exploiting vulnerabilities in the Ausnet ISP site. This earned him a three-year jail sentence. It appears to us that there was a major deficiency in corporate governance before these events which set the stage for inevitable compromise of security and privacy, leading to a loss of consumer, business and international confidence. Ausnet went out of business two months after the event due to lack of consumer confidence. This is unlikely to happen for the owner of the GST site, but the point stands.

As a security company, we highlight that many of the security issues presented by the Internet are old computing issues. There are security engineering terms for them, including authentication, authorisation, permissions management, content integrity, digital signatures, non-repudiation, denial of service, impostor attack, physical processes—and the list goes on. These terms need to become a part of the everyday e-business vocabulary. Simple business level questions to the implementers of the GST site, such as, ‘What authentication must the person present to the site?’ and ‘What authorisation rule is in place to control information release?’ would have flushed out this vulnerability before commissioning of the site. Such questions, and many more, will also need to be asked before implementation of the proposed national health medical records systems.

In conclusion, we must all recognise that the Internet now offers an opportunity for a massive acceleration in the release of information to a point anywhere on the globe which will be outside the jurisdiction of our Crimes Act. The Internet is a promiscuous network: you can catch anything from anybody. The onus must be placed on the service providers to implement systems which release information to only authenticated persons who are authorised to access the data through permissions management and in a confidential manner with audit trails. We certainly must be able to authenticate people accessing these systems within our jurisdiction. As a security company, we have provided opinions and information that would assist in managing privacy on the Internet. That is to say, it is technically possible to secure transactions over the Internet in support of privacy and we have been doing so in a large number of major corporations. However, we should not rely only on remedial court actions, but take a proactive business management and corporate governance approach to this issue of e-commerce.

CHAIR—Thank you, Mr Probert. In your professional work, have you ever come across the situation where a database has in fact been hacked into, entered, by an unauthorised person and no-one in the company is aware of it?

Mr Probert—That is a conundrum, because if I had known about it I would have been aware of it. Not personally. When I was at the Maxi multimedia site, which is the Victorian

government's e-commerce portal—for 18 months I was the technical director there—we noted numerous attempts of access to our site, or connections coming from all around the globe, such as from the research labs at Lotus. A lot of people were just curious to see what was going on. At that particular site, we had gone through rigorous security design and implementation and penetration attacks. But it goes on. Regularly, if you are running any major e-commerce site you will see unsolicited traffic coming to that site.

CHAIR—Are you confident that technology in building firewalls and restricting access is keeping up with developments and the proliferation of database information people?

Mr Probert—I believe, certainly, the security technology is keeping abreast of these sorts of things. The procedural implementation and the business rules surrounding that, ensuring that there is adequate budget to implement such technologies, is not.

CHAIR—Could you explain that a little more?

Mr Probert—Security is an insurance policy, and it is the choice of organisations as to how much to invest in security against a compromise. When you are at the pointy end of business, security does come last in many business budgets and is often an afterthought, not designed in from day one. For example, we said in our submission that when we are asked if control of information release is an expensive process we say that it is not expensive at all if it is designed in. If I design my system to be spot audited for privacy purposes then somebody suitably authorised should be able to walk in the door, push a button on my computer system and produce the audit report.

CHAIR—What about the decision to exclude small business? That almost seems, listening to Mr Aulich and you, that small business is in fact a somewhat vulnerable section of the community in relation to e-privacy in the sense that one of the important stock in trade items, I suppose, would be the customer database. If these people are excluded from legislation, are you confident that they will still place a high priority on e-privacy?

Mr Probert—I would not exclude them from the legislation. I do not think small businesses generally build their own computer systems. They buy systems from the likes of Quicken. In the medical industry, they buy pharmaceutical dispensing systems from NewSystems or Medical Director. These are databases that are put together for that industry. Appropriate legislation would result in privacy enabling features being built into the databases, being built into your Quicken and your QuickBooks. They would benefit from some overarching framework, because the providers of technology to them would engineer those features into the technology.

Senator LUNDY—You mentioned before the issue of the ABN database. Can you expand a little on your comments in relation to that and on what the legal remedies are, in your view, of some of the breaches of privacy that occurred to businesses involved in that scandal?

Mr Probert—In the GST Start-up database—I will caveat that by saying that I know only what was published in the public domain—my understanding is that a system was put up that had no security infrastructure, that it was possible for somebody to formulate a simple web query. They wrote a program to iterate through all possible account numbers, and the system was just delivering back information without respect to authentication or authorisation. So that

was either a technical oversight, which in the Internet world and in the speed to market is easy to do, or there is a lack of corporate governance there to make sure that tests and business rules are applied prior to the commissioning of these sites.

Senator LUNDY—There was a lot of media speculation around at the time on this—and do not feel compelled to comment on it. Because that lack of corporate governance led to that oversight in the technology structure, is it right to consider the person who did that a hacker, not so much in the way that they made it very public and clear that they did not subsequently use that information in an illegal fashion, but in that they were able to do it without any restriction?

Mr Probert—I am not a lawyer, but my reading of the Crimes Act suggests that there is a six-month penalty for accessing a government computer system, either on a government computer or through a carrier network, in an unauthorised manner; there is a two-year penalty for using the data fraudulently; and there is a 10-year penalty for damaging data on a Commonwealth government computer. It may come to a fine point of law as to whether that person was or was not authorised to access the data. If it ever gets to court, it will be tested in court. It is certainly unlike the Ausnet ISP hack in 1995 where the person stole about 1,000-odd credit cards and used them fraudulently and maliciously.

Senator LUNDY—Are you familiar with the guidelines that the Commonwealth government departments use for the construction of web sites?

Mr Probert—No, not in detail. I have been peripherally involved with them as a part of the Maxi projects where, on a number of occasions, we spoke to federal government agencies.

Senator LUNDY—I appreciate you are busy but, if you have the opportunity, I would be interested in your opinion on the adequacy of those guidelines—

Mr Probert—Certainly.

Senator LUNDY—in the context of looking at the privacy and data protection provisions within those guidelines.

Mr Probert—If you can make them known to me through the secretariat I will take a look at those.

Senator LUNDY—Thank you. With regard to the general management of databases within the possession and control of the Public Service, I guess that, in the same way that there is a consolidation of data in the private sector, it is to be expected that there will be a consolidation of data within the public sector as well. Do you have any experience as to the relationship between the actual technology architecture and the capacity to effectively find a wider range of applications for that data in the Public Service?

Mr Probert—I have not been personally involved in any projects that have done that, but there are certainly technologies out there that are engineered for data matching, for taking a wide range of disparate data and putting them together to try and infer more knowledge from that data. I believe a number of Australian organisations often look at that sort of data. In the interests of privacy, you are forever treading this fine line between aggregation and matching of

data to give it more value versus keeping it distributed and disparate. A classic example of that, to me, is that medical records are currently dispersed and disparate, held in thousands of doctors' clinical management PCs and thousands of pharmacists' prescription recording PCs, and they are using that for purposes of their own records keeping and individual customer service. As you aggregate, match and centralise that data, certainly more issues arise.

Senator LUNDY—We hope to get a chance to talk about those later on this afternoon. Thank you.

CHAIR—Thank you very much, Mr Probert and Mr Aulich, for making yourselves available today and also for the interesting responses you have made to some questions.

[2.30 p.m.]

