COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

Reference: Privacy Amendment (Private Sector) Bill 2000

FRIDAY, 2 JUNE 2000

SYDNEY

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

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**

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

Friday, 2 June 2000

Members: Mr Andrews *(Chair)*, Mr Billson, Ms Julie Bishop, Mr Cadman, Mr Kerr, Ms Livermore, Mr Murphy, Ms Roxon, Mr St Clair and Mrs Vale

Members in attendance: Mr Andrews, Mr Cadman, Mr Murphy and Ms Roxon

Terms of reference for the inquiry:

Provisions of the Privacy Amendment (Private Sector) Bill 2000.

WITNESSES

Committee met at 9.44 a.m.

DIXON, Mr Timothy Edwin, Chairman, Australian Privacy Foundation

CHAIR—Ladies and gentlemen, I declare open this public hearing of the committee's inquiry into the Privacy Amendment (Private Sector) Bill 2000. I welcome all the witnesses and members of the public who may attend here today. This bill was introduced into the parliament on 12 April and referred to the committee by the Attorney-General for inquiry. He has asked that we present a report back to parliament in June.

The purpose of the bill is to amend the current Privacy Act and to set up a national framework for the collection and use of private information by private sector organisations. The bill proposes to implement the national principles for the fair handling of personal information. Those principles were developed by the Privacy Commissioner following consultation with business and other interests. I understand that our first witness this morning took part in the consultation process with the Privacy Commissioner and with the Attorney-General's Department.

Mr Dixon, I should advise you that although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves, and the giving of false or misleading evidence may be regarded as contempt of the parliament. We have just received your submission. Can I ask you now to make a brief opening statement.

Mr Dixon—Firstly, my apologies for the very late submission; there have just been some extenuating personal circumstances. I think many of the concerns which the Privacy Foundation has with the legislation, and much of the feedback, has been fed through to the committee. A number of the submissions which have been made are from members of the Privacy Foundation, but there are some other issues which are highlighted in our submission.

The background to the Privacy Foundation is that it was the organisation formed to conduct the campaign against the Australia Card back in 1987, a galvanising event in terms of community attitudes towards privacy issues. I have been involved with the foundation for most of that time. The development over the last seven or eight years has seen the privacy issue—which back in the late 1980s, early 1990s, tended to be more focused on public sector issues—extended now to the private sector. That is partly a reflection of the changing role of government and the fact that a lot of personal information which was once in the public sector is now handled by the private sector, and also due to the explosion of new technologies which raise issues which were not there 15 or 20 years ago.

Broadly, we welcome the legislation and the government's initiative to move ahead with the extension of the Privacy Act to the private sector. We have supported that position for a period of about 10 years and have felt that Australia has lagged behind other countries in establishing a consistent way of protecting personal information. There are, however, a number of weaknesses in the legislation which we highlight. I guess the most efficient use of time is for me to focus on those areas where we see there could be improvement.

There are several areas of the legislation which are, in our eyes, surprising by any international standard. There is the extent, for example, of the exemption for employee records; the extent of the exemption for small business; the drafting of the wording for the exemption for the media; and the exemption for political parties. We look around the world and feel that those are not justified by any unique circumstances in Australia, pragmatically speaking. I guess in many ways they are the result of particular political circumstances here, but we urge the parliament to reconsider some of those. Possibly looking at it realistically, our position is that those exemptions are largely unnecessary, although there are some specific issues which could be covered under the specific principles, issues like the access principle, for example. Broadly, we do not think that those exemptions are necessary. However, given that the political realities might be that we do not see those removed altogether, we would urge the parliament to focus on the specific issues which are a cause of concern.

For example, in relation to the political parties exemption, if indeed the main concern there is about the way in which privacy legislation may be used to obstruct the political process during an election, the best way of dealing with that is to address that through the access principle to provide an exception to that principle, rather than providing a blanket exemption to the political parties' coverage. I highlight that issue in particular in the submission because it has not been covered so much in other submissions and because I know that it has probably a greater degree of cross-party support than a number of other aspects of the legislation

I have real concerns about the political party exemption. I think that fundamentally we live in a time when there is tremendous suspicion and cynicism in the electorate towards elected representatives, much of it unfounded, but measures such as creating a different set of rules for the political leaders and political parties than there is for the rest of community are going to entrench that cynicism. I cannot see a justification for it. I think that some of the uses of personal information by political parties, as they are rapidly changing and being imported from some of the electoral practices in the United States, raise serious privacy issues. Some of the most serious privacy issues in terms of abuse of information are happening amongst political parties, at least overseas, and those techniques are coming into Australia. So I have highlighted that in the submission.

More broadly, the other issues of concern raised in the submission relate to the enforcement, the structure which does not allow a consumer whose complaint has been rejected by an industry complaints body to have any revisiting of that other than through the ADJR process, whereas if a business has an adverse finding against it by an industry body, then it does have that opportunity to have the de novo hearing through the Federal Magistracy.

We urge that the Privacy Commissioner be given a more central role in the complaints handling process. Having worked with the industry groups quite extensively over the last three years with the development of the principles and the development of the legislation, I think there are several aspects of the bill which actually go beyond what the industry groups have concerns about—that is, for example, that mostly I hear a level of comfort with the commissioner being able to establish a consistency in how the principles are interpreted. And like a number of organisations, including the Australian Consumers

Association, I have real concerns that we will have a separate and inconsistent set of interpretations of the privacy principles by having a process where the industry complaint handling bodies are able to make rulings which do not really have a direct reference back to the commissioner.

The commissioner has a level of accountability through the process of annual reporting and through the fact that the commissioner can revoke a code, but I do not think that is going to be as helpful as a process which actually does allow an appeal from an industry complaint decision back to the Privacy Commissioner. The reason why I think that is particularly important in this context is that, unlike a lot of areas of alternative dispute resolution schemes and so on, privacy is one where the rules are not clearly established. The principles are well established, the principles have been there since the OECD laid them out 20 years ago, but how that works through in specific sectors, and with specific examples, is going to require some careful thought. There are going to be real problems if different industry complaints handling bodies come out with different interpretations, and that is where having reference back to the commissioner would, it seems to us, create a more consistent framework.

Those are our major concerns. There are some more detailed ones which we feel have been adequately dealt with by other organisations that we work with, such as the Health Issues Centre, in relation to the health privacy provisions. So what we have done is to highlight the concerns which we have, which primarily relate to the exemptions. We feel that if they are dealt with adequately, the legislation could be effective and could be a real move forward, as with a number of other countries. I guess Canada is the most recent example of a country that has gone ahead with privacy legislation. Of course, Victoria has now got public sector privacy legislation in its parliament.

We regret that privacy has been such a politicised issue in Australia, at a federal level at least, in the last 10 years. We hope that we can move on from there and that we can get bipartisan support for a good, consistent coverage which gives people an appropriate level of control over the use of their personal information. We believe that right is an absolutely essential right for the information society in which the decisions about people's lives and the ability to control their own lives and make their own choices is going to be determined by whether or not they have control over their personal information.

CHAIR—Thank you, Mr Dixon. Could we take you through your submission, particularly in relation to the specific issues that you have raised, starting with the small business exemption? Currently the small business exemption in the bill has a threshold of $3 million where the provisions kick in. Do you think there should be an exemption at all?

Mr Dixon—I think you have to look at the application of privacy legislation in its entirety. The classic example which is always thrown up at us is the local butcher: should the local butcher be covered? The answer to that question is: how much does the local butcher deal with personal information? I do not see that there is any benefit in having an exemption because having consistency so that you can say to consumers, 'You go online and no matter what .com.au you are dealing with you know that your privacy is protected,' is very important. As soon as you start creating exemptions I think you cloud the message and limit the ability to establish that basic objective.

There is another aspect to it. Look at how privacy legislation is actually enforced. It is not enforced with a hammer. It is always done through a process of resolving a complaint. If somebody has an issue with a small business which may not be aware of their obligations it can be resolved. If there is a problem, it would be resolved again through a mediation process with the Privacy Commissioner. And you can look at the experience overseas. In New Zealand, for example, the commissioner's approach has been very much an educative approach rather than an approach of kicking the boot into the smaller businesses. Given that framework, there is no reason to have an exemption. It does not involve extensive compliance costs and it does not involve extensive exposure to liability.

Ms ROXON—That really depends on what happens with this process and the government's response to it. There are a number of submissions that suggest that one of the problems with the bill—this is not my view; this is one that is suggested by a fair bit of evidence—is that there should be some penalties, some way of actually dealing with breaches or maybe persistent breaches. Does that mean that your view on the way small businesses should be treated is different, depending on what sorts of remedies might be in a final draft of the bill?

Mr Dixon—I think the answer is probably yes. Your expectation about the conduct of a large business is probably going to be greater because the reality of the processes that you know go on in a large organisation rather than in a small business. All of those factors in determining an award of compensation, which is quite unusual in this area—I have to say it is quite rare—are that the commissioner, if it is the commissioner making the decision, or the complaints handling body, would take all the factors into consideration, including the nature of the business itself. So I do not think it is exactly the same in a small business as in a large business.

Ms ROXON—So your preference in those circumstances would be that there is not an exemption for small business but that there perhaps be some principle—if there was a penalty provision—or issue that should be taken into account when determining how you deal with a breach. Your view is that you would prefer to see the size of the business as a factor rather than there being a sweeping exemption.

Mr Dixon—Yes.

CHAIR—I think you alluded in your comments to the fact that acceptance of privacy more generally in the community has been a slow process that has taken some considerable time. If you look at it in a sense that there is the adoption of privacy legislation in relation to the public sector and then to credit information agencies and now we are moving to the private sector, is there an argument for saying nonetheless that perhaps we ought to be doing this in a staged process starting with larger business and looking at how that works and hopefully having an educational effect and then a review which might extend it to smaller businesses? Isn't that wise?

Mr Dixon—I think at this stage of the game the issue is running ahead of us. It may have been the case a few years ago that, as you describe it, a staged approach made sense or established a neater way of implementing it. This morning's *Sydney Morning Herald* indicates that privacy is a very prominent public issue. If you look at the pace at which it

has moved, for example, in the United States and if you track the last two years from where the Federal Trade Commission and the Clinton administration were saying that there was no chance that they would move ahead with legislation and that self-regulation would be okay, you can almost track it month by month — as the privacy breaches become more serious and community concerns rise to record levels there is much more pressing need now for it. I think it is the case now that we need a consistent way of dealing with personal information across the board.

There is actually a lot of benefit for small business in that as well. If small businesses are not under this cloud of suspicion because your personal information is not safe, or is not as safe with a small business, then they are able to move ahead and you have this consistent across-the-board coverage. The reality is as well that for a lot of small businesses that is their perspective. Small business people are often very close to their businesses and often very tied into their businesses. For example, the issue of the ABN being for sale is an issue today because a lot of that information is actually personal information because it is individuals who run a business with a very small turnover. Small business people are often quite strongly pro-privacy. They stand to gain, and not necessarily to lose, from the application of the legislation.

Ms ROXON—Can I just ask a question on that point, still with small business. Is there any concern or any evidence for a suggestion that if there were an exemption for small business that larger businesses would simply construct their businesses in such a way that they fit within the small business exemptions, as we see businesses doing often in the workplace relations area—avoiding redundancy payments by having less than 15 employees and those types of things? Is there any suggestion that there is a problem on that front or is it more just related to wanting to have a consistency across the board?

Mr Dixon—There is some chance of that, although my understanding from the Attorney-General's Department is that a business would not be able to claim the exemption if they have a related entity which is a large business which is over the $3 million threshold. They would have to effectively divide the business into several less than $3 million businesses. Where perhaps that might be an issue is that if you had the kind of business that was at the threshold of just under $3 million or just over $3 million at least it may do that.

Of course, there are some restrictions; it is not a total exemption for small business. If they are dealing in personal information for some kind of gain or benefit then that will bring them into the scope of the legislation. If you look at that provision, it seems to me that if you, on one occasion, disclose information for some kind of benefit, which might be as small as shredding someone's credit card because it comes up on the machine and you get $50 for doing that, then one incident brings you within the scope of the legislation. In other words, if the small business exemption is thought through that way maybe a lot more people will be covered.

Ms ROXON—They will be caught by it and there will just be confusion.

Mr Dixon—It is a recipe for confusion. Working in legal practice and giving advice to clients about this is not simple. It is much better to establish something which is

consistent. As well, there is the process of progressively amending legislation: if you establish a low bar, which is the way that this bill proposes, you will see endless pressure for change and for improvement to raise the bar. The political risk with that is that governments will be forced to react to a specific issue that hots up because it is the front page of the paper and you get an overreaction in legislation. For example, in the United States, when Robert Bork was the nominee to the Supreme Court—the US has very minimal privacy protection—somebody released his video rental records that showed that he had a bit of a taste for blue movies. The response of Congress was to legislate protection for video rental records in that one particular area.

There is a risk that if you do not establish a good, consistent and internationally recognised standard across the board, then you will get pressure for specific legislation in specific areas. The patchwork becomes more complex; the legislation becomes more complex. The states will buy into that as well in areas like employee records, for example, saying, 'Look, this is the scope for workplace relations legislation'. You will see states will then legislate. I think the outcome is worse for both consumers and businesses. It is much better to establish a consistent standard which is after all tried and tested overseas and has proved quite effective with very minimal problems in countries like New Zealand.

CHAIR—On exceptions for small business, the fact that the disclosure of personal information about another individual for benefit, service or advantage or provision of benefit, service or advantage to collect personal information takes a business outside the definition of small business. If we are dealing, to take your example, with the butcher who is not likely to be disclosing except in the normal conversation that occurs over the counter at the butcher shop, but is not likely to be dealing with matters of privacy, isn't there some commonsense in that this is saying, 'Look, we do not want to bring a whole lot people into a net unnecessarily'?

Mr Dixon—There are two ways of approaching it. One is to say, 'Let us not have coverage unless a problem arises and let us review it in two years time. If we see problems, then we extend it.' The other way is to say privacy protection under privacy principles is commonsense and is the normal expectation that people have in dealing with each other and dealing with businesses. Therefore, because they are commonsense and they are enforced or implemented in an educative, reasonable, sensible and not heavy-handed way, it makes more sense to go the other way and say that these are your expectations as consumers—80 per cent of Australian consumers do expect the privacy legislation to be in place and consistently surveys show that kind of level of support—then if a problem arises, let us create an exemption.

My inclination is clearly to the latter, rather than the former, and I think there are other problems with the small business exemption. There are a number of new start-up businesses in Australia doing services such as bill management services. That is the classic kind of time-poor, cash-rich person solution. They get all of someone's bills directed to them and they handle all the bill payment, put it up on a secure web site, access it and make payments and so forth. They are not disclosing that information, but they are handling highly sensitive personal information—immensely sensitive. They get a complete picture of somebody's life from that. But if they handle that inappropriately, disclose it inappropriately, fail to have adequate security mechanisms or there is a breach

by an employee and so forth, they are not covered by the legislation, assuming they do not have, for example, health information. You will equally get anomalies that will work the other way round and, again, look at the experience of countries overseas. Does the micro-business actually have problems with privacy legislation? I don't see it.

Ms ROXON—I know we want to move on to some of the others as well. For example, real estate agents may well not have a turnover that will put them into the category where the provisions of the bill would apply, but they are still handling very personal information, not just where people live which many people regard as a fundamental sort of privacy as well, but what they pay in their rent or mortgage payments, who they rent property out to and all those sorts of things. Presumably they would not be covered.

Mr Dixon—Of course, the issues for real estate agents tend to be about collection of information and use of information, not about disclosure, whereas the exception from the exemption only addresses the disclosure issue. You have received evidence, of course, that tenancy databases and use of tenancy information and so on are in an area where there have been quite significant problems for a long time.

Mr CADMAN—Could I take up one of your opening comments in regard to CrimeNet? You seem to draw that into the privacy issue and I would like your views if you could express them on the difference between the collection of publicly available information and the collection of privately available information.

Mr Dixon—The publicly available information or public registers is a different issue because it is initially information collected by government—generally, of course, collected or created in the case of criminal database information under the force of legislation. You are still applying the basic principles, but you do need a separate mechanism or a separate way of dealing with the public registers as, for example, is done in the New South Wales state legislation. A Crime Net type of database can, of course, be a public register (although I understand that most of the current information is sourced from newspaper articles). But it is the whole issue of what is the reason for the creation of the record in the first place and the use should be related to the reason for its initial creation.

Mr CADMAN—Are you looking at motive? Should that be part of the process?

Mr Dixon—Yes, motive or purpose.

Mr CADMAN—I do not know how courts determine motive. Can they?

Mr Dixon—As to the public registers, how you would actually design or implement a framework for public registers, as with the New South Wales legislation, is to give scope for a privacy commissioner to work with the agency to create some framework, some limitations around the use of that information.

Clearly, public registers do not get covered by the same level of privacy protection as private information—absolutely not. It was never intended that those databases when they were created would be totally available for anyone to search—as is the case, for example, with things like the *White Pages*, which is not quite the same thing. It is not the intention

that people use the *White Pages* so that they can sit outside a house and find out the telephone number and the name of the person who lives there. It is the same thing with public register information, the ABN information, for example, which is the issue in today's paper. The purpose of collection for that—which is mandatory of course; individuals are being encouraged to disclose that information and to get an ABN and in the majority of cases they must do that—is not for that then to be commercially available.

Mr CADMAN—I have one other issue: you mentioned the ambiguity in the use of disclosure provisions of the national privacy principles. I am trying to do something of a comparison between the national privacy principles that we see here for the first time and compare that with the information privacy principles. Have you got any views on the relation between the two?

Mr Dixon—I guess in relation to the comparison between the two and taking the IPPs and putting them into a privacy sector context, the issue which has attracted most concern relates to direct marketing. It is the ambiguity of the terminology of what is practicable in terms of an organisation's obligation to get consent before they use information for direct marketing. Of course, from a practical point of view, the surveys show that the average Australian identifies telemarketing, direct marketing and spam as the number one privacy concern. It certainly does not have the intensity of the more rare privacy invasions that people do experience, but across the board it is a nuisance that people dislike and dislike quite intensely. Fifty to 60 per cent of people say that they find things like telemarketing—and even junk mail—a privacy invasion.

In the history of that provision was an attempt to provide some explicit guidance on the direct marketing. I think the outcome, given that there are inconsistent interpretations from experts on exactly how it would work, probably has not been what we intended it to be. But I think there is a need for greater flexibility applying to the private sector than in the public sector. Remember that information is collected in the public sector in most cases under the force of legislation, so it needs to be fairly tight in terms of usage, whereas in the private sector there tends to be more control and a greater element of consent.

Mr CADMAN—So you are not all that dissatisfied with the NPP?

Mr Dixon—There are real problems with the direct marketing exemption and I think that needs to be clarified. There are different interpretations on the NPPs. I feel that at this stage there are some issues there which could be addressed, but we do not want to revisit; we went through several years process of developing those. We could address some of the areas of weakness.

In the long run, I do not see that we need to have two separate sets of principles, I have to say. The European Union directive does not. But I am not going to win that argument. We have gone down the road of having two separate sets of principles. Let us work with what we have got.

Ms ROXON—Can I move on to the employee records exemption. Other than the general point that you do not need to make again about having a view that there should not be a large number of exemptions, I regard this as a fairly serious exemption because

people are in a position where they do not really have any choice about the information that they give their employer, in terms of mostly being required to provide their banking details and their personal details. I am a bit at a loss to understand the rationale, other than the one that people have that government should be divided in alphabetical order, A is Aboriginal Affairs, Y is Youth Affairs and workplace relations is nowhere near P for privacy or something. Do you understand the rationale for this exemption being there, leaving aside any political approach that the government may have about it?

Mr Dixon—Early in the development of the principles and the process of consultation with industry groups, there was a high level of concern about the disclosure of employee records, primarily motivated by concerns about how that information would be used in unfair dismissal actions, which has been an ongoing issue for some years.

Ms ROXON—A high level of concern about them and therefore the privacy provisions should apply, or a high level of concern about—

Mr Dixon—That they should have an exemption, because an individual could go off and find out that their boss has written some negative comments about them or maybe they have got wrong information—evaluative information, career track information and things like that—and there is concern that that could be prejudicial against the employer in the event of an unfair dismissal action.

Ms ROXON—So the concern is raised from the point of view of an individual having access to their own records, not actually trading. My concern about the exemption is that it seems to allow an employer to provide a lot of personal information to other people—future employers would be the most obvious example, I would think—that it may not be appropriate to pass on. My understanding of the way the exemption is drafted is an employer would be able to do that and would not be contravening any provisions of this bill.

Mr Dixon—I think that interpretation is right.

Ms ROXON—Provided they are not doing it for money.

Mr Dixon—Yes; I mean in the course of the employment relationship. I think that is right. The legislation does not reflect the learning process that we have actually been through over the last three years with this. The reality is that most of the employer organisations that we have dealt with have far less concerns now with this issue of employee records. However, they are concerned about employees being able to access some of that evaluative information like career track information, and I think that can just be dealt with through an exception to the access principle, rather than this across-the-board exemption. There are some really obvious ways in which this could be very prejudicial. If an employer gets a health test for their employees because they suspect that there might be a problem—some kind of exposure to toxicity or carcinogens or something like that—and the outcome is that, yes, there has been the exposure, employees will have no right to see those records. It flies in the face of any sense of what is reasonable and what is decent in the workplace.