DANIELS, Ms Helen Elizabeth, Assistant Secretary, Information Law Branch, Information and Security Law Division, Department of the Attorney-General

GLENN, Mr Richard Alexander, Acting Senior Legal Officer, Information Law Branch, Information and Security Law Division, Department of the Attorney-General

MACKEY, Ms Gabrielle Mary, Acting Principal Legal Officer, Information Law Branch, Information and Security Law Division, Department of the Attorney-General

WOOD, Ms Allison Maree, Acting Senior Legal Officer, Information Law Branch, Information and Security Law Division, Department of the Attorney-General

CHAIR—Welcome. I am sure that as senior legal officers each of you knows that the information we seek from you today we prefer to have on the public record, but if any of my colleagues asks you a question that you would like to respond to in private please indicate and we will consider that request. We have before us submission No. 25 which has already been published. Do you want to make any changes to that submission?

Ms Daniels—No, thank you, Senator.

CHAIR—I now invite one of you to make an opening statement, bearing in mind that we are running a little behind schedule today.

Ms Daniels—I will make a few opening remarks so that our submission is seen more in context for the benefit of the committee. The department appreciates the opportunity to give evidence to the committee and to assist the committee with its inquiry. As the committee is aware, the Attorney-General has responsibility for privacy law and policy in the Commonwealth sphere. Accordingly, the Attorney-General's Department has a section devoted to consideration of privacy law and policy matters which is within a division known as the Information and Security Law Division.

While the Commonwealth government keeps a watching brief on broader privacy issues, its focus has been on regulating the collection, use and disclosure of personal information as a major means of protecting an individual's privacy. The Privacy Act 1988 was enacted to implement Australia's international obligations as a member of the Organisation for Economic Cooperation and Development and Australia is a signatory to the OECD's 1980 guidelines governing the protection of privacy and transport of flows of personal data. The Privacy Act sets out 11 information privacy principles in relation to the handling of personal information by Commonwealth agencies. These principles also apply to the ACT public sector.

From the outset the Privacy Act also contained provisions concerning tax file numbers allowing for the Privacy Commissioner to issue guidelines concerning the collection, storage, use and security of tax file number information. In 1991 the Privacy Act was amended to regulate the credit reporting industry, placing restrictions on credit reporting agencies in relation

to the contents and disclosure of credit information and limiting what credit providers could do with their credit reports. For many years this was the only privacy legislation in Australia.

In 1998 New South Wales enacted the Privacy and Protection of Personal Information Act, which regulates the handling of personal information by the New South Wales public sector. In May this year the Victorian government introduced the Information Privacy Bill which, when enacted, will regulate the handling of personal information by the public sector in Victoria. At this point no other state has its own privacy legislation.

As the committee would be aware, in April this year the Attorney-General introduced the **Privacy Amendment (Private Sector) Bill 2000** into the House of Representatives. The bill proposes to amend the Privacy Act to apply information handling standards in the form of national privacy principles to all private sector organisations. Importantly, the Commonwealth's Privacy Act does not distinguish between the protection of personal information collected, used or disclosed electronically and personal information held in the more traditional paper form. The government is of the view that the underlying issues are basically the same, regardless of which media is involved. It is the means by which these issues are addressed which differs. For example, the privacy principle concerning protection of personal information from unauthorised use and disclosure is a bigger issue in the electronic environment, which calls for more stringent security measures.

Proposed amendments that will extend the Privacy Act to the private sector are also technology neutral. They aim to engender a cultural change in Australian society to one where there is more respect for personal information and enable individuals to exercise a measure of control over their information, what information is collected about them, by whom, and for what purposes. We will be happy to explain aspects of this in more detail should the committee want to know more.

CHAIR—Thank you. Senator Harradine, did you want to ask any questions of the Attorney-General's representatives?

Senator HARRADINE—What they have written is clear enough. However, I have one question that is from left field. Could you explain how CrimeNet came into being and whether the Attorney-General's Department has had any input into that decision? And if so, what?

Ms Daniels—We are aware of CrimeNet. I do not know the full background of how it was established but the department has been examining it from both the point of view of criminal law policy and privacy law policy and how an organisation like CrimeNet would fit under the proposed legislation we are referring to. I understand the issue of CrimeNet has been before the Standing Committee of Attorneys-General.

Senator HARRADINE—Could you elaborate as to what occurred at that standing committee?

Ms Daniels—Unfortunately, I am not in a position to explain any further.

Senator HARRADINE—Could that question be taken on notice? Also, could you please advise the committee as to how this legislation that we are considering is going to tackle the problems arising from access to CrimeNet?

Ms Daniels—Yes, we will take that on notice.

Senator HARRADINE—You are not able to explain the latter point to us now?

Ms Daniels—The legislation that is before the parliament now applies to most private sector organisations. However, there are some exemptions, and I think the committee would be aware of some of them. For example, there are exemptions for small business operators and there are exemptions for the media because the government feels that in at least those two areas there are also some balancing considerations to be done in the public interest—privacy versus free flow of information, for example. In relation to CrimeNet and similar bodies, it depends on the nature of the information they collect and whether they may fall within one or other exemption. For example, if CrimeNet were seen to be releasing articles which involved journalistic activities, some of their activities may well fall within the media exemption. That is by way of example.

Senator HARRADINE—In respect of a person who has been found guilty of a crime, and the punishment fits the crime, and after having paid his debt to society, what is the view of the Attorney-General's Department? Should his crime be held over his head forever?

Ms Daniels—We in this area see things from a privacy policy perspective. To fully answer your question it would be of benefit if you would also have the criminal law perspective, and those people are not here today. There is also the spent convictions legislation which might answer what you are referring to.

Senator HARRADINE—I see. There are a number of other questions, but I will wait.

CHAIR—Ms Daniels, the suggestion was made this morning that legislation that we have does not measure up to best practice in the UK, Canada and Hong Kong. Could you respond to that comment?

Ms Daniels—I am generally aware of the legislation in each of those territories. I guess the yardstick from the Commonwealth government's point of view is the relationship we have with the European Union in terms of whether they will give the Australian legislation an adequacy standard when it comes time to look at our legislation. From what I do know, I understand Canada does not yet have the adequacy test from the European Union, nor does New Zealand. I am not sure about Hong Kong.

CHAIR—What about the level of consultation that was undertaken in the development of the legislation? Are you able to outline that for us?

Ms Daniels—The legislation has had a very good history of relevant consultation. There have been a couple of points where there has been extensive consultation, both via the Privacy Commissioner and via the government or the department. The national principles in the

legislation are based on the Privacy Commissioner's national principles that have been out since the end of 1998.

Following the government's decision to legislate for the private sector, the department established what was known as a core consultative group of individuals who represented various sectors who would have an interest in privacy, drawing on business, state and territory representatives, the Privacy Commissioner, and consumer or privacy advocates. That core consultative group played a fundamental role in developing the legislative scheme. Following the completion of the scheme, the Attorney last December released the draft bill for public consultation. We got back some valuable comments following that process, after which aspects of the bill were changed. We have also had up on our web site, since the bill has been introduced, an information paper and various fact sheets covering various aspects of the bill. So I think the consultation has been quite effective.

CHAIR—One of the other comments made by witnesses this morning covered such tracking devices as the use of cookies. Are you able to tell us how you have addressed that in the legislation?

Ms Daniels—I might ask my colleague Gabrielle to explain.