The other issue which has been raised by employer groups—and really the only other one relating to this principle—is saying, 'Well, what about others having access to employee records, such as trade unions having access if they want to have access?' The answer is that is already covered in workplace relations legislation, in the Workplace Relations Act. And some of those workplace relations specific issues, regardless of where you stand on them, are more appropriately dealt with in that industrial relations context rather than taking them into the privacy area because that is a bit unusual, that is a third party having access to those records, so a union can then communicate with employees.

Mr CADMAN—That seems like breaking your own principles.

Mr Dixon—I am not taking a position on that. I am just saying that—

CHAIR—Where do you draw the line? That is the problem. I had a question which was based on your submission. I was presuming you were going to put to us that all privacy matters ought to be handled in a single, if possible, generic piece of legislation rather than dividing certain areas off into other pieces of legislation. But now you seem to be suggesting that some things should appropriately be elsewhere. How do we draw the line?

Mr Dixon—What I am saying is that politics is the art of the possible. I do not think we are going to see amendments on those issues. I would like to see the legislation go through and would rather it not be drawn into—

Ms ROXON—It would be more helpful for us if you do not assume what is possible and you actually give us your view on what you think would work or not work. The committee is not here to represent the government or anyone else. We are trying to investigate whether people think it is workable or not, and where there should be changes. Certainly, from my point of view, and I am sure from the point of view of the rest of the committee, I can understand that you say you do not think we can push for it at this time, but please give us your views rather than assuming that we have some position on it; otherwise it is impossible for us to evaluate whether it is workable or not.

CHAIR—Our report is an advisory report to the parliament. History would indicate that it does not always necessarily agree with everything that is in every piece of legislation that we deal with. It is better that we do approach it on the basis that Ms Roxon has pointed out.

Mr Dixon—Our position, in terms of what is best, is that personal information should be handled in a consistent way and that those provisions would be best dealt with under privacy legislation rather than under workplace relations legislation.

Ms ROXON—I think the point you are making about unions is different but I do not want to put words into your mouth, so tell me if I am wrong. Presumably, from your point of view, consistency in the way personal information is handled can be best achieved through one piece of legislation, as you have just said. But there will be all sorts of circumstances where information is handled—the tax office requirements in the ABN example, and the workplace relations example—when it is accessed by other than the normal people. There will be provisions in all sorts of different legislation that will have

some bearing on it. But with respect to the key principles for an individual, and for the use of an individual's information, presumably there is no reason why that cannot all be in the one place. Am I putting words into your mouth if I summarise it in that way, or is that an accurate reflection?

Mr Dixon—I think that is accurate, with the exception that there are specific sectors where the issues probably are best handled through legislation. I think health privacy is best dealt with by separate legislation rather than by trying to deal with it in an omnibus privacy act.

Ms ROXON—On the basis of their particular considerations that are too detailed?

Mr Dixon—That are very detailed. With respect to trying to deal with the health area at the same time as dealing with all of the other privacy issues, health is such a sensitive area. Health is quite unique in that it involves so many competing interests—the medical profession, health insurers, the Health Insurance Commission, the hospitals themselves, patients and medical practitioners. I think it is the most complex area and it is best covered by separate legislation.

In some other areas, in the telecommunications area, for example, you have got quite a lot of technical issues, relating to issues like interception, which are in existing telecommunications legislation. It seems to me, again, that it makes sense with respect to some of those issues. You cannot, for the sake of neatness, have everything in that one piece of legislation. But I agree with your description of my view—that is, as much as possible you want to have a consistent way of dealing with information and you put it in one law.

CHAIR—Why wouldn't that apply to employee records? There is potentially a whole range of players, if I can put it that way, involved at the employer and employee levels. It is possible that insurers of various descriptions can be involved in that. Trade unions have some legitimate interest in relation to employees. Without going beyond the question of unfair dismissals and industrial relations commissions, and the question about if someone has left a job and is then applying for another job what then fits into what is legitimate to put in the terms of a reference that might be provided for a worker et cetera, I am saying that if you say to us that health should be separate—which is what some of the submissions about the health area are saying—then, equally, cannot one say that employee records can be legitimately dealt with under workplace relations legislation rather than this?

Mr Dixon—I think the difference is that for the overwhelming proportion of the time there is a relationship between an employer and an employee which has quite a direct relationship. In every relationship there are third parties that have some role, but essentially you are looking at quite a direct relationship, whereas, in the provision of health services, there are always half-a-dozen parties involved. So I do think that health is distinct. From a practical point of view, I have been involved in one of the New South Wales government health committees for the last seven years and I would say I still do not think I have my head around the full range of health privacy issues, whereas the other privacy issues really are not as complex. So I think it is different, particularly because

obviously, with the disclosure of that information, in terms of the public interest with epidemiological research and so forth, there is a much greater public interest than there is, say, in relation to employment records.

Mr CADMAN—I do not want to delay the committee, but you made the remark earlier that privacy was highly politicised at the federal level. I must say I cannot observe that. I wonder if you could just briefly say how you see it.

Mr Dixon—I meant politicised in the sense that the process of getting this legislation through has been very tortuous from the time when the 1996 election commitment was very strongly towards world's best practice privacy legislation; the change of position in March 1997, driven largely by concerns about small business compliance costs and the representations that some industry groups have made in relation to that; and the 18 months then of the campaign to get the legislation back on the agenda at the end of 1998. I guess I look at it partly because that is the role that I have played and I know that role. I sit down with people at international conferences, people who play a similar role in privacy issues overseas, and it is consistently said that privacy in Australia is a more politicised issue than in most other countries.

In Europe for example, or in New Zealand—you do not need to go as far as Europe—there is far more bipartisan support. The New Zealand privacy legislation went through with both parties' support. This has been quite a political issue there and, working in this area over the last 10 years where there are consistently quite fundamental differences—and often it is working with the opposition, whoever the opposition is—it is not necessarily true that parties always take the same position on privacy issues. But it is a more politicised issue.

Ms ROXON—Can I ask a quick question about the political parties exemption. I understood from your opening comments that your concerns were mostly related to direct telemarketing, for want of a better word, and information that parties may be able to amass through phone polling or various other things. Is there any concern at the level of individual members who clearly handle a lot of individual information about constituents who seek assistance about all sorts of things? Many of us do surveys so that we can send people information in the areas that they are concerned about, et cetera, so even at an individual office level people have some form of database—or if not a database, information about people. Is there a concern about that level of information and how that is used for the furtherance of us serving our constituents better, or is the concern more at the party institutional level—or is it both?

Mr Dixon—It would be both. I am not clear myself as to whether all electoral work would be within that exemption—whether it is considered to be party political or whether that is regarded as more of a parliamentary service.

Ms ROXON—I am not sure that is a requirement. I understood it was an exemption for the people in the organisations rather than for the particular information or activity as it stands in the bill. But I do not claim to be an expert on it—not yet, anyway.

CHAIR—My recollection is that there were two provisions, one which related to political parties and one which related to individuals who were members of parliament. On page 24, 7C says:

(1) An act done, or practice engaged in, by an organisation (the *political representative*) consisting of a member of Parliament, or a councillor (however described) of a local government authority, is *exempt* for the purposes of paragraph 7(1)(ee) if the act is done in connection with:

(a) an election under an electoral law; or,

(b) a referendum under a law of the Commonwealth or a law of a State or Territory; or

(c) the participation by the political representative in another aspect of the political process.

Ms ROXON—So I suppose you argue about what it has done in the course of whether you want to send people a copy of your green guide or something.

Mr Dixon—Is everything that comes out of a local member's office part of the political process?

Ms ROXON—You would think so.

CHAIR—We would argue yes.

Ms ROXON—Not in the sense that 'political' is normally understood, but I just wondered about your views on that.

CHAIR—The difficulty here, I suspect, if we accept your perspective on this, is where you could draw a line. Obviously a lot of sensitive information is provided by constituents. Often I suspect our role as part solicitor, part counsellor and part a whole lot of other things is where we get sensitive information. In the sense of saying that people could check that, usually that information is provided by them in the first place. It is not something that is provided by someone else. I suppose in some areas like child support you could have information about someone else because of the nature of the problem. I do not know about my colleagues but I have always treated the information I get in those circumstances like the information that a solicitor would get from a client, and therefore it is held with a great degree of confidentiality.

It seems to me that your concern is at a different level—that it is about modern techniques of party politics or election time politics and the way that information is obtained more generally from the public. Is the core of your concern the collection of that information, on whether people have consented to it—presumably in a sense they have if they have answered a survey—or is it their ability to be able to check the accuracy of it?

Ms ROXON—Or the use of it.

CHAIR—Or the use of it.

Mr Dixon—In relation to your description of the local office activities, I have to say that I have never heard of a privacy complaint relating to the way in which a parliamentarian has handled personal information.

Ms ROXON—You need to come and sit in our office for a few days.

Mr Dixon—I am sure that is right, but certainly from my perspective, I have not heard that as an issue raised. There are a lot of privacy issues that do not rise above the surface simply because they are not known and who wants to talk about a privacy invasion? The whole point is that people do not want to talk about it but, going on the information that I know, the concern is largely at that more systemic level and it relates to the way in which the information is collected. When an organisation is collecting on behalf of a political party and not stating that and saying, 'We are Abacus research doing this survey to get information,' they are not disclosing the fact that the purpose for that will be then to use it in a particular way to communicate back to the elector what their concerns are. Fundamentally, what we are talking about is the kind of technique being imported from the United States. It is a manipulation of voters, because a different message is sent out to different constituents. In some cases it is a message that is essentially inconsistent between different constituents in the same electorate. To me, it is a zero sum game for political parties in Australia to allow that kind of practice to happen.

I do not see that one party is going to benefit over the other from doing this. It is far better if we can rule a line under that and stop it. It is a practice that is becoming more frequent now and it will become more and more frequent, given the way in which elections are conducted. It goes to the heart and the fabric of democracy and it undermines democracy when information is collected and used in that way. I have a very high level of concern about the way in which that information is used. It is highly sensitive information and I do not think that people generally understand the way in which that information is then used.

CHAIR—I am not sure that I quite follow. For instance, if people are surveyed and the survey indicates that person X has a certain set of beliefs about issues. If that is used in a way to tailor a message to that person which may be presumably individually sent by way of a letter, brochure or whatever to that person, what is the precise problem that you see with that? Is it a problem that the person did not know that the information was going to be used in such a way? How is that different, except in the technology that is used, from any of us as members of parliament walking down to our local shopping centres with a clipboard, talking to constituents? We could make a note that Mr Smith is interested in the environment and Mrs Jones is interested in aircraft noise in Lowe.

Ms ROXON—But isn't Mr Dixon's point that—

CHAIR—That is what I am asking: what is his point?

Ms ROXON—when they tell you, they know it is you that they are telling? You are talking about calls that are not—

CHAIR—For example, I am talking about someone doing a telephone poll. If any of us sent out a survey, which presumably we all do, it is pretty clear who it comes from because it usually has our picture plastered all over it for a start.

Ms ROXON—Several times.

CHAIR—So that is fairly clear. With telephone polling, can Abacus Corporation ring up and do a poll without saying, 'I am ringing on behalf of such and such a party or such and such a member of parliament.' I am trying to get to the nub of what the concern is?

Mr Dixon—The nub of what it goes to is the ability of candidates essentially to be deceptive by communicating two inconsistent messages. For instance, Tim Dixon says he is concerned about environmental issues. Joe Bloggs next door says that he is worried about jobs and development and he thinks the Greenies obstruct progress, and so forth. There is the ability of a candidate for office to communicate one message to Tim Dixon that says, 'I am pro-environment. I am in support of X, Y and Z initiatives that we have taken' and communicate a totally different message next door. That has already been happening in Australia.

Mr CADMAN—It sounds more like a trade practices issue than a privacy issue.

CHAIR—Why can't that happen even without technology? For instance, I go doorknocking and talk to Mrs Jones. She says to me, 'I am interested in the environment.' I make sympathetic noises about the environment and say that we are doing this and that and something else. I then walk next door to Mr Smith who says, 'We need jobs and we have to do more for business' and I make sympathetic noises to Mr Smith next door about that. What I am getting at is your complaint one about the ethics of inconsistency in the political process or is it about privacy? Do you know what I mean? Why I have a difficulty is that I suspect you have a legitimate complaint about something but I am not sure that it is a complaint that relates specifically to privacy. I understand the point about not disclosing that it is a survey for so and so. But the more general issue seems to me to be an age old complaint about the way in which politics is conducted.

Mr Dixon—I think the issue is different now because technology takes it to a very different level. When you deal with somebody immediately, it is clear. Of course, you do bounce off the person's concerns. Let us say you give somebody a letter. They are not aware that they have got the letter because you have a profile of their attitudes that they have given to someone they thought was an independent researcher, who was maybe doing research for a magazine, a newspaper or something like that. In fact, the letter is about your big issue. You are an environmentalist. The person who receives the letter is thinking your big issue is pro-development and this is the issue you are spreading to everybody.

I think it is a privacy issue and it relates to the way in which the information is being collected and used and, if you were to do your survey and say, 'I am the local candidate. I am gathering this information,' that would be absolutely fine because there is disclosure—you have been open. But it is the collection process that is the real concern.

CHAIR—I understand that. I wanted to tease that out because I was not quite sure what aspect it was that was your concern. I have a question on your comments about the media exemption. It has been suggested to us, I think by the Privacy Commissioner himself, that we ought to be looking at a more narrow exemption such as the one which is in operation in New Zealand or the one proposed in Victoria. Do you have a comment about those particular formulations?

Mr Dixon—Yes, I very strongly support the Privacy Commissioner's submission on that point. I think the drafting of the media exemption is quite clumsy in the way in which it will include activities which, for all intents and purposes, we would not describe as a media or journalistic activity. If you take an example, the Commissioner's submission mentions *Lock Stock and Barrel*—the web site with the politicians' home addresses and that sort of personal information in it. They can say, 'Hey, we are just presenting this information, we are providing information to the public and so we are a media organisation and we are covered by that exemption.' I think it does need to be read more narrowly. I think the Victorian drafting or the New Zealand drafting would both be far better.

CHAIR—Yes, we have probably spent a lot of time discussing this, but at least I know your view. The other matter was in relation to the review process through the ADJR of decisions made pursuant to industry codes. The complaint made against that, which we will hear more about today from the Insurance Council, is that they are arguing that there should not be a review process through the ADJR. Their reason, if I can paraphrase it, is that it will undermine the likelihood that people who go through the complaints process within the industry code will accept the outcome of that process because they can always go off to ADJR. I am just interested in your comments about that.

Mr Dixon—I am not unsympathetic to the argument of the ICA on that issue, but I think the practical means of addressing that is to give the Privacy Commissioner the recourse, rather than ADJR. It has been put in there in order to have some mechanism of oversight. There was this sense within the Attorney-General's Department in drafting this legislation. It is an unusual issue because there was quite strong support around the table on that issue for having a process that did refer back to the Privacy Commissioner, and the department really did not want to see that so they created that recourse to ADJR which allowed some kind of oversight. I think it makes far more sense from a practical point of view for it to go to the Privacy Commissioner.

CHAIR—We can ask them this, but what is your understanding of why the department did not want the course of the Privacy Commissioner?

Mr Dixon—My understanding was that largely the issue of a complaint goes to the company, goes to the industry body, goes to the Privacy Commissioner, goes to the federal magistracy, and there are too many layers.

CHAIR—The ADJR is for looking at review of judicial type decisions. I think there is some force in the argument that there is a legal fiction being created here to take it from an industry code to the ADJR process.

Mr Dixon—The argument, from my understanding and from what I have heard the Insurance Council saying, is that the whole aim of the alternative dispute resolutions framework is to have speedy, effective processes, rather than having more bureaucratic, more complex processes, and that is the nub of the concern.

Ms JULIE BISHOP—That was the aim of the human rights and equal opportunity legislation and it has been spectacularly unsuccessful. Not that I am confident that it will be more successful whether it was the ADJR process or the Privacy Commissioner. It still means that there are multiple levels of review for anyone who has enough finances to drag something out, basically. You have got to have some concern about that.

Mr Dixon—Although with the Privacy Commissioner it is not going to involve additional costs for the complainant and it is, I think, a far more accessible way of going forward than going through ADJR. My concern is that the industry complaint bodies do need to be accountable, and the ADJR process is an attempt to establish that accountability. I do not think it is a very good one; I think that it makes far more sense to go to the commissioner. Again, look at the reality of the commissioner, the commissioner's funding and so on is. He is not going to be intervening in every second decision that is made, but he does have the opportunity to establish some overall consistency in interpretation and ensure that the complaints bodies stay on track.

CHAIR—Unless there are any other pressing questions, time is getting away from us. Mr Dixon, can I thank you for the submission and also for coming along and discussing it with us this morning?

Mr Dixon—Thank you.

Resolved (on motion by **Mr Cadman**):

That the submission from the Australian Privacy Foundation be accepted as evidence to the inquiry and authorised for publication.

[10.47 a.m.]

BALLENDEN, Ms Nicola, Health Policy Officer, Australian Consumers' Association

BRITTON, Mr Charles Crawford, Senior Policy Officer for IT and Communications, Australian Consumers' Association

CHAIR—Welcome. I should advise you that although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of parliament. We are in receipt of the submission from the ACA. Can I invite you to make some brief opening comments.

Mr Britton—Thank you. I will make some brief comments and then perhaps Nicola has got a couple of comments on the health aspects of the bill. Our submission to the committee was fairly linear, trying to follow the layout of the bill and suggesting what we hope were some fairly constructive comments and changes. At this point I would just like to give an overview about the changing privacy landscape, and I have chosen a Dickensian theme, if you like, to take it along, talking about the ghosts of privacy.

We talk about the ghosts of privacy past, and we are talking there about the impact of computer processing and databases which were fairly scary in their time, and you will recall the Australia Card problems. At that point they were fairly static and historical databases. In those sorts of aspects of privacy in our submission we have talked about the existing data and the application of national privacy principles 2 and 6 to that. We have talked about the definition of the related bodies corporate and the use and collection of definitions.

We could move on then to talk about the ghosts of privacy present, if you like, and here we are talking about things like interactivity and the Net, consumer information gathered as transactions take place, the aggregation into profiles, the one-on-one marketing opportunities and the relationships that companies are always going on at us about. And here in our submission we talked about the direct marketing exception and the asymmetry of power given to the organisation as distinct from the individual over their own information.

We could then turn and look at the ghosts of privacy future where we have got Moore's Law, which applies to computer chips getting more and more powerful all the time—which I am sure it will give us free computer processing in the end—bandwidth advances which are going to give us unlimited communications capacity, and miniaturisation which is going to give us cheap audiovisual and recording device ubiquity.

We are going to end up with digital television which is going to put big fat pipes into people's lounge rooms, going both ways. We have got wireless access protocol type devices being carried around by everybody, and the irresistible allure of location

information for electronic commerce, to know where people are and what they are buying. We are talking about the growth of biometrics for authentication and we are talking about DNA metrics becoming increasingly available.

In the context of the bill, we talked about the small business exemption, an important point there being that not a lot of e-business is actually small business, and gathering information electronically over the Internet. We have talked about DNA information being included as sensitive information in its own right. We have got concerns about the corporatisation of health care and the threats that has for consumers. We are accelerating towards information transparency in society where we will be interacting with everything all the time. That could be an ideal convergent world where all data travels on one pipe, suitable for where you are, what you are doing and what you choose to be doing.

On the other hand, we could be talking about a counter-intuitive sort of future whereby, instead of watching the television, the digital television is watching you; instead of deciding when to answer the phone, you have to decide when you want to be unavailable; and instead of you driving your computer, pervasive computing will be all around you, pushing your buttons. In this converged digital future, I think we have to recognise that privacy is moving more and more towards centre stage. It is very important to get the structure and the framework right now, before this ghost of the future comes to haunt us.

Briefly, we looked in our submission at where the privacy regime will stand in this equation. We have long advocated, and we anticipate, legislative privacy protection, and we regard the legislation as a necessity. The bill makes a good start in defining the principles to be followed. We do not object, in principle, to a self-regulatory approach to the protection of privacy, but we do feel that it needs a layered approach, with an authority at the top. We believe the proposed structure has some key flaws which will undermine the effect of privacy protection on Australian consumers—the absence of a peak enforcement authority with the ability to have penalties and to hold inquiries. The capacity of the commissioner is not there to extend privacy protection by developing codes and requiring standards or undertakings. We are concerned about the likely evolution of what we term privacy silos, where the experience of privacy protection for consumers will vary from industry sector to industry sector.

Ms Ballenden—We have particularly serious concerns in relation to the health provisions. These relate partly to the self-regulatory approach in the legislation and partly to the way in which the health provisions are actually framed, particularly with right of access, where the principle sounds quite clear—that people have a right of access to their own health records—but then it is undermined by a range of exemptions that can be used to deny access to health records. When you tie this range of exemptions to the fact that, under a self-regulation scheme, the person making the decision about whether or not to get access to those records may be the person who compiled the records in the first place, you have got a fairly weak protection there for consumers.

The right of access in this bill is also substantially weaker than that under legislation which gives consumers a right of access to public health sector records. We are also concerned about the right of access that other parties have to health records, particularly in an identified form. This is also tied to the fact that it is, again, a self-regulatory scheme, so

who is making the decision about which other parties get access to those health records and how are they defining the terms that are used in the legislation?

CHAIR—We might come back to health. Can I ask some questions about your submission and the framework, Mr Britton. Your first recommendation is that the bill be amended to provide penalties which apply to serious breaches. I take it that you are concerned that the powers that the Privacy Commissioner has, which include, in effect, some compensation powers which are not strictly criminal penalty type powers, are insufficient?

Mr Britton—Our concern, essentially, is that this is a complaints based system and, so far as I can discern, there is no capacity for the Privacy Commissioner to look into systemic breaches or to intervene in the behaviour of organisations where there is perhaps a cumulative effect or a failure to comply with good practice in a broader capacity than just individual complaints—to focus the mind of an organisation to behave in that way.

CHAIR—The Privacy Commissioner—I think it is fair to paraphrase his evidence—said to us that he saw this as a light touch approach and he understood that approach. He saw that his role would be largely informative and educative and that, where there are complaints, the primary objective of his office's intervention would be to attempt to educate, mediate and come to a satisfactory outcome that would lead to a situation where there were not further complaints. Given that he has indicated success with that approach in the public sector, why should we not, at least at this stage until we know otherwise, trust that that approach will work in the private sector?

Mr Britton—I guess the private sector has more cowboys in it. The comparison I have often drawn when I have been talking about this is with the Radio 2UE inquiry that the ABA undertook. The point is that we subscribe to the notion of a pyramid of enforcement. At the bottom of that pyramid, self-regulation in the genuine sense works. Some people actually do the right thing because they want to. Then you have self-regulation in terms of codes of conduct, where you help people to know what to do. You then have industry bodies which can correct those that do not follow that. We also feel, moving up the pyramid, that it is useful to have it capped by an authority with the capacity to actually intervene if all those processes are failing to work.

The reason I mention the ABA is that they held an inquiry into the behaviour of radio stations. They held a public inquiry with, basically, cross-examination. Attending those hearings I was very impressed with the way in which the cross-examination of key witnesses penetrated behind the veil of self-regulation. It looked behind the codes that were talked about and looked at the emails and the memorandums that lay behind that and exposed in many ways a considerable breach of trust.

That resonates with me into the digital future I have talked about. This was in the realm of talkback radio, a very important trust atmosphere of people sharing a community feel for exchanging information. When you get into digital environments where there is a return path and those people are actually logged on in potentially tens of thousands, I see the potential for privacy breaches in environments that we really cannot necessarily see at the moment and where there may need to be inquiries. I think getting the structure right

now would be useful although it need not necessarily be wheeled out at every opportunity. Putting it there with those powers would be useful.

Ms Ballenden—Within health information, it assumes a sort of benign environment which is not necessarily there. It assumes that people want to do the right thing which is probably the case most of the time but not all of the time. A particular concern we have is with the corporatisation of general practice where some of the corporations are making a specific term of contracts that they have with general practitioners that patient data becomes the property of corporations. What that corporation may choose to then do with that data—sell it to pharmaceutical companies or sell it to direct marketing companies—could be really concerning. I had calls from people who were upset about even being included on a pap smear register. People are very sensitive about health information. If they had any idea that there was any chance that their health information would be given over to a corporation to sell or to do with it what it saw fit, it would be very worrying to a number of people. In a self-regulatory environment you have basically no recourse and no end point where you can go to appeal for the misuse of that very sensitive data.

Ms ROXON—We have some conflicting submissions on that. Some people say that there should be better enforcement procedures, as you are saying. The difficulty, of course, for the Privacy Commissioner is that the Privacy Commissioner presumably cannot be the person that intervenes in procedures or instigates an inquiry and also be the person that hears disputes if they are not resolved at an industry level, for example. Do you have a view from a consumer perspective about whether the Privacy Commissioner's role is best as an advocate for privacy rather than having some sort of hearing or enforcement role, or do you think that the Privacy Commissioner and the Privacy Commissioner's office can play both? Do you think it is better if they are involved in enforcement and there is some sort of consistency? From a consumer's perspective, what do you think is the most constructive role for the commissioner?

Mr Britton—The likelihood is that there will be conflict between those two roles. Whether they could be separated within an agency or whether it would be useful to separate them into two bodies would probably be a point of discussion. Looking at the telecommunications area, you have got the Telecommunications Industry Ombudsman and then you have got the Australian Communications Authority that does the enforcement. That seems to be probably a useful split, so if you were designing it from the point of view of regulation perfection, you might split them in that way. On the other hand, given the light touch—and we are not necessarily arguing for an extremely heavy touch; we are simply saying give it more heaviness—then it would not be impossible, I think, to design it for the Privacy Commissioner's office to be able to do both roles.

Ms ROXON—Why is your position, from a consumer perspective, for such a light touch?

Mr Britton—All we are saying is a balanced touch, I suppose. If we go back to the notion of an enforcement pyramid, we are trying to convey the point that we are not inimical to self-regulation; we do not necessarily want everything written in black letter law and enforced by a court system. What we are saying is we understand and, in many respects, approve of having, at the appropriate level, self-regulatory processes, but that

they need to be backed up and reinforced with mechanisms with genuine authority to monitor the self-regulatory system itself, to make sure it runs and, when it does not run, to intervene to make sure that it comes back onto the tracks. People have coined the term co-regulatory, but in our opinion co-regulatory implies an authority at the peak of that process to govern it, in a sense.

Ms Ballenden—The point is also that where you have a self-regulatory system your legislation needs to be perhaps stricter than it does if you have a more regulated system. In health records in particular there is the use of terms that might have quite specific legal meanings that if you had a regulator enforcing them you would not be as worried about. But where you have a self-regulatory system, vexatious can mean something different, impracticable can mean something different, according to who is interpreting those terms.

Mr CADMAN—Could you explain to me why the Health Insurance Commission does not really cover the matters that you—

Ms Ballenden—It is covered under different legislation. Public sector records are covered by different legislation than private sector health records. The health system is made up of both public sector providers and private sector providers. So your GP or your specialist or a private hospital would not fall under, say, freedom of information legislation or the legislation that governs the HIC.

Mr CADMAN—Is it possible to conceptualise these areas that you are talking about being gathered in under health insurance and the use of records because everybody has some health insurance of some sort?

Ms Ballenden—One of the things that we are particularly concerned about is the speculation that there will be a new national identifier for health records that will link records that are held by the public sector and records that are held by the private sector. Most people's health care is provided by a mix of those different providers. If you have this sort of fractured legislative system where you have certain legislation that applies to the records that are kept in the private sector and then other legislation that has a different standard, which it does, and applies to records that are held in the public system, it really undermines the consumer's right of access to those records and control, which we would see as absolutely key to a system of a national identifier working.

Mr CADMAN—Where do you draw the line in the health area? Medical records, diagnostic information, prognosis, all of that sort of thing, are clearly medical records, but where do the paramedical things, the pharmacological and the psychological things, fit in?

Ms Ballenden—It is a bit like Charles's speculating on the ghost of privacy future—it could look quite different in years to come. If you define it simply as any health information that is collected as part of providing a health service to somebody, then you can define health records in that way, whether they be kept in the private system or the public.

Mr MURPHY—Mr Britton you have made reference to the ABA's cash for comment inquiry, which was a very significant inquiry, and you pointed to the behaviour of the

radio stations. I would put it to you that the appalling deceit of some of the celebrated broadcasters associated with those stations—not only the arrangements with the stations but the very private contracts, lucrative contracts, that they had with their sponsors—raised a number of issues. You talked about online communication and the opportunities now with the return path and looking to the future, and I am just wondering what lessons from that ABA inquiry, and the future that you point to, might help us deal with this particular inquiry in relation to this proposed amendment bill. I would like to know what the lessons are and how they might help us.

Mr Britton—From my view, the key lesson in that was that trust is essential. Trust was abused in that affair. Trust is essential, particularly in the online environment. We have had a lot of debate about how to build consumer trust, to build e-commerce—assuming that is a desirable thing. To me, the lesson there was that there was a self-regulatory regime in place and basically there had been lip-service paid to it. The station had a code of conduct—it was there; it was purported to be adhered to—but it was only when there was somebody with some authority to drill behind that that these matters came to light. The Australian Broadcasting Authority is not notorious for launching inquiries and acting as an intrusive regulator—it was only when sort of dragged to it. What I guess I am saying is that another lesson is that a regulator with power is not necessarily going to be something wielding a big stick and intruding on the landscape all the time. In fact, none of our regulators seem to act like that even when we perhaps wish them to intervene more.

An authority with reserve powers needs to be able to delve into the machinations of self-regulatory regimes when it becomes obvious there is a systemic issue, and perhaps before that. I guess one could argue that the ABA could have well been more diligent in its investigation of talkback radio. I do not want to be too congratulatory of the ABA, because there was evidence mounted in that hearing that in fact they should have acted years before. Equally, you would have to hope that, if it had the privacy authority, that it would be given the brief to act more proactively. So I think those are some of the lessons. But the key thing for me was to be able to actually inquire into what was going on and to be able to cross-examine and look into actual behaviour.

Mr MURPHY—It is my assessment that it is essentially business as usual for the radio stations and some of the broadcasters. I am just wondering what your views might be in terms of trying to strengthen this legislation to give the Privacy Commissioner and others, and particularly government, a bit more teeth to deal with them. We know that the media is very powerful and probably presents the greatest threat to democracy in Australia because of the concentration of the media ownership. Without getting into that, talkback radio is a very popular medium for getting a message out from, I suppose, the government, to an audience, and I have some real concerns that not a lot has changed since that inquiry and that the ABA is a fairly toothless tiger. It seems that no-one is prepared to take these people on because they exercise greater power than the power invested in those who are elected to represent people in parliaments all over Australia and in the federal parliament for fear of the consequences of not toeing a particular line.

Mr Britton—Do you want me to comment on that?

Mr MURPHY—Yes.

Mr Britton—I think the key thing there is the fact that this digital convergent process is bringing things together that we did not necessarily previously think of being together. You would never have thought privacy and talkback radio, in a sense, would come together, but they come together.

As to concentrating the minds of players, I do think there should be the capability and the will within a regulator to exact penalties. Talkback radio was a systemic problem. It was not based on individual complaints; it was based on a systemic issue. One of the barristers in that hearing actually got up and said, 'Nobody has been damaged in this.' He was making a case that nobody had been affected by it because you could not point to a material loss to anybody. The whole point was that there were tens of thousands of people out there who had been dudded and their trust had been abused but not one of them could come up and complain, 'I've lost 50c' or something.

So to address systemic issues as to the effectiveness of it, I guess you start turning to things like the Australian Communications Authority with the ability to levy substantial fines if players do not come into compliance. Again, you could not accuse the Australian Communications Authority of lashing out with those fines; nevertheless, that power is there and I guess we would be advocating that both those authorities be a bit more diligent in their regulation, but there is certainly no scope for the Australian privacy administration that is being set up here to do any of that, so there is no risk at all of having to ask them to apply their powers because they have not got any.

CHAIR—Just coming back to your initial recommendations which we touched on at the outset. Can I ask a couple of specific questions that arise from your submission. Firstly, on direct marketing, I note that you are proposing that the current opt-out system which is contained in the bill be replaced by an opt-in system. Wouldn't that be impractical? If we accepted your recommendations, that would mean that the local lawnmowing service could not even put leaflets in the letterboxes of people in the neighbourhood?

Mr Britton—Potentially, yes.

Ms ROXON—They could once—

CHAIR—No, because there is no—

Ms ROXON—Couldn't they once and tell us—

CHAIR—No. They could now, but under the recommendation proposed they have no pre-existing business or personal relationship and they have not previously indicated their consent to receive mail from the organisation. So if I am Jim's lawnmowing service operating in Cabramatta or wherever, then I could not go and letterbox the neighbourhood and say, 'I've got a great deal for you if you want to sign up for six months for getting your hedges clipped and your edges done—whatever.'

Mr Britton—Going to an opt-in regime would present a lot of challenges. On the other hand, as far as the electronic mail environment is concerned, the government's recently

published e-commerce code or model has embraced opt-in for electronic mail. I guess what we are trying to establish there is the principle that permission based marketing we see as the way of the future. It is certainly the best practice approach of approaching people on the basis that you know that they want to be approached, and not approaching them on the basis that they might not tell you to get lost. So I guess one might ameliorate a strict opt-in regime with perhaps the opportunity to do it once and with an opt-out, as it were. It is getting a little muddled up between opt-ins and opt-outs.

CHAIR—That is effectively what the bill does, doesn't it? It says that the organisation gives the individual the express opportunity, at the time of first contact, to express a wish not to receive any further direct marketing communications.

Ms ROXON—But that is different to the time of first getting it and you are off. Unless you hear anything back, we will assume you do not want us to, which presumably is more in your—

Mr Britton—Which is the position we would be—

Ms ROXON—Although your proposal obviously does not do that.

Mr Britton—It would probably need to be workshopped considerably more before you could get a viable opt-in principle actually working, but the fundamental point, and I guess our ancillary point was that we feel the opt-out opportunity ought to be presented at each communication. We are not specifying the typeface or where it should be in the offering or whatever but people should be given that opportunity to opt out. I think particularly when you marry this with the broad definition of 'organisation', that permission or opt out is going to have to be communicated to potentially broad reaches of corporate empires both ways.

CHAIR—I understand that. Can I go then to the health information submission. Your recommendation is that in the national privacy principles subclauses 21D(2) and (3) be removed altogether and that clause 21D(1) be amended.

Ms Ballenden—Can I just find where we are?

CHAIR—This is on page eight of your submission and it is on page 68 of the bill. Can you explain why you would remove subclauses 21D(2) and 21D(3)?

Mr Britton—I am not sure what page ours is. We printed it up off the Internet.

CHAIR—It is schedule 3, national privacy principles, on the use and disclosure. Subclause 21D(2) relates to a use or disclosure conducted in accordance with guidelines approved by the commissioner.

Ms Ballenden—We have said that that be—

CHAIR—Removed?

Ms Ballenden—And that part (3) be removed.

CHAIR—Yes.

Mr Britton—The resolution to the problems we see there is that basically (2) and (3) deal with how you deal with the fact that you are releasing identified data. What we have suggested is we amend (1) so that you only release de-identified data. If you cannot contact people you only release de-identified data full stop and therefore you do not need any additional clauses.

CHAIR—But (2) says they can be released—this is identified data—under guidelines approved by the commissioner under section 95A, and if one goes back to section 95A this relates to guidelines that are issued by the National Health and Medical Research Council or a prescribed authority, and it relates to use and disclosure of health information for the purposes of research or the compilation or analysis of statistics relevant to public health or public safety, and there is a public interest test in it as well.

Ms Ballenden—The Privacy Commissioner is actually interpreting 95 under what conditions it is impracticable, so it is not up to an individual researcher to say, 'We tried to contact this person and we can't, therefore it is impracticable, therefore we want to use their data without their consent.'

CHAIR—I suppose the nub of my question is this: are you saying that it should always be a preclusion from using identified data even though it would have to jump the barriers of satisfying the Privacy Commissioner and be used subject to guidelines issued by the National Health and Medical Research Council and still have to satisfy a public interest test? After jumping those three barriers you still say that identified data should not be released?

Ms Ballenden—I guess the concern was around the use of the word 'impracticable' in an environment that is self-regulatory. If what you are saying is that for that part the Privacy Commissioner is actually taking quite an active role in interpreting and in governing the way in which access to that data is granted, then the concerns are somewhat ameliorated. However, when you take the fact that the act does not give consumers particularly strong right of access to their own health records, it seems quite unfair and paternalistic that somebody else can get access to their records and that they are not consulted in that decision if it is decided that it is impracticable to do so.

CHAIR—Let us take the common situation of a hospital in which there are researchers carrying on research and the research is conducted subject to the guidelines of the National Health and Medical Research Council. Say it is a women's hospital which is carrying on research into the incidence of, say, ovarian cancer amongst women. As part of the normal tests that it does when women come into the maternity section of the hospital, which they give consent for—say, tissue being taken and some of that is maintained. Ten years later the researchers, having found some new genetic breakthrough in terms of identifying the causes of ovarian cancer, say, 'We have on record the information relating to X thousand patients who have come to this maternity hospital over the last 10 years.' We make an effort to contact them but we cannot contact them. We know this is extremely

important information so why can that not be passed on to collaborative researchers in the case where they do not believe that the recipient—namely, the collaborator of the research—would disclose that information to anybody else but use it for research? It seems to me that that is entirely reasonable.

Ms Ballenden—Yes, if it is confined to that specific project and if the Privacy Commissioner is actively involved in assessing whether the researchers and the hospital have made all possible efforts. If the Privacy Commissioner is involved in determining what 'impracticable' is, I think a lot of our concerns are ameliorated there.

CHAIR—When you say that do you mean that he has to determine that in every individual case or can he issue some directive or guideline as to what impracticable would mean in these sorts of circumstances?

Ms Ballenden—He could probably issue a guideline.

Mr Britton—I do not think it is clear that he has the power to do so over the silo codes once they are set up and functioning—it is not just in health but in any other area where he has the power to make a guideline that would then be followed, let alone enforced—because there is no concept of enforcibility in the structure as set up. Without intruding on that area, the whole bill in many respects strikes me as a join-the-dots exercise. People solve problems that are thrown up by joining the dots in various ways to create an answer. In a sense the dots can be joined in other ways to create problems. It is a reflection of the complexity of this in a domain where, I think, consumers really want simplicity and certainty, not complexity and uncertainty. The way it works generates uncertainty. One of the problems with this in our mind was the long chain of text in a sense that needed to be there and the potential for things to drop off down that chain of text. That is why we went for fairly radical simplification in the end: if it is important enough, find out who they are; if not, then why can you not use the identified data anyway?

Ms ROXON—I have a question about simplicity. I am surprised that, as far as I can see, there is nothing in your submission that deals with the issue of the relationship with state regulation. Presumably from a consumer's point of view the ideal thing is to be able to go to one place and complain about one standard breach that any number of organisations might commit. Do you have a view on that or has there been any work done on whether these industry codes would be picked up at a stage level and whether you would be lobbying for that to happen?

Mr Britton—I guess one of the issues there is that we do not have a necessarily encyclopedic knowledge of all the states and their legislation, which I think is probably affected largely by time frames of preparing submissions and the depth which we can go into. I think basically, as a statement of general principle, I would go to the idea of consistency and I would agree with the notion that people want, what is almost a cliche, one-stop shops. There just seems to be a plethora of one-stop shops, unfortunately, which defeats the purpose of them. I think people want consistency, and one of the things that seems to be emerging is that a gap is now perhaps opening up between the public sector and the private sector. Although I could not go through and enumerate for you all where all those points are. It does seem to be an area with gaps, and we are going to get

additional gaps between the self-regulatory silos, which are more gaps. So you will get it at a state level and you will get the same thing at an industry level as well. I think we do look forward to a patchwork quilt of privacy, really.

Ms Ballenden—I would also make two points in relation to the earlier example that you used on health information. I guess one is that the Privacy Commissioner appears to be playing a different role with regard to this part of the legislation than he is with others, and I guess in the specific example that you use of people providing tissue samples if they have had ovarian cancer, another possible protection for those consumers would be to notify them that their samples will be kept on record and that it is possible that they may be used in future research projects and, if they object to that, then they should be allowed to tick a box that allows them to remove themselves from that process so they can be protected from the outset.

CHAIR—I take it from that though—from what you are saying and from what Mr Britton was saying earlier—that the primary privacy principle which you would want maintained or upheld is that, when people are providing any sort of information, they know to what use the information could potentially be made in the future.

Ms Ballenden—Yes.

Mr Britton—That is fundamental and I think that is where we are saying, in fact, that this bill gets off on the right foot, because that is there as a headline principle, and we are anxious to see that in legislation so we do not have a quarrel with that. Our concern is with the join-the-dots exemptions that sit below that and then the way those are used, for instance, to resolve concerns about the extent of organisations. You end up going down to dot point 2.3 and the use principles to assure yourself that it is okay to share data across large organisations. I am not sure that that is not where the uncertainties lie—in the interstices of it.

Mr CADMAN—The silo concept I find might be even more confusing than, shall we say, a more orthodox approach as we are moving with principles and specific variations, unless your silo concept takes into each silo the basic principles, plus additional industry or group specific material—

Mr Britton—The silo is actually a pejorative criticism, I have to say. What I am saying is that we will get silos emerging and we do not want to see those, so what we do not want to see is separate containers of privacy by industry with its own special code. We are happy to see self-regulation where industries could develop their own code, but we would like to see a system of oversight of those codes and the operation of them so that they do not evolve so that you get different interpretations and different codes, but that you could, indeed, in the spirit of self-regulation have codes which are developed, which do address specific industries and are sensitive to the needs of consumers of specific industries, but that they should not then become isolated from the mainstream of privacy and should be able to have directions applied to them.