Ms Mackey—The legislation does not specifically deal with the issue of cookies. As has already been said, it is technology neutral and the principles that are laid down apply to personal information in whatever guise, so the same general principles would apply. If you are collecting it, then the rules regarding collection of personal information would apply and in relation to how you use that information the same general rules would apply to cookies as apply to any other form of personal information that you would collect. There is not a specific area of the bill that deals with cookies—just the same principles apply.

CHAIR—I knew there was not a specific area, but one of the things that is already coming through in the evidence we have received so far is the extent to which people are able to discern whether information that they are gathering from one source or another is also being tracked through the sites that they visit. I think you were here when the previous witnesses were talking about the disadvantages facing older people who may not be as familiar with the new technology as young people who have grown up with it through the education system, and the extent to which they may be totally unaware that sites that they are visiting are being used to form profiles of them. I was just interested to know whether you had taken that into account in a broader way.

Ms Mackey—Certainly the principles regarding collection would require that the person be fully informed of what is being collected and how it is being used. With regard to the information requiring a privacy policy or what you are required to tell a person when you are collecting information, you would be required to inform the person, be it by a privacy policy on a web site or some other means, that these are your practices and to give them the opportunity to say whether they want to deal with you or not.

CHAIR—Senator Lundy, did you have any questions for the Attorney-General's Department?

Senator LUNDY—I want to refer to issues that were raised earlier this morning, one with respect to cryptography law to see if you could explain to us what the process would be for an e-commerce company: where they would go to find specific advice about laws relating to encryption in Australia and what level of encryption they could deploy as part of their service offering in the Australian marketplace.

Ms Daniels—I think we would need to take that question on notice because we are not really from a security side of the department, but I can go back to the department and ask the relevant people if they would be able to help you there.

Senator LUNDY—The discussion this morning indicated that certainly the Attorney-General's Department was involved. You are the information law branch. What is the name of the branch that you are suggesting is more appropriate?

Ms Daniels—Security law and justice, I would think.

Senator LUNDY—Would you be able to take that question on notice?

Ms Daniels—Certainly.

Senator LUNDY—Another issue I am keen to explore concerns the implications of the safe harbour agreement between the European Commission and the US and to what degree the bill, as it is currently drafted, satisfies the requirements of that existing agreement.

Ms Daniels—The department has been having ongoing discussions with officials from the EC about the draft bill. I am not sure whether you are aware of it, but the EC did put in a submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs explaining where the view from their point of view was not as satisfactory as it could be. We are continuing dialogue with the officials in the EC based on their submission and responding to the issues raised. Dialogue has been occurring for the last few years and I think it will intensify as the bill progresses through the parliament.

Senator LUNDY—So does it currently conform to the stipulations as described in the safe harbour agreement?

Ms Daniels—I think it is going to be slightly different from the safe harbour agreement because we have legislation and the US does not.

Senator LUNDY—I know, but particularly with respect to Europe and the operation of companies in the European jurisdiction that also operate in Australia, will they have access to that European market in the way that companies that achieve safe harbour for the purpose of that agreement can access the European market and do their business?

Ms Daniels—It will be the government's intention that that is the case.

Senator LUNDY—So they are working towards that level of compliance?

Ms Daniels—Yes.

Senator LUNDY—And what is your assessment of the implications of the European parliament which, it seems, recently narrowly rejected the European Commission's agreement. I guess this is a question of the relationship between the European parliament and the European Commission as you understand the issues at hand.

Ms Daniels—From our point of view we deal with the European Commission and they are the relevant body that you need to satisfy in relation to whether your legislation will be given an adequacy rating. I am not sure that the European parliament actually rejected the EC's proposal in relation to the US. I thought they made comments in relation to the consultation process that was undergone. It is not my recollection that they actually rejected it.

Senator LUNDY—You might take that on notice and clarify that. I think there was a vote just recently where it was not supported.

Ms Daniels—Was that the one at the end of July?

Senator LUNDY—I think so, yes.

Ms Daniels—I think there were some media reports that indicated it was rejected but I am not sure that was, in fact, the case. But we can happily clarify that for you.

Senator LUNDY—Yes, I will look forward to your clarification as will many others, I suspect. Just on a general point, through this hearing today—and I presume there will be more tomorrow—we have been hearing quite a bit about the changes that are taking place in the management of information in the government's hands, in public hands and the hands of agencies in departments. To what degree does your branch involve yourself in the creation of policies for agencies in departments in information management principles as technology progresses?

Ms Daniels—Do you mean in relation to whether our legislative proposals raise issues relating to the protection of personal information?

Senator LUNDY—I guess I am just trying to work out who the agencies and departments have as a resource with which they can consult as these challenges present themselves, presumably on an ongoing basis. You know that some principles are there and I am presuming that you have had some involvement in developing them. Are you available to offer advice?

Ms Daniels—We are and we provide a lot of advice to other departments and agencies on privacy policy initiatives that are drawn to our attention. We also see draft bills which raise privacy or information gathering issues before they enter the parliament. The departments and agencies often go to the Privacy Commissioner at the same time as they come to our branch. We keep in contact with the Privacy Commissioner on initiatives that he has got under consideration from other agencies.

Senator LUNDY—So when the issue about the circulation or sale of the ABN database or the Australian Business Register cropped up, were you consulted by DEWRSB about that?

Ms Daniels—At what stage?

Senator LUNDY—I am asking you if at any stage you were consulted and what your understanding of those circumstances is at this point.

Ms Mackey—We were consulted at various points during the development of the ABN and the ABR regime or system that they were putting into place. We had the understanding that privacy was being built into the system. Subsequently, when the issue was raised and came to the attention of the Privacy Commissioner, we were also involved in it. Once that had happened, it was really more the Privacy Commissioner's area. We were just really keeping a watching brief on it. We were not actively involved in any policy advice as such.

Senator LUNDY—Is it your role to provide advice, for example, on what government databases can be sold or distributed, both within the federal government and externally? Are you consulted actively on that or is there a requirement for agencies and departments to consult with you on that before doing anything?

Ms Mackey—Probably because the act has been in operation in the context of the public sector now for quite a long time and the various guidelines have already been put into place—and I talk about the Privacy Commissioner's guidelines for data matching and for outsourcing—if an agency were to come to us, as they often do, we would say, 'These guidelines are there. You must look at those first.' I suppose then we would be prepared to assist them in any implementation but we would certainly encourage them to use the resources that are already available rather than try to reinvent the wheel every time an agency comes to us.

CHAIR—Can I just reflect on some evidence that has also been given to us during the morning—I do not believe you were here, but you may wish to comment on it—and that is whether or not there should be a public education role for the department, the government and perhaps industry, or a combination of all of them, to offer a greater level of awareness about the opportunities and threats of e-commerce and e-privacy. Do you have any comment to make on that at all?

Ms Daniels—Education and awareness about privacy are definitely key parts of whether the system is going to work, because legislation only goes so far. The government, in making the decision to legislate for the private sector, were very conscious of that issue. They have tasked, from a resource point of view, the Privacy Commissioner to have resources for education purposes.

CHAIR—If there are no further questions, I thank you all very much for coming and giving us your information today.

[2.56 p.m.]

AITKEN, Dr Jane Stace, Assistant Director, Information Policy Section, Department of Health and Aged Care

FERRY, Ms Jane Maree, Legal Counsel (Interim), Australian Medical Association

HAGAN, Mr Philip John, Assistant Secretary, Information and Research Branch, Department of Health and Aged Care

NESBITT, Ms Julia Margaret, Senior Policy Adviser, General Practice, Australian Medical Association

POWER, Ms Prudence Howard, Director, General Practice, Australian Medical Association

QUINLAN, Mr Frank, National Coordinator, General Practice Computing Group

CHAIR—Welcome. We prefer all questions to be answered in public, but if there are any questions that you would like to answer in private, please indicate that and we will consider it. We have your submissions. Would someone like to give some short introductory remarks and then we will have some questions for you.

Mr Hagan—My branch, the Information and Research Branch of the Department of Health and Aged Care, is responsible for a number of key initiatives aimed at achieving better information management in the health sector through the uptake of new and emerging information and communication technologies. In essence, we are working with the health sector to improve the delivery of health care and achieve better quality of care and health outcomes through effective and innovative use of health information. The key initiative we have undertaken is Health Online: a Health Information Action Plan for Australia. Health Online has been developed in consultation with stakeholders as a national action plan for the health sector as a whole. Its production has been guided by the National Health Information Management Advisory Council set up by Australian health ministers in 1999. NHIMAC, as the acronym goes, has representatives from clinical practice, the AMA, industry, the public health sector, consumers and also has on it the federal Privacy Commissioner.

Health Online provides a blueprint for progressing the health information management and information technology agenda nationally. It provides a strategic framework to bring together key stakeholders in the health care system to develop a common vision and sense of purpose. Most importantly, it is intended to be a living document requiring updating and monitoring over time. We have recently held a Health Online summit in Adelaide with a view to updating the document. Key projects arising from Health Online include the National Electronic Health Records Task Force report, standards development, Telehealth, supply change management and, most importantly, privacy. Underpinning all of the work articulated within Health Online is a commitment to ensure that a robust framework is created to protect health information privacy.

As you would be aware, personal health information is extremely sensitive and consumers must be confident that their information is valued and used wisely. Any initiative undertaken in the health information area must ensure that the community's right to privacy as well as its interest in achieving better health is upheld and protected. Unless we get privacy right, the initiatives proposed under the Health Online agenda, including the development of electronic health records, will fail. Consumers and providers will not use a system unless they can be confident that the privacy and confidentiality of sensitive health information is assured.

The Commonwealth is now working with states and territories to develop a national approach to health information privacy protection that will set out the principles and guidelines by which information should be collected and used in accordance with individuals' informed consent. The government's proposed [Privacy Amendment \(Private Sector\) Bill 2000](#) provides a valuable first step in ensuring that sensitive health information is handled appropriately in the private sector. The federal Privacy Commissioner will be developing guidelines to assist in the implementation of the private sector legislation.

In addition, we support the view expressed by a range of stakeholders that separate, national health specific, privacy arrangements are necessary. To this end, a state-territory-Commonwealth working group has been established with a view to developing a single national privacy code to cover personal health information. Furthermore, in the context of the electronic exchange of health information, such as that proposed under the national health information network, we expect that some issues, such as consent arrangements, definitions of user access and so on, will need specific additional legislation. In this case, we would be seeking the support of states and territories in developing parallel legislation to deal with such issues.

However, legislation, while an essential element to privacy protection in the e-health world, is not sufficient by itself to keep information safe and secure. A range of security measures, including audit trails and monitoring processes, will also need to be instituted. This will involve the development of national health sector security standards to ensure that appropriate security measures are in place wherever health information is collected, stored and exchanged electronically.

Likewise, it will be essential to consult with consumers and providers at all steps along the way to ensure that their concerns are adequately addressed and that participation is truly based on informed consent. Ultimately, unless we build a system in which the end users will place their trust, much of the potential benefits from on line technologies in terms of better quality of care and health outcomes will simply not be realised. At the end of the day, we are committed to getting the privacy issues right.

CHAIR—Thank you. Mr Quinlan, have you any brief comments?

Mr Quinlan—Yes. Just to make members aware, the General Practice Computing Group has been established as the peak national group to represent general practitioner interests in relation to improved information management and technology, and it is some 18 months old. The General Practice Computing Group has a membership of general practitioners and was established by the major general practice organisations. Our management structure and secretariat, which is now funded by the Department of Health and Aged Care, has as representatives the Australian Medical Association, the Royal Australian College of General

Practitioners, the Australian Division of General Practice and the Rural Doctors Association, along with representatives from the Department of Health and Aged Care, the Medical Software Industry Association, health consumers, the General Practice Partnerships Advisory Council and the Health Insurance Commission.

Our principal work has been to establish a strategic framework and an implementation plan to move forward on improved information management and technology in general practice, and this has been part of a two-year program. I am happy to present to members a report on our first year of activity and make that available to you to review the detail of that activity.

In very brief summary, the major areas of activity that the General Practice Computing Group has focused on have been twofold. Firstly, it was clear to the management committee of the General Practice Computing Group that computerisation and improved information management was proceeding at a massive rate in general practice. The aim of the group was to support that work with the sort of practical assistance that GPs would require in order to implement good policy on the ground. While doing that, the group has also had an interest in developing standards for information technology across areas such as messaging, data modelling and electronic health record architecture to enable the interoperability of various computing standards in this area. Security and privacy standards are obviously one of the essential components to general practice computing systems.

Again, summarising briefly, any of these standards will have implications across general practice, and some of these implications will increase as the technology becomes ubiquitous. They include a range of issues that I would be happy to detail in relation to the implementation of various hardware platforms that might be required; the implementation of various software that would be required of general practitioners; the implementation, importantly, of controls of the physical environment in which general practice computing systems are working; and, importantly and as highlighted in earlier submissions, the education and training that general practitioners will support to participate securely in these kinds of programs. The General Practice Computing Group is working collaboratively with the Commonwealth and the various GP organisations to ensure that GPs are well placed in relation to the implementation of these activities.

Ms Power—The AMA is pleased to accept the invitation to come and talk to you today. Particularly in relation to e-privacy, we have quite a few comments we would like to make. You have probably been aware as members of this committee that we have been quite vocal over recent months on the issue of electronic health issues, particularly as they relate to privacy.

There are three key and topical areas in which we have been directly involved in consultations to varying degrees. The first area is the National Electronic Health Records Taskforce report that has been referred to earlier. It may be called *HealthConnect*, as I think there is some issue around the name at the moment. The second area is the Better Medication Management System, BMMS. We have been participating in the development group, the privacy subgroup and will be participating in the technical working party when it gets up and running. The third area is the proposed legislative arrangements for improved entitlement monitoring which will legislate a requirement for inclusion of an individual's Medicare number on PBS prescriptions.

I will detail how they are linked but, before I do that, it is very important right at the outset that you realise the AMA's view on electronic health information systems. We are quite clear of the benefits that can be derived from electronic health systems and the contribution that such systems can potentially make to improve health outcomes both at the individual level and at the broad community level. In this context, it is also important to be aware that GPs are making great strides, particularly with the contribution of the GP Computing Group, in taking up the new technologies.

It is true to say, however, that there are some areas of resistance. These relate to concerns that protection of the ethical and philosophical basis of the profession is central to any and all electronic health information systems. That is why the AMA has maintained the view that overarching health information privacy legislation is an essential precursor to the development of electronic health information systems. I believe the National Electronic Health Records Taskforce supports this position, but I am not sure that it is supported in all other areas of the department. So while our concerns about health privacy are numerous, it would be true to say that our overriding concern is the piecemeal manner in which privacy, in the context of electronic health records, is being addressed, particularly through proposed legislation.