Mr CADMAN—But you have got no objection to the establishment of the NPPs as a separate entity?

Mr Britton—They are the governing basis on which those codes are generated.

Mr CADMAN—You would not like to see that consolidated to one code?

Mr Britton—A concern that is emerging as I talk with people about this is the fact that you have then got a thing that is set in legislation, if you like, and that the Privacy Commissioner does not necessarily have the capacity to evolve additional codes or standards as required, whereas, for instance, in the telecommunications arena, the Australian Communications Authority has the capacity to require a code to be made. They can issue a standard for a code. The Privacy Commissioner does not have those sorts of powers. He has got principles in legislation and then administers them. I guess what I am talking about is a privacy administration, not an authority.

I think it would be useful to see more authority and that might mean the capacity of the Privacy Commissioner to require a code to be developed in an industry based on the national privacy principles, but possibly being extended in the context of that industry but under his authority. I think that then goes to things like those codes being disallowable instruments, which they are not in the bill because they would need to be reviewed by parliament. I think it does change the nature of what we are talking about, obviously, but you counselled a previous witness to talk about what we want rather than what we think might be possible, and I think that is along those lines.

CHAIR—Mr Britton and Ms Ballenden, thank you for the submission from the ACA and also for coming along and discussing it with us this morning.

[11.33 a.m.]

DRUMMOND, Mr Robert, Executive Manager, Operations, Insurance Council of Australia

MASON, Mr Alan, Chief Executive, Insurance Council of Australia

VINEY, Mr Richard, Chairman, Privacy Principles Committee, Insurance Council of Australia

CHAIR—I welcome the representatives of the Insurance Council of Australia to these hearings. I have to advise you that, although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. We are in receipt of your submission to the committee. I now invite you to make some opening comments.

Mr Mason—Thank you, Mr Chairman, and thank you to the committee. I might take the opportunity to make a few opening remarks. We are happy to answer any questions in support of our submission, but before I get to the detail of the submission I thought it might be helpful to the committee if I just gave a little bit of background to the two gentlemen with me today.

Mr Viney is the chairman of the insurance industry's privacy compliance committee, which is a body we have set up under the general insurance information privacy principles to examine privacy complaints. He has extensive experience in dispute resolution schemes. Within the insurance inquiries and complaints scheme he is the alternate chair of the scheme's complaints review panel. He is also the alternate referee for dealing with claims where there are reasonable grounds to suspect fraud, and he is the alternate adjudicator for small claims.

He has also had considerable background in the development and implementation of industry codes of practice. From 1992 to 1994 he was the leader of the policy team responsible for the development of the uniform consumer credit code and he has been the chairman of various Victorian regulatory authorities. He is currently undertaking the review of the Australian bankers code of practice, although that is not a matter we wish to take any questions on today. Mr Viney's views are obviously drawn from considerable experience of alternative dispute resolution mechanisms and their appeal to consumers.

Robert Drummond has been totally involved over the last few years in the development and launch of the industry's privacy code. He served on the working party assisting the Privacy Commissioner in the development of the Principles for the Fair Handling of Personal Information. More recently, he participated in the core consultative group which provided input to the Attorney-General's Department on the proposed structure and content of the bill.

As for myself, I have some experience in this area because I am a director of Insurance Inquiries and Complaints Ltd, and I was also instrumental in the establishment of the

original insurance industry code of practice and the dispute resolution mechanisms that underpin that. That code has been acknowledged widely by government and consumer bodies as one of the most effective dispute resolution schemes for consumers in the financial services arena, and I think it has been used in many circumstances as a model for others to follow.

The mechanisms we have established for dealing with complaints under our privacy code follow the same procedures that exist in the insurance industry's Insurance Inquiries and Complaints Scheme. The point is that the views we are expressing to you today are based on 10 years of practical experience of the management of consumer complaints mechanisms.

If I may turn to the bill, the Insurance Council supports the bill. We support the application of the national principles to the private sector and, broadly, we support the overview by the Privacy Commissioner. Our submission, and the points we want to draw to the committee's attention today, are based on a very serious concern about the proposal to introduce what we believe is an unnecessary bureaucratic and legalistic overlay to the supervision of determinations that would be made by the industry's complaint handling process.

These things are outlined in our submission, but you will note that there are three main concerns. The first concern is that decisions by dispute resolution bodies should be subject to review under the Administrative Decisions (Judicial Review) Act. We believe that this proposal is at odds with the concept of self-regulation and, more importantly, we believe it is going to introduce a level of legalism and formality which is inconsistent with an effective consumer dispute resolution mechanism. We believe that it will disadvantage consumers.

Secondly, we are greatly concerned about the proposal to make decisions by the dispute resolution body enforceable in the Federal Court. At first sight this proposal may appear to bring added power of recourse to the complainant, but we believe that the practical effect of this will be to weaken the authority of the dispute resolution body and its ability to enforce its own decisions and to apply sanctions.

Our third concern relates to the power of the Privacy Commissioner to make guidelines about the handling of complaints by ADR schemes. We believe that these guidelines should, at the very least, be made subject to a mandatory process of consultation with the schemes.

Our considered opinion is that these three matters, collectively, are more likely to bring an unnecessary regulatory overburden, with the net effect, which we are happy to explain in more detail, of disadvantaging consumers and at the same time discourage industries such as ours from making the financial and resource commitment required to make an effective privacy code work.

The stated aim of the bill at its outset was, I believe, to provide what was described as a light-touch framework which provided certainty and support for voluntary industry codes. We believe this is changing to one of co-regulation with legal enforcement. The

interpretation that we put on that is that the bill as it presently stands represents a rejection of the principle that the industry accepts and can apply the decisions of private scheme adjudicators, and it will substitute a highly technical and expensive judicial enforcement process in its place.

We think these are fundamental to the insurance industry's support of the complaints resolution mechanism. It is our view that, if these aspects of the legislation remain, the best interests of insurers and consumers may well be served by our abandoning our own voluntary scheme and for companies to rely on the default mechanisms in the bill. If that took place, I think that would be an unfortunate day for consumers and for the industry. Mr Chair, that concludes our opening remarks. We are happy to add to those or to take any questions.

CHAIR—Thank you, Mr Mason. To come to your point about both the recourse to the ADJR and enforcement through the Federal Court or the Federal Magistrates Court, I suppose that is based on a sense that what exists at present is effective and is working. On page 5 of your submission, you set out sanctions for organisations which fail to implement a decision, such as naming the organisation in the annual report; further, that clause 6(2)(a) of the standard deed of adoption empowers the board of IEC to terminate the deed of adoption executed by the defaulting organisation, thus effectively expelling that organisation from the scheme. My question is: what is the history of such sanctions?

Mr Mason—The industry's complaints mechanisms have been in place since 1989. They have gone through different names, but since the establishment of the claims review panel in 1989, I do not believe that there has been a single determination of the claims review panel, the adjudicators or the referees that has not been complied with by the insurance companies. Most of those involve insurance claims.

Ms ROXON—How many have there been?

Mr Viney—Currently there are about 2½ thousand a year, of which over 500 would be adverse to the insurer.

Ms ROXON—What sort of standard remedies are there?

Mr Viney—Essentially, these disputes that Mr Mason is talking about are disputes where an insured has had his or her claim denied, either absolutely or in part. So the complaint is against the failure of the insurer to meet its obligation under the policy. The remedy is that, where the insured succeeds, the insurance company has to pay the claim.

Ms ROXON—The aspect that we are considering is the effectiveness of your scheme in protecting people's privacy, not the effectiveness of the insurers in avoiding or paying out under insurance claims. So what figure of those complaints are related to privacy matters?

Mr Viney—None.

Ms ROXON—None because none is made?

Mr Viney—No, because the insurance industry's own privacy principles scheme is still in the stage of being formed. The experience that we are drawing on is the experience of the existing long-running dispute scheme, which does not deal with privacy matters. But in drafting our scheme and our rules of procedure and so on, we have stuck as closely as we can, and that is quite closely, to the same principles and procedures that we have in our ordinary insurance dispute scheme.

Ms ROXON—With respect to your threat that if you have to abide by the terms of the bill as they stand it is better to take your bat and ball and go home—I know I am paraphrasing a bit—are you talking about walking away from your self-regulatory scheme which applies to other insurance complaints?

Mr Mason—No, not at all. The complaints resolution mechanism deals with insurance claims and the sorts of complaints that we have just described. Under the insurance companies code of practice there is a range of other obligations that insurers have which do not result in necessarily monetary problems; they are issues of disclosure, of documentation being in plain language, training requirements and issues like that. That process has a disputes and monitoring process within IEC.

To further answer the chair's question about experience with that, over the years there has only been one company which has not complied with a direction of the Code Compliance Committee, to the point where it was named in the IEC annual report. That must be two or three years ago. The consequence of that was ultimately in the practical effect that that company withdrew from selling those products in the marketplace. For the insurance sector, reputation is an incredibly important facet. The sanction of naming a company and the damage that that potentially represents to their reputation is not to be underestimated.

CHAIR—I understand all that, but if there is not a level of complaints about privacy and there is not in operation an Insurance Council scheme in relation to privacy, I am not sure why there is this concern. You are going to continue with your normal complaints mechanism for other matters about, for example, whether or not there is a payment due under a policy. I understand what you are saying.

Mr Mason—Can I clarify this. There is a code of practice for privacy in the insurance sector. It has been in place since August 1998. There are 20 companies that subscribe to that at the moment. Hardly any complaints have come forward, but I think that is just a practical issue. There has not been universal take-up of that code yet because a lot of companies, quite understandably, have been holding back waiting to see what happens with the legislation. We very strongly would like to have an industry-wide code and we believe the industry would very strongly support that.

Our concerns on these specific aspects of the bill are that the industry will not welcome having a process set up like the other process which we drew as an analogy, whereby the Privacy Compliance Committee could make determinations and then those are subject to second-guessing, to further legal process. I think the industry's view would be that that would be unnecessarily expensive and repetitious and that if there is no certainty about the outcome of a voluntary dispute resolution mechanism, why have one, putting it bluntly.

CHAIR—Is that an objection to any review or specifically to the review by way of ADJR?

Mr Viney—It is an objection to any review which has the possibility of producing an outcome that the consumer does not get the benefit of the decision of the privacy committee. If we hear the consumer's complaint and make an award in the consumer's favour, we believe that the current system we have for other complaints ought to apply—that is, that the insurance company has to give effect to that decision whether they like it or not. I would make the point that in the 500 or so adverse decisions that they get under the ordinary insurance complaints scheme it is certainly not the case that they agree with them all, but they give them unqualified application.

Mr CADMAN—So what you are saying is that the insurer's immediate reaction would be to take it up to ADJR and fight the thing out legally?

Mr Viney—They have the possibility of doing so. Under the deed of adoption which they currently sign when they sign up, they covenant to give effect to any decision made by the privacy committee. That just cannot sit alongside the rights of review that are provided for in the bill.

Ms ROXON—Well, it could. There would presumably be no reason that the insurance companies still could not covenant to continue to adhere to the decisions that were made through that process. Of course, they might not be inclined to because, presumably, an individual consumer would not sign on in every circumstance to abiding by the decision, and I can understand that is why you do not want to do it. I am not clear what would prohibit the industry as a whole from saying, 'All right, we actually want to make sure that this continues to have credibility and we will sign off on not appealing.'

Mr Viney—My own view is that, if a Commonwealth law expressly gives a party who is aggrieved by a decision of our privacy committee a right to apply under the ADJR act for review of that decision under one of the nine grounds that are in there, it would be ultra vires the Commonwealth law for us to argue that they effectively have to forgo their rights by—

Ms ROXON—It would be ultra vires if you were trying to legislate to do it but, presumably, it is not if you have a voluntary scheme where you say these are the standards which you intend to adhere to.

Mr Viney—But our scheme becomes drawn into the network of this thing. It is formally approved by the commissioner. In fact, for the very purposes of conferring jurisdiction to review decisions of our committee, our scheme becomes fictionally deemed to be an enactment. And I suspect that gives rise to constitutional doubts as to the validity of this.

Ms ROXON—I think that had other problems.

Mr Viney—I think that once this legislation is in force in the terms in which it is currently proposed, one can no longer say that the industry scheme stands in isolation and the terms of that deed are unaffected by that. I don't think that is likely to be the view.

Ms ROXON—I am sure it is not likely to be the view; whether it is possible or not is a different thing.

Mr Viney—It is too difficult to take away people's rights conferred directly on them by a Commonwealth act and say, 'Well, you are in breach of your deed of adoption if you exercise the rights given to you by the law.'

Ms ROXON—I understand your point about your capacity to compel people to do that but I just do not understand why—if that is an industry practice—it could not continue that way. I am not doubting your view that this is a successful scheme—I am just trying to understand it—because from your introduction, I assume that all of you are industry representatives, meaning representatives of the insurance companies rather than industry as a whole.

Mr Mason—No, I am. Mr Viney is not.

Ms ROXON—No, you are not—sorry. However, you are not a consumer representative either—presumably, because of the position you are in, you are not an advocate of either. Do you have any information from the consumer groups? I don't think we have had concerns—that you have expressed—from consumer groups. I am just interested in whether there is a consensual approach throughout the whole industry, including the insurance companies and the consumers, that this system is working.

Mr Mason—I would quite confidently say that the insurance inquiries and complaints model has the support of the consumer movement.

Ms ROXON—I am not implying that it does not by the way, for the record. This is just a query.

Mr Mason—As a model, I do believe that people generally think it is very effective and functional. There is parity of consumer representation in the dispute determination process and on the board of the company. The other important issue—and I do not want us to leave you with a wrong impression—is that the model we have in our code means that the determinations of our dispute resolution process are binding on the companies that are signatories to it, but they are in no way binding on the complainant to accept them. The complainant still has access to all the other legal or other routes they want to take if they are not satisfied with the decision. I think that is one of the best features of this. The industry has for years seen the merit in voluntarily submitting itself to these things, to have quick and effective resolution of the complaints of its customers, because there is not much value to insurers in ongoing and long-running disputation with its customers.

CHAIR—I think I understand what is the basic thrust of your point. I think your figures were about 2,500, and about 500 were resolved in favour of the consumer and, if the companies are bound by 20 per cent of the cases, they should not be not bound by the

other 80 per cent or whatever the relativities happen to be. I understand that. One difficulty, though, it seems to me in relation to privacy is that generally there is not a range of other remedies. For example, if there is a dispute about whether or not an amount is payable under an insurance policy, yes, I understand you saying it is advantageous to the industry and to the companies to resolve that in the way in which you do. But you say there are still remedies available. Presumably the company could still be sued for breach of contract in the courts by the consumer whereas one of the difficulties where it is not quite analogous with privacy is that there is not the range of other remedies available. One cannot generally go off to the courts and sue for some breach of privacy in the way you can for breach of contract.

Mr Mason—Yes, but our underlying concern with this appeals process is that it is available to all the parties.

CHAIR—I understand that.

Mr Mason—I am not here to be an advocate for the consumer.

CHAIR—I understand what you are putting. Without going into it, potentially it does seem to me there are some legal problems in deeming, effectively, private enterprise, private industry and private bodies to come under the ADJR. That may be a question that others have some legal opinion about. Leaving that aside, there is also to be weighed up in all of this the notion that there is a sense of fairness in something being able to be reviewed. I am talking about a common sort of justice, I suppose. If a consumer does not have recourse to ADJR, then I would like to explore with you if there are some other means by which the public can be satisfied that the voluntary codes that are in operation are ones which are fair. I presume you would say that consultation with the Privacy Commissioner would be the method of achieving that.

Mr Mason—Also, I think Robert is correct, that the determinations will be published and will be publicly available.

Mr Drummond—I think you are right, Mr Chairman. I think the public confidence would come from the Privacy Commissioner's overview, firstly, in approving any privacy code and any dispute resolution scheme, and then having a continuing overview of the determinations made by these adjudicators.

Mr CADMAN—Has he had a look at the privacy code that you are developing?

Mr Drummond—Our privacy code has already been launched.

Mr CADMAN—Okay, but was the commissioner involved in that process?

Mr Drummond—The previous commissioner was, yes. Secondly, of course, the determinations made by the Privacy Compliance Committee would be made public, as the present determinations are. These would be immediately available to the Privacy Commissioner and he would have an ongoing ability to review determinations almost as

they were made. Any concern that he was beginning to develop in his mind could be immediately addressed in consultation with the Privacy Compliance Committee.

Mr CADMAN—Do you expect the same proportion of endorsement on your dispute settlement code as you do on the privacy code?

Mr Viney—I expect so.

Mr CADMAN—You have no indication to the contrary but no indication that they will?

Mr Viney—We have no cases on which we can base any concrete view on that, but I would expect there would be the same acceptance in the decisions.

Mr CADMAN—If that is the case, then you have made further comments about the difficulties in the powers of the commissioner to issue guidelines which would have some sort of statutory strength.

Mr Viney—Our point about that is simply this: we believe we have got 10 years experience in running a dispute resolution scheme—not dealing with privacy complaints, admittedly—which has proved to be a success and which has had significant endorsement from consumer groups in recent times. We believe that there is in our panel—in our referee and adjudicator personnel—a great body of expertise in fairness of process in these sorts of disputes. We feel that we need to be guaranteed a right of argument with the Privacy Commissioner before he effectively forces us to change our procedures.

Mr CADMAN—You would like to see a public notification process, perhaps in his annual report, to the effect that, 'I've had problems with the Insurance Council of Australia on this area of privacy,' and that would trigger some process or even require you, for the sake of public appearances, to enter negotiations.

Mr Viney—Our concern is perhaps at a lower level than that. It is that the commissioner's power to make guidelines concerning the making and handling of disputes is in section 18BF or something like that. To all intents and purposes, it seems to us to be unfettered in any way. But when one then turns to section 18BB, one sees that the guidelines, which is a term that you normally think is being helpful, become coercive, because he cannot approve a scheme. If a scheme deals with dispute handling, the commissioner cannot approve it unless it meets his guidelines. In that way, the guidelines get the force of law rather than being just a help. As a scheme adjudicator, I would like to have some say as to a proposal, for example, that witnesses have to be dealt with in a particular way or that their evidence has to be taken in a certain way, and other procedural things. We handle 2½ thousand cases a year, so we think we know a bit about it.

CHAIR—So you are suggesting—

Mr Viney—Mandatory consultation.

CHAIR—I accept that it does appear that 18BB(3)(a)(ii) has the effect that you are suggesting. I presume what you are suggesting is that in 18BF there be some proviso added—in effect, to 18BF(1)(b)—that, in issuing written guidelines relating to making and dealing with complaints under approved privacy codes, the Privacy Commissioner consults with the representative industry body prior to entering into; I am not getting the wording right but—

Mr Viney—That is right. Just to clarify something: we do not say that the commissioner should not be able to make guidelines which are binding. As part of the general effectiveness of the commissioner's role in overseeing the proper running of these schemes, and particularly when we are arguing that ours ought to be given effect to without any review, it is imperative that the commissioner does have a power to ensure that the procedures adopted by the private schemes are adequate. I would not debate that; we strongly support that. It is just that we think we ought to have an opportunity to express a view and to have a debate.

CHAIR—That seems a reasonable proposition to me with respect to being consulted.

Ms ROXON—Could I ask a question going back to the statistics. With respect to the 80 per cent of cases that come before you that are not decided in favour of the consumer—for example, the 2,000 out of 2,500 that you mentioned—do you have any statistics on how many of those are then pursued in other forums?

Mr Viney—No, we do not. We have had some difficulty because insurers just do not seem to keep records. We have been particularly interested in following that through in the context of the most difficult group of cases—that is those where the denial of the claim is based on alleged fraud because there are other consequences to consumers in that position. The difficulty of getting insurance in other contexts is the issue; so we have been trying to follow that down. I think some progress has been made—but, I am sorry, there is just no idea at the moment.

Ms ROXON—It would just assist on this question of the breadth of support for the scheme and how it operates. It would not necessarily indicate that those claims were not meritorious if they were not taken—

Mr Viney—I do not know of any cases where it has happened.

Ms ROXON—But you would not. Is that what you are saying?

Mr Viney—I think that if it were going along at any volume we would be aware of it.

Ms ROXON—You would get a sense of it.

Mr Viney—Just to put something else in its context, I might say that, because the insurance industry code of practice obliges them to have an effective internal dispute resolution process, there is a fair filtering of the refusals before they get to us. My understanding of the current position is that, on average, in the general insurance industry, just over one-third of claims decisions are overturned—are objected to. So one-third of

claims denials which are objected to by the client are overturned within the IDR scheme. Of course, an effective ADR scheme actually empowers the IDR scheme because it encourages you economically, and for other reasons, to get it right.

Ms ROXON—So what you are saying is that by the time the statistics come to you they are going to be more heavily weighted towards the insurance company because they have already—

Mr Viney—You would expect a higher success rate for insurers, yes.