There are three related initiatives currently being developed in the Department of Health and Aged Care, and so far each one of them appears to involve separate legislation or legislative amendments for implementation. Firstly, there is the proposal for the BMMS, the Better Medication Management System. It incorporates the development of specific legislation and provides a drafting and consultation period of only two months. Secondly, there is the Electronic Health Records Taskforce report, or *HealthConnect*, which will require specific health information privacy legislation and which we assume will cover all aspects of e-health, and possibly even involve the states. The legislation component of this timetable is around two years.

Thirdly, the improved entitlement monitoring system for the Pharmaceutical Benefits Scheme is already at the stage of drafting of legislation. It represents an amendment to the Health Insurance Act and addresses privacy issues in a somewhat superficial manner in the view of the AMA. I say 'superficial' because this initiative will have enormous privacy implications as it is integrated into the Better Medication Management System.

Finally, there is the electronic health records system. The reality is that although this initiative is being established under separate legislation, it is linked to the Better Medication Management System. Basically, it represents the establishment, we believe by stealth, of the unique patient identifier for the Better Medication Management System and the electronic health records systems. The draft health legislation amendment—it is called Monitoring Pharmaceutical Benefits Entitlement Bill 2000—paves the way for the Better Medication Management System to legitimately include the Medicare number in operation of its system by prescribers and suppliers. This legislation would give the authority for the Better Medication Management System to incorporate the Medicare number and, as such, the system also becomes an entitlement monitoring system, as well as being linked to a vast array of data which is not relevant to that purpose, in our view.

There is no doubt whatsoever that the Better Medication Management System will become incorporated into a wider electronic health records system, and so it should, but it is unaccept-

able that by sleight of hand the unique patient identifier will already be there, the legislation in place to cover it, and the link made between prescribing information and a vast array of other information, all in the absence of real public debate. It is not the fact that the Medicare number should be a unique patient identifier, it is probably quite appropriate, but not without public debate. The fact of separate legislation will not prevent the linkages, in our view, but it will, we believe, ensure that function creep can occur.

It seems completely illogical and highly inefficient to be pursuing separate privacy legislation for each initiative, particularly given that all these initiatives will ultimately be integrated into a national electronic health records system, HealthConnect. These initiatives commenced first in medication management, and should not be dealt with in such a way as to hamper the longer term development of the electronic health record.

The AMA believes that the government must drive the agenda on the new technology. In our view, however, there must be a consistent approach to the establishment of building blocks for health information technology, with privacy issues as central. There is ample evidence from overseas, and increasingly from Australia, that if we do not get the privacy issues right, this can have a direct impact on health outcomes. The community is becoming more and more aware of the importance of privacy in relation to their individual health information, particularly as industries increasingly seek to use this information to make decisions on individuals' access to services and resources, basically providing the capacity to actively discriminate on the grounds of current, and even more frightening, potential health status.

Preliminary market research undertaken for the Better Medication Management System already indicates that consumers are highly suspicious. Consumers still remember the Australia Card. A Roy Morgan survey in July this year, commissioned by the AMA, revealed that 66 per cent of consumers would not consider their records safe if maintained and safeguarded by the federal government. The printing of highly confidential individual identifying numbers for Centrelink customers on the outside of envelopes, in conjunction with names and addresses, has been reported in the press today. Not only does this incident highlight the consequences to individual privacy, where rigorous standards and protections are not maintained, particularly around unique identifiers, it also contributes to declining community trust, and we do not want to see that happen in respect of e-health.

To say that there is a lot of work to do in the area of public confidence in relation to privacy and electronic health record systems is clearly an understatement. It is in this context, for example, that we continually question the government's timetable for the Better Medication Management System that has parallel legislation drafting and a consultation phase of just two months. It is the AMA's view that the benefits that we want to see derived from electronic health information may not be fully realised if the community's level of suspicion is not addressed through careful and comprehensive attention to privacy issues. The failure to address privacy in a manner that satisfies the community will doom the initiatives to failure, and we do not want to see that. In trying to establish critical elements of an electronic health record, such as the unique patient identifier, in a piecemeal way through strategies that bypass public consultation and debate or that do not expose the inevitable linkages between each initiative will result in a consumer backlash against the electronic health record system.

The fact is that getting highly sensitive issues like privacy right takes time and not only involves the complex areas of consent but also access to technological factors, including technical security. There is also another important point here: implementation timetables also have to address the pace of technology take-up in the health sector, particularly at the GP level. GPs, in particular, I believe, are eager to realise the as yet unimaginable benefits of e-health systems. The capacity to share patient care information with other medical practitioners and the benefits to patient health outcomes are eagerly anticipated. A rigorous privacy framework with consent as central and reliable technical standards, including security, can protect the ethical requirements of the profession. But what is common to both GPs and consumers—that is, their patients—is an overarching concern that the privacy of an individual's health information is protected and that the information they provide is not used in any form, identified or deidentified, for anything other than clearly defined health purposes, which could include research. The AMA, for example, would oppose the use of any data gathered through an electronic health information system for any commercial or commercially related purposes. With appropriate privacy protection, we do see the value for defined uses in health policy and planning.

In conclusion, the AMA's view is that it should not support electronic health information system initiatives which do not place privacy as central to the operation of the system. We are concerned at the piecemeal approach to privacy legislation and the numerous smaller initiatives that are being developed in isolation from one another, particularly in isolation from the larger *HealthConnect* proposal. Arguments that these initiatives stand alone are simply not true. They will ultimately be an integral component of the broader *HealthConnect* and in our view must be subject to the same stringent establishment of the essential building blocks, with privacy as a highest priority. It is not the AMA's intention or desire to thwart what in principle are excellent concepts that could benefit the objectives of the medical profession for the highest quality care to be reflected in patient health outcomes. It is the AMA's intention, though, to ensure that these initiatives work. In such a sensitive area as health information, enabling technology alone offers no assurance of success. I conclude with those remarks, and I am happy to follow up with a written submission.

CHAIR—Thank you very much. Perhaps I will kick off by asking a question of either Mr Quinlan or Mr Hagan. One of the concerns related to me about privacy and having health online is the overprescribing aspect of people who go doctor shopping. I am just wondering whether the linking of doctors online is going to enable greater crosschecking of people who do go from one doctor to another and who in fact often collect prescriptions quite prolifically?

Mr Hagan—I do not work in the Health Insurance Commission, but I will relate what I know. It is a medication management thing; it is not about doctor shopping. It is about preventing adverse health outcomes for people who may be on medications that, when taken simultaneously, interact badly. It is not the intention to use better medication management other than for individuals and their health.

CHAIR—I am sure that is a priority for all of us. Nevertheless, the question has to be asked to the extent that these people consider their own health when they go from one doctor to another getting the same prescription. My question is focused on whether going online is going to enable doctors themselves to have access to whether or not these individuals go from one to three, four or five doctors getting the same sorts of scripts, or whether the doctors are going to

be able to get access to that patient's information in a way that will assist them to enhance their health by not overprescribing.

Mr Hagan—Maybe I should point out something else: the intention is that the whole thing is voluntary. If a consumer does not want the doctor to find out what other medications they might be on, they do not have to participate in the scheme. It is voluntary for both providers and consumers. But if the consumer does say that they believe a provider ought to know what their medication record has been, then the whole idea is that the doctor could see what other medicines they were taking and possibly be alerted to possible adverse interactions, or would just know it or be able to see it. So, yes, that is highly relevant information that it is in the interests of the consumer that the provider knows. The problem at the moment is that the poor old doctor most of the time would not have a clue what other medication a person is on and would blithely go ahead—

CHAIR—Hence my question.

Mr Hagan—and prescribe this thing and inadvertently cause a bad outcome.

CHAIR—I raise the question based on the doctor's duty of care as much as the patient's duty of care to disclose the information, but very often that is not something that the patient is willing to do. The doctor is much more likely to be aware of the health contraindications of any prescription if they have access to that data.

Mr Hagan—Absolutely.

Mr Quinlan—That is particularly the case where care is handed from one setting to another. For instance, when patients leave hospital and often return to a GP, under the current system the GP is largely going to be unaware as to the medications that may have been prescribed in the hospital setting; and vice versa, when the patient moves from the community into a hospital setting, the hospital is just as likely to be unaware of medications prescribed in the community by the GP. As Phil has suggested, these initiatives will certainly capture duplicate prescriptions where that is not in the interests of the patient.

The proposals to date, though, would not capture those systems where the patient is intentionally trying to keep the duplication of those scripts from various medical providers, although the scope would be there, technically at least, for various organisations such as the HIC to potentially use the information that is gathered as part of these other systems that are providing for quality of care. That is the main concern around separating out the intentions for use of data right from the outset.

CHAIR—Thank you.

Ms Power—I would like to give a clarification. The Better Medication Management System, as the others have pointed out, is proposed to be an opt-in system, so presumably doctor shoppers would not opt in if they did not want that to be shown up. It certainly will benefit prescribing because doctors should have access to a wider breadth of information on medications that might have been prescribed by other people. It will not, at least in the first

instance, assist with information from hospitals or any other areas; it does not intend to include that in the first instance.

There are a number of issues around informed consent that have to be dealt with, so it is not as simple as just a patient opting in or a pharmacist opting in or a doctor opting in. There is not a lot of understanding about what might happen if, for instance, only two of those participants opted in at this stage—say, the pharmacist and the patient, but not the doctor. There is uncertainty about how the information might flow if the doctor did not opt in. So, although I hope it is going to allow the doctor to have access to wider information, there are a lot of difficulties to overcome first.

Senator LUNDY—To what extent in Australia in these three tiers of activity has there been involvement of private sector dot.com companies in providing innovative solutions? Having recently looked at some of the approaches in Europe, Canada and the US, there is quite a presence of dot.coms pitching up to government departments and agencies offering a solution. How much of that are you experiencing as part of the health establishment in this country?

Mr Hagan—Certainly that is a true statement. The number of solutions to whatever your problems are out there is legion. The role of government there is to say what the rules of the game are. The Electronic Health Task Force Report, for example, identifies the problems we have to solve: privacy, standards, safe patient identification. It lays out the things that it is in the public interest to solve for the whole nation. After all, there are only 19 million of us. That is what Health Online is all about—trying to get us to roughly row in the same direction, to use the same standards. It was encouraging that health ministers, when they saw this report, unanimously said, ‘This is the way we should go.’

That said, if *HealthConnect* is to come into existence—and we have to debate that yet—a lot of the design work is still ahead of us. Privacy is a good example. The health ministers said, ‘We want all the jurisdictions to get together and say, ‘These are the sensible rules and we can all agree on that and we will enact them in parallel, if necessary.’ One of the rules of *Health Connect* might be that you cannot be part of it unless you have signed up to the privacy code. You cannot be part of it unless you can conform to these standards, including security standards. That is the way something like *HealthConnect* can sensibly advance. On NHIMAC, that is the advisory council, the private sector is represented. They look to government to say what the rules of the game are. Then they will be able to come forward with their solutions, knowing the sorts of hurdles they have to jump over, including what sort of privacy regime they must comply with.

Senator LUNDY—Reflecting on earlier evidence—I have tended to do that all day because the issues overlap so strongly—there seems to be a distinction between information management, where it is strategically controlled and managed by those within the agency and the department, that is, the public servants and those who effectively outsource that strategic control and management issue. When that is managed in-house obviously the infrastructure and so forth has been outsourced to quite a prolific degree. Everyone seems to have indicated the deficiencies in the current privacy bill. There would need to be something far more strident and explicit relating to health. But even with the best-case scenario legislation relating to health, is there a view amongst you that it needs to be something strategically controlled by those with the statutory responsibility for that public information? Or can that effectively be outsourced by

virtue of a tight contract?—which, quite frankly, is how it has been approached in many other jurisdictions. Has a lot of concern been expressed about that?

Mr Hagan—Part of the answer comes back to trust: will patients trust a system that is not under tight control by government? I suggest that probably a lot of people would say no. You will get quite a variety of answers on the trust question. The task force that put this together had a view that the best thing would be for government to run it, not necessarily to operate it, but to run it, and also to have an independent access control authority. If somebody says what the rules are, we have someone—

Senator LUNDY—It is a separation of powers approach.

Mr Hagan—Yes, a separation of powers. If there is a disclosure, deliberate or otherwise, it goes then to the access control authority who will offer redress, because none of these systems are perfect, we know that.

Senator LUNDY—I have a question concerning who has a vested interest in this. This is always a question I am curious about, particularly with regard to the AMA. In entering this debate as an organisation representing your members, are you aware the degree to which any of your members have an active interest in potential private providers—as directors of dot coms, for example—that are offering perhaps one of the range of solutions available for a health service online?

Ms Power—We are aware certainly of people in the medical area, some of whom would be members and some of whom would not be, who are setting up companies to provide health information online, or maybe even to encourage an interaction between doctor and patient online. When it comes to the full electronic health record for the population of Australia, I am not aware of anybody who is contemplating, other than government, setting up to manage that.

Senator LUNDY—No, but it is a question of architecture because in terms of building that sort of underlying database, where the innovation can actually occur is in how you access that underlying database. I am interested now in terms of the range of models that the government is contemplating and the range of interest, though not necessarily from the AMA, amongst others. I mean everyone out there with an interest, private health insurance providers, et cetera. They are all part of that bag of what I would consider people who could potentially have active vested interest in not having a ubiquitous application that actually accesses that data and is available to GPs and everyone else who is a health service provider. Do you see what I mean?

Ms Power—Yes. The options for the structure of the database are being heatedly debated right now. There is not yet an agreement whether it should be distributed, totally decentralised or centralised, or somewhere in between. It is highly likely that it is going to be somewhere in between.

Senator LUNDY—But you would agree that that architecture and its nature is an absolutely critical factor in determining, I guess, how it is accessed, and hence privacy implications?

Ms Power—It is a totally critical factor. It is one of the reasons why we are having difficulty dealing with the speed with which the government is approaching the Better Medication

Management System because these very crucial issues have not been finalised, they have not been agreed.

Senator LUNDY—It works both ways. If that underlying architecture is determined, it could, depending on its nature, close off opportunities for innovation for service provision on top of that database and, equally, depending on its nature, it could open up a vast range of opportunities?