CHAIR—Presumably, individual insurance companies must have a record of how many times they have been sued. I was thinking that one of the other remedies available to a client is effectively to take the insurer to court. We will report in a couple of weeks, but it might be possible for you to actually ask your member insurance companies what their records are, over a period of time, of having been sued—which, presumably, their legal departments would have pretty accurate details about—and then match that up with—

Ms ROXON—Ask them quickly because they will not be able to pass on the information after the bill goes through.

CHAIR—You have at least a couple of months, I would say.

Mr MURPHY—Mr Viney, we have just been talking about the proposal to make decisions by dispute resolution bodies subject to the proceedings of the ADJR Act. This inquiry is concerned with privacy and protecting privacy. Are you saying that anyone who might have some avenue through the ADJR Act to go to the Federal Court on a matter of privacy would weaken a legally binding agreement that might have been mediated with an insurance company because of the privacy issues that might have been thrown up? I am an accredited mediator with LEADR, and I have sat in on many mediations. I am just trying to understand. If you have a legally binding agreement and someone wants to go off to the Federal Court on a matter of privacy in relation to the mediation process, how does that weaken the legally binding agreement? The parties in the Federal Court would be concerned about matters of privacy and not about the issues that arose during, for example, the mediation.

Mr Viney—First of all, our procedures are not strictly that of a mediation; they are more in the nature of an arbitration. The insurer puts a view, the claimant puts a view, and we make a decision. I will speak in terms of just our ordinary scheme at the moment. Under our privacy complaints scheme, it only applies to insurers who have signed a deed of adoption in which they covenant to give effect to any decision of the committee. That is identical to the obligation which they have in the general insurance complaints scheme.

If the complaints committee is satisfied that the insurer has committed a breach of the principles and there is some compensation or remedial action that ought to be taken and it makes an order, our scheme, as it currently stands, will oblige the insurer to do that whether it agrees or not. They must do it or else they will be named and potentially expelled from the scheme. That is the enforcement mechanism that we have. Once this bill comes in and says that the insurer who has been the subject of such a decision of the

committee has a right to apply for review of that decision under the Administrative Decisions (Judicial Review) Act, then I think the obligation in our deed is affected by the creation of that statutory right of appeal.

Mr MURPHY—But isn't the access to the Federal Court, in relation to this, on privacy and not on the decision?

Mr Viney—It is on the decision.

Mr MURPHY—Are we sure of that?

CHAIR—In relation to complaints about privacy.

Mr Viney—In relation to complaints.

Mr MURPHY—Of privacy?

Mr Viney—Yes.

Mr MURPHY—Okay, but that is the point I am trying to make—we keep talking about the decision and that is why I want to understand your concerns.

CHAIR—John, I think what you were raising was where some question of privacy arises out of the process of the mediation and the arbitration, which is one aspect. But, generally, one would assume that a question of privacy would arise out of the dealings between the insurance company and the insured. The allegation would be that XYZ insurance company somehow made some of my private information available to someone else or released it or disclosed it or used it in an unauthorised manner. That is what I understood would be the normal course of what we are talking about.

Mr Viney—And the issue before us as a committee is whether the insurance company has committed a breach of the privacy principles as currently approved and, if we have found that a breach is committed, what sanction we think is appropriate, what remedy is appropriate for the consumer. That is the only issue before us. It is not a peripheral issue that has come out of something else.

Mr MURPHY—And your concern, of course, is once you are in the Federal Court on a question of law you are in tiger country, depending on the Federal Court judge.

Mr Viney—I do not think it matters very much which tribunal we are in; it is the question of being in any tribunal because we want—

Mr MURPHY—Which has the potential to disturb—

Mr Viney—The automatic acceptance of decisions.

Mr MURPHY—I understand.

CHAIR—Mr Drummond, you wanted to comment?

Mr Drummond—Mr Murphy's question raises another interesting point. It is not a major point, but I think it is worth making in the context of what can happen to a scheme when you introduce an unnecessary legislative overburden. And it is to do with privacy because the process of accessing the privacy complaints scheme, as our present is, is a private one; it is not a public process. The determinations made by the panel do not in any sense reveal the name of the claimant. All of the details of the claim are anonymous so that for anyone reading a determination there is no identification at all of the claimant. If that is opened up to a process of the Federal Court or the ADJR, then of course the claimant must immediately become identified and the whole process of anonymity that is present in our process is destroyed.

CHAIR—What proportion of the couple of thousand cases—if I can call them that—that come to you that are rejected would relate to alleged fraudulent claims?

Mr Viney—About 18 point something per cent. About a fifth.

CHAIR—So 500 or so are rejected on the basis of alleged fraud involved in the claim?

Mr Mason—We have got published statistics on these determinations. We can provide that to the committee.

Mr Viney—I am sorry. I think it is wrong. I think it is more like 10 per cent. The figures ran for a couple of years at about 200 a year with fraud reviews. They jumped very considerably in the last six months and started to look like annualising at 300 plus, but they have dropped back a bit. It is more between 200 and 300.

CHAIR—Mr Drummond's point is that an unintended consequence of this could be that, where there is a rejection of the claim based on the finding that the claim is being made allegedly fraudulently, if that then was taken to court then what has remained private would, in fact, become public?

Mr Viney—I do not think Mr Drummond is contemplating that the general insurances claims procedures would change.

CHAIR—No, but only in relation—

Mr Viney—Only in relation to the privacy ones. They might be the ones where the considerations are the greatest.

CHAIR—Yes. My point is an analogy but it could equally apply to privacy.

Mr CADMAN—With compliance costs, you have had a voluntary scheme running and you have some idea of compliance. Do you have any predictions about additional compliance costs it might impose on insurers to bring in privacy principles? I know that you are not resisting it, but I would like to have some understanding of what compliance might mean.

Mr Drummond—Of course, we already have produced the general insurance privacy principles so the cost of developing them and gaining their acceptance by the industry and gaining their approval by the Privacy Commissioner has all been achieved. The ongoing costs to our members would be the costs of having complaints heard by the committee. At the moment, that is being dealt with by simply an annual levy on members who adopt the privacy scheme. The cost to members is about $750.

Mr CADMAN—And you have how many members?

Mr Drummond—We have 80 members.

Mr CADMAN—And how many adopting members?

Mr Drummond—There are not 80 adopting members; only 20 have adopted so far.

Mr CADMAN—So that is not an extraordinary compliance cost at this point?

Mr Drummond—Not at this point.

Mr CADMAN—I would like to tease that out.

Mr Mason—If a large volume of complaints and matters come before the committee then the costs will develop. In the general complaints scheme over claims, the budget for running that scheme now is of the order of $5 million a year. Even so, it is regarded by the industry as a very effective and very cost efficient mechanism of dealing with these problems.

Mr CADMAN—I can understand it in your industry but I find it very difficult to apply the same principles to, say, the Independent Grocers Association.

Mr Mason—I do not know enough about grocers.

Mr CADMAN—No, but you would understand that the more organisations you have to deal with and the smaller they become—

Mr Mason—Yes. The reason this is so important to us is that the financial services sector is a massive holder of data. The general insurance industry itself has some 37 million policies that it deals with every year. To have an effective privacy regime, especially with the development of e-commerce, is seen to be a very necessary thing by the industry. I would not like to offer an opinion about grocers, but I suspect that grocers do not have the same computer systems, data records and history that the insurance industry has to deal with and protect. Many of our personal injury claims, for example, stay alive on the books for 10 years or longer, where there are periodic payments and things. We have a lot of very sensitive personal information about thousands and thousands of individuals. For us, having an effective regime and having the sorts of industry mechanisms we put in place, are seen as being very valuable.

CHAIR—Could I ask one final question to clarify a point? When there is a dispute which comes to you, Mr Viney, between an insured and an insurance company, do I take it that the identity of both parties is only known to the parties themselves and yourself as the arbitrator? Do they both remain anonymous?

Mr Viney—Yes, they do. The determinations, which are public documents sold on disk in great volume, I understand, are anonymatised. Not only do we not name the claimant or name the insurance company, but we also generalise descriptions of towns and district regions and those sorts of things which would otherwise make it fairly easy to identify who we are talking about. There is a major problem that when you quote a section of the policy that the argument is about that may, in fact, identify the insured to people in the know. Most insurance companies would say, 'That is from such and such a company's policy.' That is unavoidable.

CHAIR—Thank you for your submission and also for coming and discussing it with us here today. We appreciate it.

[12.23 p.m.]

EDWARDS, Mr Robert Leslie, Chief Executive Officer, Australian Direct Marketing Association

McCLELLAN, Mr Scott, Director, Communications and Regulatory Affairs, Australian Direct Marketing Association

CHAIR—Welcome. I have to advise you that, although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. We are in receipt of your submission and I invite you to make some opening comments.

Mr Edwards—Yes. I would certainly refer you to our submission. In my opening remarks I would say that the Direct Marketing Association represents around 450 corporations in this country that have an interest in the technique of direct marketing communications with their customers. One thing, in particular, that differentiates this activity from other forms of marketing is the use of the marketing database and use of marketing databases raises the issue of privacy and, in a sense, that is why we are here today. Like my colleagues that preceded us, ADMA played a very active role in development of the national privacy principles and was also a member of the core advisory group that advised the Attorney-General in the drafting of this bill.

We actually became the first organisation to incorporate the national privacy principles in their entirety into our code of practice. Compliance with our code of practice is a compulsory condition of membership of the association and the code itself was a section 88 authorisation by the ACCC last year. The code is administered by an independent code authority. The code authority is currently chaired by Deputy Commonwealth Ombudsman, John Wood, and has equal numbers of industry and consumer representatives on it. ADMA itself has a long track record in code administration. The association has been around since 1966 and since 1986 we have administered a service a ‘do not mail, do not call’ service where consumers can call us and register their preference not to be receiving unsolicited marketing offers from our members.

We recently launched, in conjunction with our colleagues overseas, a similar service for email. Members of this committee would have received earlier this year a package of information from us on the mail schemes. The philosophy behind our programs can be expressed in one word—choice. Our members believe that consumers have a right to choose not to receive marketing communications and exercise their preference and they agree to respect that choice. It is in their commercial interests at the end of the day to do so.

For example, if a person is very interested in gardening and investment and would like to receive offers, discounts, promotions and information from responsible companies about these two interests but asks for no further unsolicited advertising mail, telemarketing calls or emails, it is in our members’ commercial interests to carry out this privacy request. Fortunately, the same technology that is enabling greater storage

integration and analysis of data also enables companies to cost effectively tag data with these individuals' personal preferences.

If we use technology to help record and act on what consumers do and do not want to receive, I think we achieve three things: a lower cost of business at the end of the day; better relationships with customers; and greater control for the consumer over what he or she receives. Frankly, if marketers can arm themselves with high quality data, they can be more confident that their offers will be welcomed. Increasingly, I think consumers expect and even demand this level of service. They need to know what is happening. In a marketing world a new language is being invented to describe this phenomenon. There are terms like 'infomediary', 'mass customisation' and acronyms like CRM, which stands for customer relationship marketing.

I believe the bill incorporating the NPPs gives business the flexibility it needs to meet consumer expectations in the area of customer service, relevant product and service offerings and responsible personal information and handling practices. It also gives consumers what they need—choice about whether or not they want to receive direct marketing communications and control over their personal information.

I do want to make one more point: the Attorney-General has said that light touch does not mean soft touch. I certainly agree that compliance with this legislation will not be easy for some organisations. Some organisations are going to have to undertake major improvements to their information and handling practices. They will have to keep more accurate records and provide access to their customers. That in itself will be a costly exercise for some businesses. Keeping track of who does and does not want to be contacted will involve a whole new level of database complexity for many organisations.

However, we believe the future in marketing is certainly one to one. So, in the long run, the higher standard is going to be good for business, good for customer service and, in the end, good for consumers. Certainly on that basis ADMA would be pleased to announce that, provided the legislation with NPPs makes its way through parliament intact, ADMA would certainly step forward to have its code authorised by the Privacy Commissioner. I am happy to take questions.

CHAIR—Thank you, Mr Edwards. I note in your submission that you oppose the small business exemption. Can you expand upon that?

Mr Edwards—Basically, we believe there should be a level playing field. To the extent that our members—many of whom may be under the $3 million threshold—are covered by our code of practice already, we would be concerned that they may in a sense use the small business exemption for non-compliance with our code of practice and we do not think that makes sense.

Ms ROXON—But your members in particular would not come within the exemption anyway, would they, because they are specifically exempted from the exemption because of the type of material you are handling and work that you are doing?

Mr Edwards—But it could very well be in their other business practices they would fall under that exemption as well, to the extent that they are using the data—

Ms ROXON—So that they would try to separate out which parts of their business they do not have to—

Mr Edwards—Correct.

Ms ROXON—I am not disagreeing with your view but I was just wanting to point out that presumably the direct marketing aspects of it would still be covered by—

Mr Edwards—Yes, to the extent that they would be using the information themselves, but only if they are disclosing it. If they are using it for their own purposes, they would still be covered by principle 2.1, so that is true.

CHAIR—These are always judgments, but if you accept the argument that you were putting forward that we should not have a small business exemption, nonetheless is there any level where it just becomes a nuisance—because you are talking about a micro-business? Take an analogy: with the GST, there is a level of $50,000 worth of turnover below which you do not have to register unless you believe it is in your interests for the GST. Is there practically some level at which we should just say that this should be exempted?

Mr Edwards—We would certainly agree with the government's view and the aim to try to reduce the regulatory burden on business. I think we share that in common but, at the end of the day, the overriding concern I have is one of a level playing field amongst businesses. I think this has the effect of actually creating some imbalance in the marketplace.

Ms ROXON—Presumably, as a consumer you are just as offended if your privacy is breached by a small business or by a large business?

Mr Edwards—I would share that view.

Ms ROXON—I want to ask a question about existing databases. It is interesting that in most of your submission you are very supportive and probably, in the public's view, surprisingly supportive of the principles and things, which obviously is a reflection on how much you have done throughout this process to get to the stage where you are. It surprises me that in passing you say that this exemption for existing databases is no big deal because the value of the database decreases if you are not updating that information. Presumably there is still a massive amount of information which is already out there and some suggestion, which I think is implicit in your submission, that you would not need to look at applying principles to those existing databases.

Mr Edwards—I put it to you this way: in terms of the disclosure provisions of the bill, if an organisation has, for example, two million customer records on their database and the bill now provides that these people must be given the right to opt out, what I am suggesting to you is that, if that data is to be of any benefit to the organisation, they

would, over time, contact those customers anyway. During the course of contacting them, they would have to go through the processes of making the opt-out provisions available to those individuals. To say that it should apply to all existing data as a blanket on day one, I think defies reality. It just could not happen.

Ms ROXON—Is your concern in relation to having some sensible transitional period rather than not wanting the principles to apply to any existing material?

Mr Edwards—The latter.

Ms ROXON—You do not want the principles to apply to any existing material?

Mr Edwards—No, what I would suggest to you is that, provided there is a transition period, businesses could live with that because data, in itself, is a living and breathing thing.

Ms ROXON—Let me be clear about this because I think it is quite important. Do you say that the transitional provisions need just to be during the course of your ordinary business—so that by the time you have made contact with them in the future you will then do the opting provisions or check that the material is accurate—or could you live with some other phasing-in scheme, which would perhaps put a higher obligation on you actually having to ensure that those customers are given the rights that they would be given if they were now being put on your database but in a time frame that is manageable? Is there any objection to that?

Mr Edwards—No, provided the time frame was manageable, I think both aims could be achieved. I say again that, if an organisation is not contacting their customers once or twice during a year, the data they have on their customers runs the great risk of being out of date anyway, because the customer may have moved and things could have happened.

Ms ROXON—That might be the very thing that people object to—the fact that it is out of date. You might have a legitimate concern of correcting that if you were the consumer.

Mr Edwards—Indeed, you would. The point was: what time frame is reasonable for organisations to have their data compliant?

Ms ROXON—It is purely driven by the practicalities of it. That is really what I am trying to get to.

Mr Edwards—Yes.

CHAIR—Presumably the answer to that—and I am trying to also live in the real world—is going to vary from company to company. There may be some companies where, if contact is not done on a quite regular basis, the value of the data quickly loses significance. I presume there are other companies who have other commercial interests where a contact every year or so may simply be sufficient.

Mr Edwards—Yes, that is true. But, once again, it depends on what the organisation itself uses the data for.

CHAIR—Yes, I understand that. I wanted to put to you the proposition put to us by the Australian Consumers Association about an opt-in approach rather than an opt-out approach.

Mr Edwards—Why doesn't that surprise me?

CHAIR—I was going to say before you said anything that I think they conceded there were some difficulties in how you would formulate it, so the way in which it is formulated in their submission would obviously have to be varied if you were to go down that path. I am interested, nonetheless, in your comments on the record to the proposition.

Mr Edwards—I guess the first thing I would say is that opt-out is an international convention that has been established. It is now the standard in the EU in their data protection directives. That has been established. I think it does set out a precedent that allows organisations to have a constructive relationship with their customers and give them the right to object to further communications. I harken back to the days nearly 20 years ago when telephone marketing, in a sense, first came into this country. There was a fair hue and cry that it was invasive and created a fairly significant privacy issue. I sat through a number of government committees under the old Austel regime that looked very closely at this. At the end of the day we came to an opt-out provision—that is, businesses could contact you provided they gave you the right to opt out of receiving further communications. At the end of the day it almost harkens back to the issue of almost freedom of speech. My view is that businesses should be able to contact you to make an offer of a product or service but give you the right to refuse further offers.

That is not to say, and the ACA made a point and it is true, that there is a fairly significant shift in the online marketplace to permission based marketing. I would agree with that. I think that permission based marketing is probably the future. But we have to understand that we have a benchmark, we have a baseline of opt out. If organisations want to build on that through an opt-in process with their communications with their customers, I would encourage that.

Ms ROXON—Do you have a view that the ideal is serial opt out and each time you make contact you have to give the consumer the opportunity to opt out, or do you have this once off—

Mr Edwards—It seems to me it is like someone going to a business—if I could just be somewhat light-hearted about it—going to a customer and saying, 'Would you like to hear from me again? Are you sure you would like to hear from me again? I wrote to you last time and I think I would like to write to you again, but do you really want to hear from me?' It is like you are going back asking them all the time. It seems to me as though it is not commercial reality. I will give you an example. As an early part of the Austel work in this area there was some push at one stage to impose upon Telstra the mandatory requirement that they give their customers the right to opt out of further communications at the time that they establish the relationship with Telstra. The argument was run for

some time and I made the point then that you have to understand. You can imagine a situation where you sign up for a line service with Telstra and at the same time you tick a box that says, 'Don't send me any further communication,' so you opt out.

Three months later you are having a dinner party with your colleagues and in the conversation—God forbid that it would come up—the cost of telephone calls may be the issue. Some of your friends make the comment, 'Gosh, I have this new deal from Telstra that has halved my telephone accounts.' You are enraged and say, 'Why haven't I been told that?' It is because at some stage you have told Telstra that you do not want to receive any further communications from them. I think it can materially disadvantage individuals. I am talking about a mandatory serial opt out. That is what I am saying.

CHAIR—In the email world it is common now when you receive emails that there is a standard box, 'If you don't wish to receive this, link here.' Is that difficult to do generally? I understand your point but it is not saying, 'Tell me again if you want to opt out,' it is just a standard box you get. If that is how you feel you click it. I have to say that there are some that annoy me but I still have not opted out of them. I do not know why.

Ms ROXON—Presumably if it is email or mail, it is easier to have a proviso at the bottom saying, 'Note: you can stop receiving this mail any time if you call such and such.' It is a bit different if you are doing it over the phone. I understand the point you are making about some client-customer relationship. It depends how active the relationship is. Did you say that your do not call, do not mail service has been going since 1986?

Mr Edwards—That is correct.

Ms ROXON—And it has only 20,000 people registered.

Mr Edwards—Twenty thousand this year.

Ms ROXON—Does that mean you have to repeatedly ask for it?

Mr Edwards—No. People come on to the database. It is for two years at this stage, so they drop off after two years. The reason is that people move; 17 per cent of the population move every year, so we need to make sure that it is up to date.

Ms ROXON—Would you be in the odd position, in maintaining that database, in keeping information with which you are trying to respect people's privacy, that the handling of that material—presumably informing your affiliate organisations—will in any way breach the provisions?

Mr Edwards—No, because they are opting in to the service.

Ms ROXON—They are opting in to opt out.

Mr Edwards—Yes, it is like that.

Ms ROXON—So they are giving you permission by doing that—to pass it on to your affiliate companies and say, 'Keep us off.'

Mr Edwards—It is very clear.

Mr MURPHY—Why are you not able to use the opt-in approach when the Internet is?

Mr Edwards—For a number of reasons. The Internet is immediate. It is a very simple thing to do—click the box and it is done.

Ms ROXON—You would want it to be hard for people to opt out.