Ms Power—Yes, that is why it is extremely important, as all of us are saying exactly the same things, that we must have very strict protocols and rules around privacy, access and consent. Then, if we have those in place, as technology evolves, the structure of the database will also probably evolve. The AMA is saying that we would prefer a distributed database system and that we do not really support a centralised system. However, given that there are already some centralised databases, such as the PBS and MBS, we are not advocating that they be dismantled. What we are advocating is that within the system we do not set up new databases where there is no need to have them and we do not widen access beyond where the real need is. This is probably fairly well identified now when a patient sees a doctor and that privacy is maintained when the patient is referred or other information is given out. Does that answer that? There is a lot more I could say about that.

Senator LUNDY—Yes, it does. I appreciate that this is a discussion. I know the process through which you actually make decisions about the nature of it is very controversial and the Labor Party has had a lot to say about it and all the rest of it. For me, it is the relationships between the policy, the architecture and the nature of the hardware in the databases that are so critical in the decision making process here, because their nature predetermines, to a large degree, what sort of privacy management system we can lay across the top.

Ms Power—Or vice versa.

Senator LUNDY—Or vice versa, yes.

Ms Power—Probably vice versa.

Senator LUNDY—Or what the potential model of providers is and whether or not a range of interests can get access to that and under what terms and conditions.

Senator HARRADINE—I think that has been a useful discussion. From what you have said, it seems to me—and correct me if I am wrong—that the [Privacy Amendment \(Private Sector\) Bill 2000](#), if enacted, will be inadequate to allay the concerns of the AMA and perhaps the concerns of others as well in relation to the BMMS, for example, or the proposed health record system. Am I correct in assuming that?

Ms Power—Yes. What we are saying—

Senator HARRADINE—Could you say, in truncated terms, just precisely in what area and how?

Ms Power—I do not believe that the **Privacy Amendment (Private Sector) Bill 2000** is strong enough in the e-health area and, as I mentioned before, legislation that is being developed in the e-health area is being developed with a piecemeal approach.

Ms Nesbitt—One of the key issues is that it has not been developed in the context of electronic health issues. I think even the specific inquiry into that identified a lot of the problems that the AMA had with it and agreed with those problems.

Mr Quinlan—With both the National Electronic Health Records Taskforce and the Better Medication Management System people have recognised and acknowledged the need for specific legislation in relation to personal health information, particularly legislation which details quite precisely the purposes for which the data might be used and also explicitly details exclusions as to how that data might be used. I think the need for that quite specific legislation in relation to personal health information is widely acknowledged.

Ms Power—That is identified and de-identified data. We are not really confident that the meaning of de-identified data, the point at which data could be re-identified and the purposes it could be used for are well understood. Just because it is de-identified that does not mean that there is *carte blanche* about how it could be used.

Senator HARRADINE—Does the department have any comment on that?

Mr Hagan—Australian health ministers discussed this subject when they met in July in New Zealand. They proposed, as I mentioned in my statement, that the various jurisdictions get together and see if they could work up what is called the health code, which would sit either in parallel or under the Privacy Act as it stands at the moment because e-health does raise some issues. The bill, as it sits, is across the whole economy. Although it has been tweaked for health, health ministers would like some further work done to see whether something can be shaped that is much more specific to the health sector, given the nature of personal health.

Senator HARRADINE—Would you see any constitutional problem in national legislation in respect of e-health? Do you see that the Commonwealth parliament may not have the constitutional head of power upon which to base such an approach to e-health?

Mr Hagan—I am no constitutional lawyer, but going back a year when this private sector bill was being mooted, health ministers decided that they would wait and have a look at it. In Australia the Commonwealth has the Privacy Act and some of the states and territories do as well, so if you want a uniform privacy regime to apply across the whole of Australia then the private sector was the very large sector that was not covered at all. Then there are the state and territory jurisdictions as well. The express wish of health ministers was to have as near as possible a uniform privacy regime for health. They looked to that bill at that stage to see whether that could get them closer to that objective. If that bill were to pass we would be almost there. The only thing that would not be covered would be the state and territory agencies. It was in that context that health ministers said: 'If we could agree on a code then perhaps the jurisdictions could sign up to that and thereby get uniformity across the whole of the country.'

Senator HARRADINE—Could you take on notice the issue, as you see it, of whether national legislative action should be taken and whether that could be based on the corporations

power and the communications power in this instance. That is one point. Perhaps I should have asked the Attorney-General officers this but no doubt you—

CHAIR—The Attorney's witnesses are still here so perhaps they could take it on notice if you raise it with them.

Senator HARRADINE—The AMA may not feel confident that health ministers arrive rapidly at a common conclusion about matters. I refer to the urgings of the National Health and Medical Research Council to have common legislation in the states and territories on the IVF matter, for example—since that is topical. They made that recommendation in 1996, I think it was.

Mr Quinlan—There is certainly an intention to introduce legislation to deal specifically with the better medication management system. I believe a draft is due to be circulated in September or so on. The connection between that legislation and legislation that may be required for the electronic health records task force is not yet clear. I do not think it is clear either what the links are between that legislation and any legislation that may also be required in states and territories in order to fully implement that regime of protection.

CHAIR—I thank the panel of witnesses for their helpful answers to questions and for agreeing to take some questions on notice.

[3.45 p.m.]

EARLE, Mr Terry Leo, Acting Chief Executive Officer and Business Development Director, Australian Retail Group

CHAIR—We now have a teleconference with Mr Terry Earle from the Australian Retail Group, and I apologise to Mr Earle for the difficulties that the committee had this morning when fog closed the airport and prevented us having a quorum.

The committee does prefer that all evidence is given in public but if at any time a question is asked of you which you would like to respond to in private, please indicate that and the committee will consider it. I should also remind you perhaps that any evidence given in that way could subsequently be made public by an order of the Senate. The committee has before it submission No. 2 which has already been published. Are there any changes that you wanted to make to that submission?

Mr Earle—No.

CHAIR—Would you like to now make some opening remarks and at the conclusion of that statement we will have some questions for you? I should say that we are a bit tight on time because people need to leave to catch aircraft so I will ask you to keep your opening remarks as succinct as possible.

Mr Earle—I guess I was invited to put a submission in following a paper that I presented at a conference in early July. As a result of that I was asked to comment on and to submit a position that related to rewarded loyalty programs, which is really the basis of my submission. Essentially it was to make a clear statement as to why these programs are basically being run and the need to have adequate access to the information that is currently captured, but at the same time recognising the rights of privacy of the individual.

Senator LUNDY—I was interested in the degree to which your association actively monitors the use of data mining for the purposes of marketing or other uses amongst your membership.

Mr Earle—A lot of the data mining that we do is at a high level which is at an aggregated level which, if I take a shopping centre program as an example, effectively enables us to do demographic analysis. So what we are able to do as a result of registering our clients who then shop within the program is find out where they come from, what their age groupings are and so on. So essentially in this case the shopping centre that was the owner of the program—the custodian of the customer records—used the data primarily for high level marketing and demographic analysis and then specifically for invitational and promotional mailings to the customers. It really is at that level and that sort of program that they are trying to build more custom for their shopping centre and get more value, obviously. So the direct marketing channel of knowing who these people are and how they react is very much the flavour of how they actually make the promotions.

Nobody else has access to that information. So the owner of the shopping centre in this case drives the extent of the program and the use of the data. At the personal level, that data is not made available to any other third party. In the case of the coalition loyalty programs, which we run, where you have many retailers party to the one program, we protect the data of the consumer level by outlet of the retail groups. That means that if the retail outlet recruits the member to the program, basically they are the owner of that data and nobody else gets that data in a form that they can use for any other purpose, other than the reward program.