Mr Edwards—Not necessarily. It is a different environment. The environment with email is the immediacy of it. With mail, you might put it aside and open it at some stage, have a look at it and say, 'I don't want to receive any more of this.' This issue has been the subject of fairly substantial debate overseas. I think that opt out is the benchmark for most jurisdictions that I am aware of around the world. You need to be very mindful that we do operate within a global environment and that any move to have an opt-in environment in our legislation could materially disadvantage Australian business vis-a-vis their overseas competitors who would not have that same restriction.

Ms ROXON—Doesn't it cut the other way as well? If we do not have standards that comply with what is expected internationally, our businesses will be disadvantaged because the EU said they have given all countries a window to basically have compliant privacy legislation or else they will not exchange information.

Mr Edwards—That is true.

Ms ROXON—So it goes both ways in terms of affecting business, if we do not have—

Mr Edwards—You would all be aware that the Americans have held out against the EU directive. Recently, I read where the European countries have now agreed on what they call safe harbour arrangements when dealing with American companies. That is on an individual contract basis, because they realise that the US government is not going to move in the short term to introduce satisfactory legislation. So what could actually happen is that there would almost be an artificial trade barrier established between Europe and the United States because of non-compliance with the EU directive. So to try to find a way through that minefield they have established what they call safe harbour arrangements. It can be transferred provided it meets these contractual agreements between the transferring parties that agree to abide by the EU directive, anyway.

CHAIR—Given that we are in a global environment, what do the major multinational organisations who are trading in this environment and who are American based do? With respect to the absence of complementary or similar legislation in the United States, what is the practice of these US organisations? Do they adopt, in effect, the EU standards?

Mr Edwards—It would be fair to say that that is the case. Most enlightened big multinational organisations have pretty well embraced the EU directives as part of their normal trade practices.

CHAIR—You may not be able to answer this: why then is the American legislature, the American Congress, not going down this path? The obvious answer is that they believe it is in their interests not to, but I am interested.

Mr Edwards—I think you are probably also right, but I am not the expert in the area, although I do spend a bit of time on this area. Clearly, the Americans are not quite as quick to legislate as we Europeans or Anglo-Saxon type folk anyway. There is a difference. I also think that the Americans have left it up to the individual businesses to resolve the problems themselves, rather than try to have government intercede in this. And looking at the press releases recently, I understand the American Democrats are going to introduce a privacy bill into Congress, but it will not go up until after the US elections. The Republicans have a very strong view that they do not want to introduce such legislation, so it is likely to go nowhere, I would have thought.

Mr CADMAN—I notice your membership list may not be comprehensive. What proportion of direct mailing services do you think your members cover?

Mr Edwards—I have said this before: direct marketing, in a sense, is a technique. It is a function that we try to regulate, so it is not an industry. So someone operating from home with a personal computer and 20 customers and mailing to them is in the business as much as Citibank is with two million customers. So to try to get a measure on the volume is very difficult. However, the work we have done with Australia Post—and they monitor what is called advertising mail, and that is a great volume of mail—indicates we cover about 80 per cent of the market by volume, not by practitioners but by volume.

Mr CADMAN—What about by practitioners? Do you have an estimate of that?

Mr Edwards—I have no idea because, as I said, all small businesses, in a sense, are in the business of direct marketing, as are public institutions, public bodies, and increasingly so.

Mr McClellan—Most of the major service bureaus in the industry—the list bureaus, the data manipulation organisations and the major mail houses—that handle on a contracted basis the mailings on behalf of whatever organisation, would be members of ADMA. Even if the particular organisation generating the campaign is not an ADMA member, the chances are that the campaign will fall within the orbit of ADMA by virtue of the fact that one of the suppliers in the chain is an ADMA member.

Mr CADMAN—That is clear. So a substantial proportion of industry participants are involved in your organisation. Are you concerned about non-members and their ethics and conduct?

Mr Edwards—Yes, of course we are. In another area I work with a government body, the task force that has been set up to advise the government on a template for self-

regulation. We have been working in this area for the last six months. It is symptomatic of any self-regulatory body like ours that you are never going to get 100 per cent market coverage, but what you can do over time is develop best practices. I think that part of the authorisation we sought from the ACCC with our code was to enable our members to insist that their suppliers were also code compliant. That could be held to be anticompetitive but the ACCC has seen that there has been an overwhelming public benefit in that. A bank, for example, may be in the business of bringing in data from outside for its credit card acquisition programs—

Mr CADMAN—Perhaps from the tax office!

Ms ROXON—Only if you pay!

Mr Edwards—but it has the effect of cascading codes through non-member companies over time.

Ms ROXON—Concerning that code of practice, would you talk to us a little bit about what stage it is at and how it is working? I understand that you have got it up and running. Are complaints made? How do people know about it and those types of things?

Mr Edwards—I might defer to my colleague who is actually the administrator of the code authority.

Mr McClellan—The system was launched when we launched the new ADMA code of practice in late 1998. The code authority has received, in the roughly 18 months that the system has been operating, about 75 complaints, with half of those having a privacy dimension to them. The ADMA code of practice also covers fair trading, telemarketing and e-commerce related issues, so we deal with complaints in those areas as well.

If you were to categorise registrations to our 'do not mail, do not call' service as privacy complaints, and most of the people who actually call us and register for that service are, as Tim Dixon was expressing earlier this morning, registering a grievance or an annoyance with the invasiveness, if you like, especially of telemarketing calls. If you include that number of complaints there are another 12,000 a year that we are getting, roughly 200 a week.

Ms ROXON—What is the figure—20,000, 12,000 or 200?

Mr McClellan—We have about 20,000 to 25,000 this year.

CHAIR—What proportion or what number are related to privacy?

Mr McClellan—The complaints that come before the code authority and that are dealt with under that administration are, generally, substantive written complaints about a grievance that the consumer has under some element of the code of practice. By far the vast majority of those registrations for the 'do not mail, do not call' service are simply dealt with in a systemic way.

Mr Edwards—We do not categorise those as code complaints, so the complaints that the authority deals with are generally issues around transactions.

Ms ROXON—But you are aware that a large proportion of the people who are calling to register on that are doing so because they object to or are irritated by the contact?

Mr Edwards—Yes.

Mr CADMAN—I have a comment about compliance costs. You have put in place a complaints mechanism—and let us include the 'do not mail, do not call' as being a privacy complaint. What is the cost?

Mr Edwards—I would have to pull a figure out of the air, but I could certainly get back to the committee with more substantive figures on that. Certainly, for the registrations it is hard to say because they are in different areas. I will take that question on notice.

Mr CADMAN—That would be a great help in looking at a range of industries.

Mr Edwards—Yes.

Ms ROXON—We would want a typical cost for a particular organisation.

Mr CADMAN—For, say, a medium-sized mail house that might be operating in, say, Castle Hill—not one of the big operations. I have no names in mind, but I know that there are some there.

Mr Edwards—I think the other issue is that, while the association itself is incurring some costs in running the affairs of our authority, it is certainly not to the extent that the insurance body is because, in a sense, our authority does not actually hear complaints from the individual consumers. The authority's job is to make sure that our members comply with the code of practice. Our members are bound to have their own complaint mechanisms in place that deal with the individual complaints from the consumer. If their complaint is not resolved and the consumer contacts us directly then that is when the authority steps in.

Mr CADMAN—So you would not be able to give us an estimate, for example, of the cost to that individual I described?

Mr Edwards—Not the cost within the organisation—for our member company. I could not tell you that.

Mr CADMAN—Have we got any way of getting at that through you, or do we have to go to them direct?

Mr Edwards—We could probably do something. We could look. It is a difficult thing to measure.

Mr CADMAN—Maybe there is a privacy factor here.

Mr Edwards—There could be.

CHAIR—On that note I thank you for your submission and thank you for coming along and discussing it with us today.

Proceedings suspended from 12.53 p.m. to 13.45 p.m.

CORNWALL, Ms Amanda Jane, Senior Policy Officer, Public Interest Advocacy Centre

CHAIR—Welcome. I advise you that, although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. We are in receipt of your submission to the committee and I invite you to make some opening comments.

Ms Cornwall—As you see from the submission, the Public Interest Advocacy Centre is a community legal and policy centre. We are the only organisation of its kind in Australia providing public interest test case litigation and public policy advice on public interest issues. The main focus of our interest in this bill is the impact it will have on the health industry. One of the priority issues for PIAC since its inception back in 1982 has been protection of consumers and advancing consumer rights in the health sector. A crucial measure to achieve that goal is to ensure that consumers have appropriate information to make properly informed choices about their health care and an important part of that work has been to work for consumers to have a right of access to their health records. That, of course, is available in the public sector where most health services in Australia are provided, but it is not available in the private sector.

The Public Interest Advocacy Centre supports a nationally consistent legislative framework for the protection of privacy in Australia and particularly in the health sector. What we have particularly supported in our submission is a separate regime for the health industry. This is consistent with the approach taken in the UK, in most states of the US and in New Zealand, where there is a separate code under the Privacy Act for health and there is not a proliferation of other codes for other industries. Health and police and security matters are always singled out as being quite different in the considerations of protecting privacy. We are quite concerned that, by putting health in with all other sectors in this bill, there will be distortionary effects on health consumers and the health industry.

In particular, I want to draw your attention to the issue of access to records that is provided in clause 6 of the bill. What I would first like to do is just run through some of the other arguments and the need for a separate regime for health. We have not seen in any of the materials in the lead-up to this bill, or in any of the explanatory materials, any public policy justification for putting the health in together with other industries. Because this is quite an unusual approach and it is quite a departure from the practice anywhere else in the world, we believe there needs to be that justification. It has been said that this was the view explicitly expressed, or was the preference expressed, by the Privacy Commissioner in his report on health privacy. However, we would say that the terms of reference of the Privacy Commissioner gave him no choice but to recommend that health should be put together with all other industries.

The nature of the information held in the health industry in personal health records is quite exceptionally sensitive. This is one place where a wide range of very intimate and

personal information is collected together and it is, therefore, a matter of great concern to people that that information is being widely shared without their knowledge of who is having access to it or, indeed, what information is held in that record. A lot of that information leaves people open to discrimination, whether it be because of information about their mental health status or other public health status, or their attitude to doctors—maybe they are rather questioning and regarded as being difficult. There are a whole range of reasons. This is not just about people who might be regarded as marginalised; this is about all of us who might have all sorts of information recorded in our health records that we would not be happy about a wide range of people having access to.

Another concern is that the provisions of this bill do not address the need for regulation of health information online and electronic health records. We understand that the Department of Health and Aged Care are at present preparing legislation to deal with that aspect of health records. It would be better to have one piece of legislation dealing comprehensively with the health industry rather than having some health privacy issues dealt with in a general privacy bill rather inadequately and then separate legislation dealing with electronic health information.

Another particular effect this bill will have is on the legislation in the ACT, the Access and Privacy (Health Records) Act. This legislation is widely regarded as a model for providing access and privacy for personal records in the health sector. It actually reflects the views and consultations around the country at the time that the bill was prepared and we are quite concerned that the effect of the proposed privacy amendment bill would be to override the ACT legislation wherever there are inconsistencies between the federal legislation and the ACT legislation. The ACT legislation appears to have worked quite well. The sky has not fallen in and doctors have not been tied up in all sorts of dramas as was anticipated before it was introduced. What this is flagging is that the Commonwealth bill, in fact, will impact on other state legislation where attempts are made to provide more progressive provisions for access to health records.

One of the issues that we have dealt with in some detail in our submission is the distorting effect of the wide range of exemptions to the right of access that apply in clause 6. While we agree with the exemptions in clauses 6(a) to 6(b), which are basically saying that access can be denied where providing a health record is going to cause serious imminent harm or where it is going to compromise the privacy of others, we do not support the application of the other exemptions in the bill that are fairly typical of the exemptions that generally apply in privacy regimes, for example, where providing access to the record would interfere with a police investigation. We would say that this ignores the reason you provide patients with access to their personal health records. The primary reason for doing that is to improve communication between the health service provider and the consumer. It should never be a relevant consideration that there is a police investigation going on or any of the other exemptions that apply in that clause.

Ms ROXON—Would you explain? I am not sure I understand your point on that.

Ms Cornwall—In health there is a different rationale, we would argue, for providing people with the right of access to their personal records. The primary motivation in health is to improve communication between the doctor and patient. The exemptions that should

legitimately apply should really be only those that would interfere with the privacy of other people or where there is a risk of imminent harm. We believe it is not relevant and not an appropriate exemption that a police investigation is going on, whereas the bill would say that that is a relevant and applicable exemption.

Ms ROXON—And, therefore, access to the records should be provided?

Ms Cornwall—Should be denied. That is what the bill provides.

Ms ROXON—So your point is: a consumer should be able to access the information, whatever the circumstances, if it meets your objective of improving communication between the consumer and the health practitioner. It seems that in health there are two quite distinct issues, whether it is access for your own purposes, if you are the person whose records are being held, or if it is access for other people.

Ms Cornwall—At the moment I am just dealing with the patient's right of access, which is in clause 6. The position we argue is that the only relevant exemptions to a right of access is where the privacy of others is going to be harmed or where it is going to cause imminent harm. These are the typical exemptions that you find in the New Zealand health privacy code, in the UK and in some states in the US. We believe that the other exemptions in clauses 6(d)-(j) should not apply in health, but they do in this bill.

Ms ROXON—I am just trying to think of a situation that you are dealing with on that, but perhaps we can come back to it when you have finished your opening comments.

Ms Cornwall—One of the reasons why we would argue that exemptions other than those provided in (a) to (c) are not appropriate is that it would in fact introduce a standard in the private health sector that is quite different from the public sector. Under freedom of information people have a right of access to personal health records held by the public sector, except where it is going to interfere with the rights of others or where there is, again, imminent harm likely. So we would say that the standard that applies in the public sector under FOI really is the standard that should apply in the private health sector. That is not what this bill would achieve; it would actually provide a much wider range of exemptions.

Another concern resulting from having such a long list of exemptions is that it would facilitate, in effect, the status quo being preserved—that is, that doctors would be able to have a wide range of options from which to choose to base a refusal to provide access to personal health records. The experience with FOI shows and a range of medical literature document that doctors' attitudes remain that patients should not have access to their personal health records—that that is a matter that is entirely in the discretion of the doctor and no-one else should dictate those rights. By providing a list of eight or nine exemptions from which doctors can choose, you are really assisting them to continue with that situation. Another concern with this provision is that, under FOI, where a patient is refused access to their personal health records on the grounds of the exemptions that apply, an option that is made available under FOI is for the records to be provided to a doctor of the patient's choice. Under this amendment bill the only option that is available

is that the agency take reasonable steps to come to a mutual arrangement, which is a significantly lesser obligation than is provided in FOI.

Copyright is another concern, and I am sure a number of others have raised this issue. Because the High Court made a ruling in the Breen and Williams case in 1996 that health providers hold copyright in personal health records, unless this amendment bill specifically addresses that issue there will be some confusion and uncertainty as to whether this bill has the effect of overriding any right to copyright that is understood to exist in the private health sector.

I have also outlined in the written submission a number of advantages to having a separate privacy regime, and these are essentially administrative—that you could potentially have one consistent standard across the public and private health sectors. We have health services being provided in Australia in the private sector at state and territory level and, to some extent, at federal level. At the moment we have entirely different standards existing in each of those jurisdictions. This bill is an opportunity to provide a model that could become a consistent national model if we had a separate health privacy regime rather than trying to fit privacy uncomfortably into a general privacy structure. I will conclude my comments there. I am happy to answer questions.

At the moment we have entirely different standards existing in each of those jurisdictions. This bill is an opportunity to provide a model that could become a consistent national model if we had a separate health privacy regime rather than trying to fit privacy uncomfortably into a general privacy structure. That concludes my comments there, and I am happy to answer questions.

Mr MURPHY—You expressed some reservations about police investigations leading to access to records. I could imagine that in police investigations there could be occasions where the prosecution might need to get hold of certain evidence. Could that not be got around by suppressing the names of people?

Ms Cornwall—No. My concern is that a police investigation be an exemption to the patient being allowed to have access to their records. At present, in clause 6, one of the exemptions to a person's right of access to their personal information is that it may interfere with a police investigation.

Mr MURPHY—Okay. So you are saying in that circumstance that we should protect the rights of the patient?

Ms Cornwall—What we are saying is that the only exemptions that should apply to personal health records are where providing the patient with access to that record would interfere with the privacy of others or where it would cause a risk of imminent harm. But all of those other exemptions that currently apply within this bill should not apply to health.

Mr MURPHY—Okay.

Mr CADMAN—It would seem to me that, as far as private practice is concerned, the only organisation that has access to that information is the Health Insurance Commission with the exchange of provider numbers with the GP generally or the specialist. So the only governmental role really is the insurance role and those agencies. The GP or the specialist has a very great interest and in fact a professional requirement to keep that information confidential. Is that right?

Ms Cornwall—Under the common law they do have an obligation, yes.

Mr CADMAN—Okay, fine. Could you explain to me how a privacy law will further enhance the privacy that I might have with my doctor, provided the health commission and all the research institutes and universities are hedged off by proper protection against my records being released by them because they have got access to my information?

Ms Cornwall—Privacy is often confused with confidentiality, and confidentiality is actually only one aspect of privacy. Protecting privacy requires not just that information be kept entirely confidential—the 11 privacy principles in the current Privacy Act, for example, actually allow disclosure to third parties, but only on certain conditions and in accordance with those principles. At present in the health industry I think it would be quite incorrect to say that information that you provide to a GP or to a specialist is disclosed to nobody else. There is really no effective legal protection from that information being shared with a wide range of others.

Mr CADMAN—Who?

Ms Cornwall—With private health insurance companies, for example, there is no regulation of private researchers having access to that information.

Mr CADMAN—The National Health and Medical Research Council has got—

Ms Cornwall—That is only where that is publicly funded and publicly supervised research—not private health research; that is not currently regulated.

Mr CADMAN—And so access to my records may come through a private insurer who commissions research into certain conditions?

Ms Cornwall—Potentially at the present because it is not regulated. Another thing that I guess people are not understanding—and it is very difficult to get a grasp on it because the change is happening so quickly—is that GPs are increasingly being relied upon to provide a coordination point for a range of allied and community based health services, particularly, for example, where we now have a greater reliance on palliative care being provided in the home. People are going to GPs as just one of a range of providers, and all of those providers in that team are going to be sharing information in the record which increasingly is going to be stored electronically, and this is something that the federal government has actively encouraged through quite significant funding in the last two or three budgets.

Our concern is that, when people find out the extent to which their personal health information is shared, they are going to become very nervous about what they disclose to doctors and other health professionals, because they have no confidence—

Mr CADMAN—The focus in your submission does not arouse that concern in us, because it does not spell it out that clearly?

Ms Cornwall—Our submission is focusing on the patient access to medical records and particularly the issues in clause 6.

Mr CADMAN—I do not think you focus on the threats to privacy for the individual, where they may come from and how the legislative prescription needs to be changed to accommodate those concerns that you have.

Ms Cornwall—That is right, our submission focuses on clause 6, on the issue of patient rights of access to their own records. That is all we have chosen to focus on. We are aware of others who have focused on the third party access issue.

Mr CADMAN—Fine. I move to patients' access to their own records. In group practices, who owns the records, the doctor, the patient or the group?

Ms Cornwall—The patient never ever owns the record unless it is a X-ray or a pathology report, for example.

Mr CADMAN—You make that clear in your submission. That is good. But what about the group or the doctor?

Ms Cornwall—That depends on the legal arrangements, because the hospital might own the records, for example.

Mr CADMAN—So the patient has now a say in that?

Ms Cornwall—No.

Mr CADMAN—Is the patient ever informed of who owns their records?

Ms Cornwall—Probably not. I do not know. We would all have a different experience of that. Ownership is not really the issue for most consumers, the issue is whether the information contained in the record is accurate and—

Mr CADMAN—Well it is for me, if the practice splits and I have some other group cart my records away and my doctor, who I think is my doctor, has got no longer access to my records.

Ms Cornwall—Yes, that is an issue that we came across very strongly in our 1996 study. The Health Care Complaints Commission in New South Wales, for example, has to pay a lot of money each year for storage of records where real estate agents ring them up

and say, 'There was a doctor's practice here, they've gone, we've got these filing cabinets full of records, what do we do with them?' So in light of there being nowhere else, the Health Care Complaints Commission ends up just paying for them to be stored. But they are not meant to be the custodian.

CHAIR—There are going to be a lot of records all over the place.

Ms Cornwall—That is another thing, people have also told us in our inquiry that they had come across situations where they had visited a retired doctor and the records were lying all over the back shed. They had access to anybody's if they wanted them. There is no regulation. This is actually an issue that the New South Wales Medical Board have taken up and they have attempted to impose some regulation now on the proper management of personal health records. There are now some minimum obligations to the period of time for which personal health records must be kept and obligations as to proper disposal.

Mr CADMAN—Obligations on whom?

Ms Cornwall—The doctors and on hospitals. There is regulation in New South Wales of private hospitals and day procedure centres and they actually include a regulation of maintenance of proper records and what should be in them and require them to be kept for a certain period of time. With individual doctors and individual practices, it is much more general, but it is in the medical practice regulations. But that would not be the case in every state, that is only something that was introduced relatively recently in New South Wales.

Ms ROXON—Can I ask you a question in practical terms: I understand that the major thrust of your submission is that it would be preferable for health to be dealt with separately. The fact that this legislation has got to the stage that it has got to and you obviously have very serious concerns about patient information is handled, would it not be more in your interest to have something in place, even in an interim way, even if your long-term goal is to have health dealt with separately? Or do you think that the health aspects of this bill are so flawed that you would actually prefer to have no coverage. I am not saying they are the only options, but would you prefer to have no coverage and wait for whatever the inevitable delay will be for health to be dealt with separately?

Ms Cornwall—There are two aspects to answering that. Yes, we do believe that the provisions of this bill are significantly flawed and there is a serious risk that they would not just be interim, but they would permanently be enshrined. The issues that we have dealt with in clause 6, I think, would be a step backwards, rather than a step forwards in terms of principles applying to patient access to medical records.

Ms ROXON—How is that when you have said that there is currently no coverage for them?

Ms Cornwall—I guess because the practice with a lot of the policies of professional bodies and industry associations tends to be better than this—yes, definitely better than this. As I understand it, there is legislation being drafted in the department of health at

present and we anticipate the delay will not be very long. The introduction of protection of privacy in health would not be a long delay but that remains a hope, I guess.

CHAIR—You seem very confident about that. The Australian Medical Association gave evidence to us last week. They were effectively saying something quite the opposite of what you are saying and put very strongly to us that we should not be allowing this legislation in any way to undermine the High Court's decision in Breen and Williams.

Ms Cornwall—They opposed the bill?

CHAIR—No. They are saying that in a couple of instances it ought to be clarified so that there is no doubt about the copyright and ownership of records and that there is no way in which that should be undermined by this legislation. I am only saying that in the context of what seems to be confidence that some legislation being drafted somewhere else will finally see the light of day and be enacted.

Ms Cornwall—The AMA's position on patient rights is about the most conservative aside from the psychiatrists and the insurance industry.

CHAIR—The question though is you are effectively asking us to largely in effect override the High Court's decision in Breen and Williams. You say in your submission that all six judges said that that was where copyright lay. Whatever we may say about the technical arguments that were advanced in the High Court, I would be highly surprised if any of the High Court judges did not appreciate that this was a case in which access to patients' records was effectively the public policy argument at the basis of the case.

Ms Cornwall—No. The High Court made it very clear that there were not public policy considerations. They were very specifically interpreting the law of contract, the law of negligence and the law of trust. They made it very clear that they recognised that it was out of step with public expectations. On the issue of copyright I cannot—

CHAIR—Having dealt closely with a few judges in my time I do not believe whatever the reasons advanced in the case that judges are unaware of the public policy which is at the base of what they are doing.

Ms Cornwall—I do not disagree on that. I do not wish to argue about that. I would say at present that you cannot have an effective privacy bill if what you are saying is that people can have access to their record but they cannot have a copy of it and only in health and not in any other industry. That would be the current effect of this bill if you are saying that it does not override the copyright recognised in Breen and Williams.

CHAIR—What I am saying, to take up Ms Roxon's point, is that, given that there is effectively no access to records except perhaps in legal proceedings or things like that at the present time and that the doctor has copyright of the records and therefore can exercise that copyright against revealing what is in the records, largely this bill would seem to me to codify that situation if I can describe it that way. It is not taking it beyond that although, given that there is a list of exceptions, if you can find your way around these exceptions

you do have access which you do not necessarily have at the present time so is it not an advance on what there is now?

Ms Cornwall—I think you are confusing two things. Copyright is only a right to copy. It is quite narrow. That is quite separate from being able to have access in any other form. The copyright act only relates to copying.

Ms ROXON—You are arguing against your point before. Presumably people in some circumstances would still regard it as an advance to have access if not a copy because at least it gives people a chance to seek to correct if something is inaccurate.

Ms Cornwall—Let us have a look at the experience with freedom of information. The freedom of information acts are quite explicit. It says in its objects clause—I am speaking about seven different acts, but I am speaking generally—that people have a right of access to records held by government subject to certain exemptions. There is usually a specific provision called the therapeutic exemption which applies to health records and that basically says one of the exemptions is where it is judged that there is a threat to someone's health to provide access to that record. I lost my train of argument now. That is a very explicit right in FOI.

If you look at the Australian Administrative Review Council and the Law Reform Commission report on FOI, it shows that that exemption in FOI has been interpreted consistently against the rights of the applicant, and that has been our experience in New South Wales as well. That is a regime where you have a fairly strongly worded right and you have got the public health sector where you are able to change culture, where you have public hospitals that actually have a structure in place to facilitate patients getting access to their records, and even then the status quo has tended to be maintained because doctors have an attitude against patients having access to their records. So if you want to put in place a clause like you have got in this amendment bill you probably are going to be effectively preserving the status quo because you are doing nothing to overcome a very high bias.

CHAIR—That is what I am saying.

Ms ROXON—That is what we were trying to understand. Is it your view that it preserves the status quo? Is it your view that it makes it worse? Is it your view that if we did not accept your primary position, which is take out health altogether and deal with it separately, just that we should take away some of the exemptions other than the one that you acknowledge being the serious and imminent threat—

Ms Cornwall—It is A to C.

Ms ROXON—I am sure you do understand that we are trying to explore all of these different options so it is important for us to be clear on what hierarchy there is of where you see positive damage being done by the bill, where you see it would just maintain the status quo or where you see it might be at least some improvement although not everything that you would think was in the consumer's interest. I am not really clear

where you are drawing some of those lines at the moment. That is what we are trying to tease out.

Ms Cornwall—I think it would do more damage than good.

CHAIR—Namely?

Ms Cornwall—Because of the circumstances and the bias that already exist.

CHAIR—But what is the damage? If in the private health sector there is no access now because we have not got an FOI against your GP—

Ms Cornwall—Yes, but you have policies of industry associations that are more progressive than this bill—significantly more progressive.

CHAIR—Which health industry associations?

Ms Cornwall—Off the top of my head—

Ms ROXON—You do not have to tell us off the top of your head. You can let us know.

Ms Cornwall—There is the Standards Australia provisions. There is the Royal College of General Practitioners. I have got them listed in some of the material that I have given you as an attachment.

CHAIR—We can check that.

Ms Cornwall—Even some of the public health bodies have policies; I do not know whether to describe them as progressive—

Ms ROXON—More progressive than—

Ms Cornwall—They are basically more consistent with the standards in freedom of information and more consistent with the standards in the public sector than this. I think it would cause positive damage as much because it would cause some confusion. It is introducing yet another standard into an industry that has a wide range of standards. The other codes and guidelines are the ones that exist at state level. The New South Wales Department of Health has privacy guidelines. The Northern Territory government has the Department of Health and—

CHAIR—But is that in the private sector?

Ms Cornwall—No, these are public sector ones.

CHAIR—That is what I am saying.

Ms Cornwall—But I am saying that in the health industry you are looking at a proliferation of policies and standards—

CHAIR—I understand that.

Ms Cornwall—that are generally higher than what this bill would provide.

CHAIR—They exist against a background of FOI.

Ms Cornwall—The public sector ones?

CHAIR—Yes.

Ms Cornwall—Yes, and often state privacy legislation.

Mr CADMAN—There is legislative compulsion behind it.

CHAIR—That is right. The private sector does not exist against a background of FOI.

Ms Cornwall—No, they do not, but they exist against a background of the health industry and some attempt to have some consistency.

CHAIR—Yes, I understand that argument but—

Ms Cornwall—So it would actually be providing an imprimatur to have a lower standard or a more confused standard by enshrining what is in this bill and applying it to health. That is the concern.

CHAIR—So your bottom line is: excise from the bill the health provisions?

Ms Cornwall—Yes.

Mr CADMAN—And apply the public sector provisions to the private sector as well?

Ms Cornwall—To have a separate health privacy legislative regime which, on the issue of access, has a provision that is consistent with the public sector and also which addresses a range of issues that are not addressed in this bill; in particular, the issue of electronic health records.

Ms ROXON—On electronic health records, you made a comment in your opening statement and in your submission that you have a view that shared patient records and unique patient identifiers are already being used within the health system in some parts of Australia without the public being aware of it. What are you saying is being collected that people are not aware of and is being used? Is that the same as the comments you were making at the start—that people are not aware that information is being passed between practitioners in the same general practice?

Ms Cornwall—No, not within the same general practice. If you go to any hospital in New South Wales, as I understand it, and you would need to confirm this with New South Wales Health, obviously—

Mr CADMAN—No, you cannot make assertions unless you can back them up somehow.

Ms ROXON—Let her finish.

Ms Cornwall—You have asked me a question and I am telling you to the best of my knowledge—

Mr CADMAN—Fine.

Ms Cornwall—what the situation is. That is the qualification that I have to make because I can only tell you what I know; I am not here to speak on their behalf. But if you go to any public hospital in New South Wales, as I understand it, as a patient of a number of hospitals in this state, the information that is kept about you in any hospital will be accessible if you go to any other hospital, or any other public health service.

Ms ROXON—Presumably, the rationale for that is because if you turn up somewhere having had a heart attack, they will know that you have had a propensity to it.

Ms Cornwall—And they have got a complete record of your patient history in terms of your contact with the public health system.

Ms ROXON—To the best of your knowledge, that information is just being used and shared within the public health system, not passed on to other people, or sold, like we are finding the tax office does?

Ms Cornwall—That is to my knowledge. Particularly with some of the programs being funded by the Commonwealth government in the primary health care area, where you have allied health providers, you have nurses, you have GP practices, increasingly being encouraged into case conferencing, and there are now Medicare items that recognise case conferencing and encourage it for good health reasons—to have more coordinated care—it means more and more providers are actually sharing information. There are obviously good reasons for that, but there does not seem to be much consideration of whether providers are getting only the information that they need, or whether they are getting everything.

The sort of thing that people can be concerned about is errors. In the medical literature that we reviewed in our 1996 report, out of about six studies, we found on average that about 50 per cent of personal health records contained factual errors and these are only picked up when they are shown to the patient. That can be anything from an error about date of birth, to whether a person is a diabetic, to whether their tumour is malignant or not. This is the sort of information that has been brought forward to us. So errors are quite important. There can be information in records that needs to be verified, that people will be very concerned to hear is being shared widely. I guess I am making two points there.

One is that people need to have access to ensure that the information is accurate, but they also need to have a very clear and relatively simplified mechanism for knowing who else is having access to that information and at some level being able to have some control over that.

Ms ROXON—I have one more question on a specific matter—and tell me if it is not really within your area. It is an issue that we have raised before and it is not to do with an individual's access to their own patient records; it is to do with other parties seeking to access it.

I know that some time ago there was a lot of dispute, particularly from counsellors who were working in the sexual assault area, that their records were being sought by either the prosecution in some sort of criminal case or by a former partner in a family matter. The counsellors, as I understand it, were determined not to provide that information to any court proceedings on the basis that people would lose confidence about what they could tell in the heat of any moment or in the middle of a trauma or whatever. I think it arose because there were lots of cases where women who had been the victims of domestic violence were saying, 'It was my fault; I did such and such, and I shouldn't have, and I wish,' and this was recorded as part of counselling that was being given, that parties were seeking it. Does this bill in any way to your knowledge affect access in those circumstances?

Ms Cornwall—That matter is governed by the Evidence Act or the equivalent legislation in each state. In New South Wales, it has been addressed recently by an amendment to the legislation so that the courts now have a discretion as to whether to allow that sort of information to be admitted in evidence, and there is quite a long list of at least six considerations that the judge is compelled to take into account. That was really regarded generally as the best way. It was too difficult to have a black and white, 'You can have social workers records or you can't, or you can have doctors' medical records or you can't.' Really, it was a matter of having to still leave it to the discretion of the judge taking into account basically competing public interest considerations, and I would not think that this would affect it.

Ms ROXON—That this would in any way cut across?

Ms Cornwall—Yes, I cannot see that it would.

Ms ROXON—Thank you for that. I just wanted to check it with you because I know that PIAC had been involved.

CHAIR—Thank you very much for your submission and also for coming along to discuss it with us.

Ms Cornwall—Thank you for the opportunity.

[2.27 p.m.]

CONNOLLY, Mr Chris, Executive Member, Australian Privacy Charter Council

CHAIR—Welcome, Mr Connolly. I advise you that although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. We are in receipt of the council's submission and can I invite you, if you would like to, to make some opening comments and, in the course of doing so, could you just explain to us what the Australian Privacy Charter Council is?

Mr Connolly—Yes. Thank you very much for the opportunity to appear. The convener of the council, Nigel Waters, had hoped to be here, but he unfortunately could not attend. He was the author of the submission, so I guess I am appearing as his second, so I hope people will go easy on me on that basis. The Australian Privacy Charter Council is a non-profit, non-government organisation that was set up to examine what sort of privacy principles should be applied in Australia in the new century. However, that was set up some time ago because there was a fear amongst both business groups and privacy advocates and consumers that the privacy principles we have inherited from the OECD, for example, are fairly old-fashioned, and this was basically an attempt to set out best practice.

Obviously, the first aim of the charter council was to write the Australian privacy charter, a copy of which is attached as an appendix to the submission, and you will see that it goes further than the national privacy principles. It has a few additional principles and it is not specific to any technology or to any legal regime. They are just the principles of protecting privacy. Some might consider it an aspirational document, but the charter council considers it a work in progress and, for example, the implementation of this act, if it was implemented unamended, would develop a legal regime for protecting some of the principles in the charter but would fall short of others. It is a mixture of advocacy groups and business groups and just ordinary consumers.

That is the brief history of the Australian Privacy Charter Council. It should be noted that the charter council has played an extremely active role in the development of our national privacy principles. The charter council was involved in the negotiations. It was also involved in the core consultative group on the provisions of the legislation before us. It was also involved in negotiations on the exemptions—for example, the law enforcement exemptions that appear in principle 6. So the charter council has had that detailed involvement in the wording of the principles and some of the provisions.

I am happy now to talk to a few key points in the submission rather than going through it at any length. One area in the submission that we only mentioned very briefly but which, because of current events, we would like to spend a little bit more time on is public register information—things like the electoral roll and the Australian business number database now established as a result of the new tax system. The current legislation does

not really deal with public register information in a satisfactory way. We would suggest that it is a large task. There are a lot of public interest issues to be determined as to how public register information can be accessed, and we would suggest that that might indeed be the subject of a broader inquiry than this one.

A good example of a use of public register information that would be seen as a challenge from a privacy perspective is the collection of information for the new tax system in terms of the Australian business numbers and the disclosure of that on a commercial basis for sale. A lot of people who have applied for ABNs are in fact sole traders, consultants, people who work from home and professionals who also do a bit of private practice. On this point, there is a very well-known privacy complaint which was dealt with by the Privacy Committee of New South Wales from a psychologist who had to register as a psychologist in New South Wales. Her information therefore appeared on the register. It was sold by coincidence for $20 to a person who turned out to be an ex-client and an offender who tracked her down at her house and appeared at her house at a time when only her children were home. That person today would probably have had to register for an ABN because she did some private practice and would have provided a home telephone number for contact to the Australian Taxation Office. Again, the information is proposed to be sold for $20. What we are doing here is not really learning from the past. While we note that the Privacy Commission has said it will investigate the matter further, I think that we need to put in place for the long term controls and restrictions over the use of public register information.

Ms ROXON—I would just like to ask a question on that. Clearly, the bill we are considering in this inquiry would not provide any extra assistance in that situation, but are you saying that your understanding about the current legislation is that it is also inadequate to protect the use in that situation?

Mr Connolly—Yes, that is right.

CHAIR—This is the current New South Wales legislation or the public sector legislation?

Mr Connolly—The public sector legislation at the federal level. People will be aware that one of the exemptions within the current legislation is that a publicly available record is not treated in the same way that information collected from a party is. That is an area which is dealt with in our submission. It is not the only problem. I think the current law has not set out a principle or regime for dealing with public register information in a way that has been dealt with, for example, in New Zealand.

Ms ROXON—Is that because 'publicly available record' is being interpreted to include things on a register where parts of it might be publicly available but the rest might not? For example, you were referring to not only today's discussion about the ABN but also the use of the electoral roll for the distribution of information about the tax package and who has access to that detail and who does not.

Mr Connolly—The trouble is that if it is available to the public for, say, one purpose and perhaps in quite a limited way—such as your being able to go to your local electoral

office and view the roll—it then falls outside a more projective regime. As we know, the use of those records can then be done on a more comprehensive basis, perhaps electronically on a disk, et cetera, and commercialised.

CHAIR—With regard to the New South Wales case that you referred to, is there a public record of that and can you give us the citation?

Mr Connolly—I believe the New South Wales Privacy Committee annual report 1996 deals with the matter. The matter was dealt with by a change to the public register in question, which was held by a New South Wales professional body.

CHAIR—On that, you said that the New Zealand legislation does have provisions relating to publicly available records. Can you elaborate on that?

Mr Connolly—I am afraid I cannot. I apologise for that.

CHAIR—We interrupted you.

Mr Connolly—That is fine. The charter council is basically of a view overall, with this legislation, that because we have been lobbying for legislation for a long time we are very welcome to see it and very welcome to see it in the House. Our concerns are that the legislation will not deliver the privacy protection that Australians deserve, mainly because of certain exemptions, and I will spend just a few minutes talking about a couple of the exemptions.

The Privacy Charter Council just does not really understand what the motivation is for the employee record exemption. We suspect that it is partly to do with a compliance burden in that a lot of businesses have employee records, so this is something they would have to deal with even if they are not in the general business of collecting information for commercial use. But as to the privacy principles—such as that the information should be kept secure but the quality of the information should be protected—there does not seem to be any justification for not applying those principles to employee records. I guess what we would like to see is that either the exemption should be removed—and if employer groups come forward and say that it is just too difficult we would be happy to concede that they might need to be given more time in order to apply the NPPs to their records—or that some of the NPPs are applied in a way which ensures that no commercialisation can be made of employee records and that employees will not be prejudiced in that they will not get basic information, basic access to their own files, information about whether they are the subject of surveillance or not. Commercialisation, I guess, is one of our greatest fears about employee records, especially as we move into, for example, a regime of superannuation choice of fund. Employee records are actually gaining quite a deal of commercial value, and seeing them exempt from the Privacy Act would send a signal to employers that this might be something they could make money from.

We are also concerned about the media exemption, and I am sure we are not alone there. The trick with the media exemption is that it seems, because it allows an exemption where information is published, too broad to us. For example, any organisation could structure themselves in such a way that they did publish information in order to deliberately gain an

exemption from the Privacy Act. For example, I am sure members might be aware that there is a gun lobby group that has links to a gun lobby magazine. That gun lobby magazine published the home addresses and photos of politicians' houses on the Internet—people who are advocates of gun control or gun reform. They would be exempt under the current proposal because they published the information in a journalistic fashion—it was a magazine. It was an Internet site that reflected the magazine's content.

What are the options for tightening the media restriction? You either have to pursue a public interest test—is the information in the public interest?—and it is obviously an additional challenge for a privacy regime to introduce a public interest test for a media exemption; or you have to find a more restrictive definition, for example, to news and current affairs. At the moment our view is that the public interest test is worth pursuing in the case of trying to get a tighter media exemption for privacy. Obviously the media are responsible for a great many privacy intrusions, but I think the public has expectations and the public interest test could match those expectations with the law.

CHAIR—I must say I find it difficult to find where you draw lines in this. It is usually Internet sites that are given as examples. Regardless of one's personal view about the motive behind or the content of the Internet site or what they are pushing for, why, one has to ask, is publishing a picture of a politician on an Internet site—to take the gun lobby one as an example—any different to the publishing of a picture of a politician or other public figure with his or family in leading newspapers? It seems to me that the problem here is that it is easy to express moral outrage about groups that we do not necessarily agree with and say that we need to tighten up the laws to deal with them, but if it is published on the front page of the *Sydney Morning Herald* or the *Daily Telegraph* it seems we do not express the same sort of moral outrage. I am just trying to tease out where you draw the line.

Mr Connolly—That is a really useful point and it actually illustrates how a public interest test can be useful. For example, the Internet publication that I mentioned, which is also a magazine, was publishing the home address details and a photo of the houses of the politicians, and obviously their families live there as well. Would you say that that was in the public interest? I think that is different to publishing a photo of the politician when, as you say, that same photo is going to appear everywhere, in the *Herald* and then on the television, et cetera.

CHAIR—I do not want to single anyone out, but I have to to try and take this a step further. Was it in the public interest to publish the well known if not notorious photograph of ex-Senator Woods and his wife at the time of the troubles he was having?

Mr Connolly—At a very important personal moment in their lives.

CHAIR—Talking over the back fence, in the back yard—that sort of thing.

Mr Connolly—The legislation as it is written today precludes an argument even being entered into about whether that is in the public interest or not. What we are suggesting is that the media exemption should be there, but that an argument could at least be entered as to whether that was in the public interest and then, just as all other privacy complaints are

decided, an arbitrator or the Privacy Commissioner would make a decision. That is the problem with exemptions, that we are not really leaving it up to oversight, to anyone to look at; we are actually giving carte blanche to anyone who publishes to take those sorts of actions and be free from oversight. That is quite a big difference.