For example, if I have a pharmacy and I sign up 300 of my customers to a coalition program I have proprietary right as the pharmacy to that data. We provide that data to the pharmacy as and when required or we may embark upon a marketing program, which might be a mailing or some other program which uses that data on behalf of the pharmacy, but with their permission. If, however, a customer who has been signed up by somebody else in the program comes into that same pharmacy, that pharmacy is able to communicate with that customer, but it never at any stage gets access to the data for its own use, other than specifically for the promotional purpose. Basically it goes to a third party mailing house, as opposed to being delivered in a form that the outlet could take a copy of and keep that data.

Senator LUNDY—You are familiar with the proposed legislation in the area of privacy for the private sector?

Mr Earle—I am not really au fait with it. I have not studied it at length.

Senator LUNDY—Perhaps the best way to deal with that is if you could take on notice a question to cross-reference the business practice of your members with the provisions of the proposed bill. That would be interesting information for the committee. With respect to the third party mailing house, the sort of clearing house you described, obviously personal names are a part of that. In aggregating that information and then giving it to coalition participants, it is a question of integrity as to how you go about it. To what degree can you verify to coalition participants the accuracy of your information? Or is that they are buying a service that they have to take at face value, but you never let them have a look at your consolidated database?

Mr Earle—The reality is that it is like any database that changes in time. I do not know what the exact statistics are, but about 15 per cent or so of households move in one year—it might even be greater than that. There is always part of the database that is not absolutely right. If you are asking me how I reassure the participant organisations that their data is not misused, an audit could be undertaken by them at their request. Alternatively, we would be in breach of the obligation we have in terms of our contractual arrangements with them, and they could take action against us.

Senator LUNDY—The most public example of a large data warehousing outfit was the reported incident relating to Acxiom. To what degree are those really large central data warehouses critical to you providing your services and your members doing what they do? Are the databases from which different organisations draw or data mine information about given markets becoming more and more centralised?

Mr Earle—If I forecast what is going to happen in the future, it is that the role of companies like Acxiom is to take data from many disparate sources and effectively mine that data into a

meaningful output as determined by their clients. There is no doubt about the sophistication that is required to be able to do that. If I am talking about taking transaction data that relates to participants in our program and trying to predict what the consumer might do as a result of that data, then clearly that is an area of expertise for organisations such as Acxiom. What that then does is move the output of that data into a format that goes back to, if you like, a member of our program which says, 'I want to target those people who might be early technology adopters with an offering that they are likely to accept.' It is statistically based and behaviour based. They will play a key role in doing that. That is their business.

Senator LUNDY—To what degree is the practice of silhouetting profiles by, for example, establishing those comprehensive profiles on people or families but without actually having their formal identity attached to them forming a part of the services you offer? Is there any use in doing that in doing market research or is it focused on being able to contact them personally?

Mr Earle—Not for us. The reality of what we do is based on transactional history and data. From our point of view it is not predictive.

Senator LUNDY—Have you ever done any research to what degree participants in your programs are aware that their data is cross-referenced and distributed amongst other organisations or businesses?

Mr Earle—Our programs have only been running just over 12 months. Each of our participants is acutely aware and conscious of them protecting that data in a proprietary way. I can give you an example of that. Guardian pharmacies are a partner to one of the programs. Information that is held at one Guardian pharmacy is not allowed to be given to another Guardian pharmacy.

CHAIR—You have worked in one of the major banks for many years. I am interested in the degree to which banks use information on transactions and people's spending patterns to perhaps better inform themselves about the use of some of the bank's products or, in turn, better inform organisations with which they may be affiliated. Can you make any comment on that in a general sense?

Mr Earle—In general, banks have underutilised that information. They have built very sophisticated systems to deliver transactions from point A to point B but never mined the data in terms of tracking it back to a consumer or a business outlet. When I was running the credit card division for ANZ we were looking at ways in which we could generate more revenue from business. That was one of the ways that was identified, but it was never adopted.

Today they do a little more than that, mainly because they now have some reward programs associated with them. They tend to do that through the reward manager. Effectively, in the case of the Telstra Visa card program, for example, the organisation that manages that program—Pin Point Marketing—gets all of the transaction data and is able to look at that and profile customers. To the extent that the banks then take that data and target offerings, my own experience is that it is still at a very minimal level. There is a great deal more potential for where it could be used but it does not seem to be used successfully or widely to date.

Senator HARRADINE—Has there been any attempt, to your knowledge, at hacking into your consumer databases?

Mr Earle—Not to our knowledge. In our case, we do not have any of the data online to consumers or retailers at this point. That becomes an area that needs to be managed from a security point of view when we move into the environment of providing that access via the Internet. At the moment, effectively the data is really quite restricted in terms of who can get access to it.

Senator HARRADINE—Do you anticipate problems? If so, what steps have you taken to anticipate them and ensure security?

Mr Earle—It is effectively an issue that is evolving all the time with technology. What I can say is that, at the end of the day, we have to satisfy ourselves that we have put in appropriate security measures before we implement those things. If we talk about security that was available five years ago, the reality is that that is readily hacked in and breached today because, as quickly as you put in some protection, there are minds greater than ours working at trying to break those protections. So it is a constant thing.

From the point of view of the programs that we run, we do not carry personal financial data. We might carry transaction data, but we do not carry information like salaries or value of assets or any of those sorts of things so there is less issue or exposure in terms of the value of the information to a hacker. The value is probably being able to get names and addresses to do marketing, but that would need to be at an orchestrated level.

Senator HARRADINE—Thank you, Mr Earle.

Senator CALVERT—I have been an ANZ bank customer all my life and a great user of credit cards.

Mr Earle—I have been gone from ANZ for about eight years now so I need to be careful about being characterised that way.

Senator CALVERT—I am going to ask you a question that probably has nothing to do with this. Just how safe are credit cards, particularly now when there is wider use of giving your number over the phone and the probability of giving it over the net? Just how secure are they?

Mr Earle—The net created some other problems of security with credit cards which were really about organised crime replicating multiple credit card numbers and putting through transactions. As I understand it, that really came out of North America and Asia, where there was less control about the merchants who could register to be part of Mastercard or Visa card schemes and who could then effectively put into the system fraudulent transactions which would not be discovered until they hit a cardholder's account, the cardholder objected and they were found out.

In Australia, the fact that the banks by and large control all of the merchants means that there is significant protection in this country against that. That is not to say that there are not occasions when it is breached; and certainly the Internet has created opportunities for breaches

that the banks are very aware of and are taking steps about all the time. At the end of the day, the bank takes the risk. The reality is that the cardholder is protected for transactions that they do not authorise. My sense is that that is the protection. The banks and organisations like Visa and Mastercard spend significant sums of money to ensure that the security is appropriate and it is constantly being upgraded and refined. So we are fortunate in Australia, but we are now living in a global village and that is being undermined all the time. But on the Internet, I understand, it is primarily due to the controls that relate to those merchant organisations that are authorised to accept transactions.

Senator CALVERT—When you give your card number over the phone, is that more secure than the way the Net is operating, or is it a similar type of security?

Mr Earle—The Net is probably a little more secure than the phone.

CHAIR—Thank you very much, Mr Earle. We do appreciate the submission that you have given to us and the questions that you have answered today.

Committee adjourned at 4.05 p.m.