CHAIR—The alternative approach that has been put to us, I think by the Privacy Commissioner amongst others, is that we ought to have a definition more akin to the New Zealand definition in this area, or even the one in the proposed Victorian legislation.

Mr Connolly—It is open for us to sort of steal ideas from other jurisdictions, but I think it is probably overstating the reality to say that any jurisdiction has actually solved the media problem. We cannot solve in a few paragraphs in this legislation the media exemption unless what we are doing is setting up a body which can have oversight and can develop expertise and precedent, et cetera. If there is a public interest test, the chances are that, under the regime as a whole, it would be administered by, for example, the Press Council under an industry code and they would develop expertise, and people who thought the Press Council had got it wrong would be appealing to the Privacy Commissioner.

Ms ROXON—That is what I was going to ask you, because presumably even if the media was covered by this legislation the existing codes of conduct that they do have would be what would be put forward as the appropriate standards and I think that most of us do not think that the current standards come anywhere near to what is being expected in other areas.

Mr Connolly—They would have to match the NPPs and their content. That would be the difference. What we are doing by exempting them is leaving it to the current status quo of those documents and there is no way, as you say, that they would match the content of the NPPs.

Another exemption that we are concerned about—or there are two, and I will speak about them more briefly—is the small business exemption. Our concern here is that, as a group which is advocating privacy protection, we play a role in educating and informing the public about how well privacy is protected. The small business exemption is the one that really scares us in that we will just have to tell people that they do not know whether the act applies to that transaction and they do not know whether the act applies to that collection of information—unless they can work out what the business's turnover is or unless they can work out that they also meet the other part of the small business exemption. That is really going to undermine confidence in new technology companies which will not have that sort of turnover and in electronic communications et cetera. Often that sort of undermining of confidence will have a wider impact for all businesses. It is important, I think, for this committee to get to the bottom of how many businesses will be covered by the act and how many will not be. On the figures that we have, we now know—through the ABN process—whose turnover is more than $3 million. If that information is in your report, people can make a decision about whether they want a privacy act that applies to only 30 per cent or to 70 per cent of businesses, or whatever. I think that is really important information to get and I think it is now available.

The final exemption I want to talk about is the exemption for use by related corporate entities. Here I should confess that, as well as being a privacy advocate, my full-time job is a role in consumer advocacy in the financial services area, which often involves pursuing companies that have been involved in scams or mis-selling et cetera, and trying to pursue their directors to get damages. The law which we use there is the Corporations Law definition of what is a related entity and, as a consumer advocate, we want it to be as wide as possible and to catch as many as possible directors, linked companies, holding companies and people who have managed to structure their business to hide their assets et cetera. Unfortunately that is now a test that is going to be used in the Privacy Act to exempt transfers of information between related entities. So we have actually got a test which, for one purpose, has been set up to be as broad as possible and we have picked it for the Privacy Act when obviously the privacy protection would best be served by a much narrower definition of what is a related entity. There is a real challenge there that consumers will have absolutely no idea of the intricate and complicated links between different corporations, especially where holding companies are involved. If the information is transferred and is exempt then they are going to be losing their privacy protection in very unexpected circumstances.

Ms ROXON—But are there not exemptions to the exemption if you are passing on the information to related corporations for use for a different purpose?

Mr Connolly—Yes, this is what I am getting to. If the intention of this clause is to say that, if information is going to be for a different use, you are not exempt, then we cannot see any reason why the existing NPP2 just does not apply to everyone and why the exemption is given because in the existing NPP, if the purpose is unrelated and without consent, then it is disallowed.

Ms ROXON—That does not follow, I don't think. Aren't the provisions seeking to allow the transfer of the information to a related corporation for whatever the approved purpose was for collecting the information to start with? So the magazine publisher provides the information to the related corporation who is the distributor, for example, to ensure that when you have ordered the magazine you can get it delivered—I am trying to think of an example—and you want those related corporations to be able to pass that information between each other, but if you were providing that information to the television station or something, not for anything to do with the ordering of your magazine, then even if the company was related, you would not fall within this exemption—I think.

Mr Connolly—The Privacy Charter Council's argument is that in your first example, NPP2 would apply anyway and that it would be an allowable transfer.

Ms ROXON—You would get the protection through that?

Mr Connolly—Yes.

Mr MURPHY—Just raising Mr Waters's submission on this topic, he said inter alia:

The structure of corporate groups is usually quite opaque to consumers and often bears no relation to functions, activities or lines of business.

Ms Roxon gave the example of a publication being handed then to a distributor. Can you give me an example of a product, or some sort of parallel situation as illustrated by Ms Roxon, that would support your concern. Quite plainly, Mr Waters says that there is no justification for this broad exemption from the application of the collection and use and disclosure principles to transfers of information between organisations simply on the basis of an arbitrary company law association.

Mr Connolly—I think that there are some examples out there of where the consumer would have absolutely no understanding of the relationship.

Mr MURPHY—I am sure of that.

Mr Connolly—It is difficult to give them in this sort of setting without appearing to be critical of particular companies. But if, for example, a person purchased, using a credit card, tickets to an event through a ticketing organisation, and that ticketing organisation happened to be owned through a holding company structure by a media company, and that media company happened to also own a merchandising franchise in a sports club, people might make the link between this person being interested in AFL because they bought tickets to an AFL match; the merchandising company for an AFL club would be able to get their address details et cetera and approach that person for targeted marketing, and the consumer might think, 'How on earth did that company know about my personal records? I have never had any dealings with them.' In their mind, it might twig that there is a relationship. Obviously, I am trying to be as diplomatic as possible, but the structure exists but without the knowledge or expectation of most consumers.

Ms ROXON—I have not found it necessary to be diplomatic today, so there is no reason you should.

Mr Connolly—I guess what happened in discussions about related entities last year and the year before was that a lot of people had in their minds an example like AMP Bank which has AMP banking, AMP insurance, life insurance, et cetera. To me it is less opaque to consumers that perhaps they are a bank customer. They might have expectations that perhaps related insurance companies might have access to information. I think that they were the examples we were using. There are much more complicated corporate examples once you introduce the Corporations Law test—it is just incredibly broad, for very good reasons, but I am not sure that it should be the test in the Privacy Act.

CHAIR—There obviously has to be some exemption here but, as I understand you are saying, you think this one is too broad?

Mr Connolly—There are two arguments: either that we just use NPP2, because in most circumstances you will either have consent or it will be a related use, or we drop the current test of what is a related entity and come up with something which includes a limitation to what would have been the expectations of normal consumers.

I am happy to finish up by linking our submission back to the charter by talking about what we see as potentially a weakness in how the enforcement of this will be structured. Obviously, we are very concerned to see that privacy protection is there on paper, but even

more importantly that it is enforced appropriately. Having said that we will rely on industry codes to a great degree, we are very concerned to see that consumers have adequate appeal procedures. We are hoping that the Privacy Commissioner is able to receive appeals from any of the industry association codes. We see the Privacy Commissioner as having a role in developing ways to improve, based on complaints. If one person is seeing all of these complaints they will be able to say, 'That's what's going wrong there.' But also in the current discussion there appears to be a reliance on codes of conduct and their alternative dispute resolution schemes meeting some government set standards or benchmarks. The only benchmarks available to date are for alternative dispute resolution schemes. They are out of date and were due to be reviewed this year, but the review has not begun yet.

Ms ROXON—Which industries are you talking about?

Mr Connolly—It covers everyone. The ADR benchmarks were issued by the then Department of Industry, Science and Tourism, which has now changed its name many times. They are the consumer affairs division of Treasury. There just seems to be a lot of reliance on those benchmarks in this legislation. I think it is important to flag that they are not the subject of any confidence amongst consumers who use ADR schemes. There is no testing of those benchmarks against any ADR scheme on a regular basis. It is not like you are audited against them. Where they occasionally are, the reviews and recommendations take a long time to be implemented.

Ms ROXON—Could we ask you specifically about that because we had evidence—and it might be with your other hat on that you might be able to answer this—from the Insurance Council of Australia that they were very confident about their industry ADR scheme working successfully. In fact, they proposed that that should be a model that is used for any code that would be set up to cover the insurance industry or others under the privacy legislation. Do you have a view about how effective it is?

Mr Connolly—If I am allowed to switch hats momentarily, the consumer movement is a big fan of the Insurance Inquiries and Complaints Scheme, which is the scheme you are referring to, and we hold it up as the benchmark for—

Ms ROXON—Who is 'we' when you say that?

Mr Connolly—I am the Chairman of the Consumers Federation of Australia, which is the peak body for national consumer groups. We have a lot of problems with other ADR schemes. Our real fear is that it is much more consistent to have a single complaints scheme for privacy. We have not headed down that path. So now what we need to do is to make sure that we have methods for ensuring the quality of the different ADR schemes which are going to be out there, like the press council and the Banking Ombudsman and the Credit Union Dispute Resolution Centre, et cetera. How is it that we will be able to ensure that all of those meet satisfactory standards? It is all very well for the insurance companies to say, 'We belong to the best,' but there are a lot of other ones out there that do not.

CHAIR—Could I take up that point that was being advanced by the Insurance Council? They are opposed to the ADJR review process applying to themselves and say that that will cause problems because, firstly, the legal nature of what they have got in place will change because of this legislation and, secondly, just from a practical point of view there will not be the incentive for parties to feel bound by determinations that are made and so they would prefer not to have the ADJR.

Mr Connolly—Yes, I am well aware of the issue and it has been under discussion. I guess the industry dispute resolution schemes that work well have a level of informality that makes them very cautious about themselves being subject to any legal oversight based on any particular legal principles. They really are much more informal but that has advantages because it makes it affordable for consumers to use those complaint services. Then, in addition, the insurance companies agree not to appeal; they agree to be bound by the decision. Now that it is open for this review, that appears to them to be a disincentive to be bound to these decisions. They do not mind being bound to a decision by the AEC, but they are not so sure that they want to be bound to a decision by a tribunal that they do not have any experience with.

I think those issues can be worked out. I do not think they are insurmountable under the current structure. I guess what needs to happen though is some recognition by the appeal body—in this case, the ADJR—that they cannot review the insurance inquiries and complaints scheme in the same way that they would review the fair trading tribunal. They are not set up as court or tribunal structures. I think that it is really not impossible for them to do that, for them just to say, 'Here are the terms of references of what these ADR schemes do. Here are their day-to-day operating procedures.' As long as those were followed—and, in our experience, with some schemes sometimes they are and sometimes they are not—then I do not think they would then necessarily apply another layer of legalese to what those schemes do. On the question of whether you should still be bound by the decision, I think if the ADJR could come forward and say, 'That is the sort of thing we are going to look at,' that would reassure the businesses and they would continue to be bound by the decision.

CHAIR—You do not think that those who are making decisions under the ADJR are going to be, because of background and training, legalistic in the way in which they approach it?

Mr Connolly—There are two answers to that. One is that if there were no roundtable discussions, training or exchange of information, yes, they might be too legalistic. But, second, my answer is that it would be curable. For example, a lot of people who sit on panels on industry dispute resolution schemes are actually ex-judges and they start off being quite legalistic but they soon get the hang of informality which is required to deal with the sorts of consumers who come forward to those schemes.

CHAIR—Is another option to not have the ADJR process but have some sort of review by the Privacy Commissioner?

Mr Connolly—That is a very attractive option. I think that the more review powers, the more appeal powers that are held by the Privacy Commissioner, the better. I guess we are

trying to promote this idea that the Privacy Commissioner could develop a corporate knowledge about what is going on out there. The more matters that come to the Privacy Commissioner, the better.

Mr CADMAN—I have got a real fear that the ADJR process would be an excuse for the insurers to up the ante and say, 'Let's pay some sort of cursory acknowledgment of our industry dispute resolution process but really we are heading for the tribunal, and it is legal.'

Mr Connolly—I am not sure that that is a fair assessment of how companies think about complaints. Most companies do not want complaints to drag out. For example, in the insurance industry, most complaints are dealt with—

Mr CADMAN—But they wouldn't because the consumer would not go to that extent.

Mr Connolly—What you are suggesting is that the industry would like to drag out matters so that they get—

Mr CADMAN—Get it settled without ever appearing.

Mr Connolly—I just do not think that is the case. Everything acts as a filtering process. Insurance companies under their code are required to have an internal dispute resolution process. By the time it has got to the insurance inquiries and complaints service it has already gone through one other process. That is why the IAC make a decision. I would be very surprised if there was much interest in dragging out complaints and attracting more publicity to them. It is not really the nature of how privacy complaints are dealt with. There is often not money involved. It is not a question of financial settlements although it is in some cases. There is not great motivation for either party to drag out a privacy complaint. If privacy has been breached, you want it dealt with reasonably quickly.

Ms ROXON—You made some comments about enforcement where you said your preference would be to see the Privacy Commissioner have some role in both reviewing decisions from industry processes and in the formation of the principles to start with. I am just concerned about how many hats the Privacy Commissioner can wear. A number of the witnesses want the commissioner to play the role of doing everything. Can the Privacy Commissioner be creator and adjudicator in all of these things given that they are the traps we have fallen into with other similar forums? All we do is make them totally unworkable and unenforceable.

Mr Connolly—That is a really good question. Part of the problem with it is that we see the Privacy Commissioner as a person rather than an office. They have the current ability, for example, to deal with complaints about credit reference where they were involved in the promotion of the law on credit references. They are involved in reform, they are involved in training about credit reference, they are involved in education to consumers about credit references et cetera, but at the end of the day if there is a complaint and it gets appealed it goes to the Privacy Commissioner's office and they do deal with it. That is a structural issue for the commissioner's office. At times their structure has changed. They have had a policy section, a training section, a compliance section et cetera. It is an office

rather than a person but we tend to talk about the office as the commissioner and I think that—

Ms ROXON—It has not helped other offices in similar ways not breach our own constitutional requirements about not being an administrator and having a judicial function at the same time and doing everything else. Will we not just fall into the same difficulties if we try to do that even with the whole office of the Privacy Commissioner not just the person?

Mr Connolly—It is a risk but there is also a risk in them not having multiple roles in that they become isolated and just do one task. For example, because the Privacy Commissioner's office is going to play such an important role in education it is important for them to know what is going on in complaints to see where the education gaps are. There are risks on both sides. It is pretty clear that we are in favour of the commissioner and the office taking on a more active role in each of those areas.

Ms ROXON—It does not matter what the risks are. If it means that they are unconstitutional or unlawful in some way, it will not help. I can see the public policy reasons for doing it but whether we have the power to or not is a different thing.

Mr Connolly—There are probably some interesting lessons there from the Superannuation Complaints Tribunal legal action as well. That legislation knocked out the Superannuation Complaints Tribunal for a few years and was a major blow to consumers who had complaints. When you say there are constitutional risks, if I switch hats again and wear a consumer hat, I will say it can be really devastating if you do get a constitutional challenge. And now they have got a backlog, which will take them years to fix.

CHAIR—I take it that there have not been any problems constitutionally in relation to the credit—?

Mr Connolly—No.

CHAIR—There have been no challenges?

Mr Connolly—It has not come up. You could ask the Privacy Commissioner about that, but I am fairly certain that that has not come up. The commission has this sort of multi-tasking role in terms of credit under part 3A.

CHAIR—Mr Connolly, I thank you for the submission and also for coming along and discussing it with us.

Mr Connolly—Thank you very much.

Proceedings suspended from 3.10 p.m. to 3.20 p.m.

SMITH, Mr Christopher Robert, General Manager, Postal, Consumer and Government Affairs Australia and New Zealand, Reader's Digest (Australia) Pty Ltd

CHAIR—I welcome Mr Smith from Reader's Digest. I advise you that, although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. We are in receipt of the submission from Reader's Digest. I invite you, if you wish, to make some opening comments.

Mr Smith—I will keep them fairly brief because a lot of the information is there. Reader's Digest is one of the world's largest direct marketers and, in fact, a practitioner of direct marketing, with involvement in privacy for many years. We carry out our marketing activities in 40 countries, selling a wide range of products. Many of those countries in which we operate already have privacy laws in place and some are in the development stage in reviewing consumer protection laws. Therefore, privacy is not a new concept to us; it is a good business practice. Reader's Digest has been around since 1922, so we have had a lot of involvement in development.

Here in Australia, we have about one million active customers. An active customer to us is someone who has purchased within the last 12 months. On average, we generate 20 million promotional offers a year to customers and prospective customers. Therefore, we are quite a large customer of Australia Post. We were involved in the evolution of the New Zealand Privacy Act, which went through a number of stages, and also with the Hong Kong ordinance. Within the last several weeks, we have had discussions with members of the Singaporean parliament on the development of some new consumer legislation there.

I have been involved with privacy for about the last 10 years and attend all the Privacy Commissioner's meetings each year as an observer. I also chair one of our regional government affairs committees, where we look after from New Zealand to India and across to Japan. Reader's Digest has been involved in the development of the national privacy principles and I was a member of the Attorney-General's core consultative group.

We as an organisation support the bill. We believe it meets the balance required for consumers, business and government to be able to achieve their objectives in accordance with OECD guidelines. Rather than talk about aspects of the bill, I thought it might be more appropriate to answer questions. I will just make a couple of comments on what I heard earlier.

The New Zealand legislation has provision for codes but, in operating since 1993 under the New Zealand Privacy Act for our New Zealand customers, we have never had to look at developing a code because the principles, which are very similar to the Australian one, are workable for business to operate without having to be very specific in the code. Basically, the only codes that have been developed in New Zealand are those that are put out by the Privacy Commissioner himself, mainly relating to health and police, and I think there is now a telecommunications one.

One of the other interesting aspects of the New Zealand legislation is that there is a requirement for each company to appoint a privacy officer—and that may be a point to include in this legislation—which then gives the consumer or the Privacy Commissioner's department a point of access in every company, so that someone is actually responsible. The biggest thing with privacy is actually getting the word out to the people in the company as to what they should be doing, and that becomes one of the roles of education. Education is a key component of privacy.

I heard a question earlier about publicly available information, which is in the New Zealand act. Basically, you can use publicly available information if it is already publicly available. The key to it is that once you have used it once you have actually enhanced that information and therefore it is no longer publicly available, that is the way that is used.

CHAIR—Just on that, take a hypothetical example—if it is not appropriate I will try to think of another one. If Reader's Digest were able to access the electoral rolls, which are publicly available, and then use them to send an offer to potential subscribers, you would not be able to do that again unless you met the requirements of the legislation. Is that how it works?

Mr Smith—Basically, if you took the electoral rolls and used the name and address portion to derive a mailing list, once you got replies from the people you have enhanced the list because you know people are responsive. That moves it away from publicly available, but the rolls could be used again with another set of names.

Ms ROXON—But that does not mean another set of names. Provided you had unlimited funding you could keep sending offers—offer A one week, offer B the next week and offer C the next week—and it would not matter whether people responded to the first one or not.

Mr Smith—You could if you had the funds.

Ms ROXON—That is a hypothetical case we will have to deal with if we are looking at the privacy considerations. You can keep using the publicly available information?

Mr Smith—You would not do that, though, because you would not run a business that way.

Ms ROXON—Only because it would cost a lot, not because you were worried about upsetting people.

Mr Smith—Also, you need a mixture of types of information in a mailing list. You would have your core customers who make up the majority, and you know they respond to certain products, but there is a top-up that you want to put in to get new customers, so you would take portions of, say, a telephone list.

Ms ROXON—How do you, for example, get that information to start with—not for your existing customers, for your new contacts?

Mr Smith—There are several ways. One is that you could compile a list, and that could be from the telephone book or from the electoral names and addresses, or you could rent a list from another company—the names and addresses portion of their database.

Ms ROXON—What is the difference between renting it and just using it?

Mr Smith—It has a value. If a marketing company has names and addresses they are normally of people who have responded to a promotion; therefore, they have been enhanced so there is a value on reach and frequency of an offer.

Ms ROXON—I understand you would have to pay for that, but are you saying 'rent' because organisations let you use their information once but they do not let you use it again?

Mr Smith—Yes, you rent on a one-time basis.

Mr CADMAN—You never get the original data?

Mr Smith—No.

Mr CADMAN—And you cannot enhance their data?

Mr Smith—All you have is a name and an address, so you are really running it through one of your promotions.

Mr CADMAN—And if they reply they reply to you; therefore, it becomes your asset?

Mr Smith—Yes.

Ms ROXON—Presumably the ones that you rent are already selected out for some reason. Otherwise you would just use the telephone book or the electoral roll.

Mr Smith—No, because it is not that reliable. That is why when you a compile a list you make up certain components. You have to get a return on your investment.

Ms ROXON—I am sorry to say that you have a very poor return on your investment with the mail I constantly get. I am mystified as to how I am on your list, but I am and I am very interested to know how you do that. No doubt you will not be able to tell me the answer to my specific case, but that is why I am interested.

Mr Smith—I could do. If you like to give me the details, I can tell you exactly.

Ms ROXON—It worries me more that you can do it that easily.

Mr Smith—No, no. That is our business and to take your point, we should know where we got your name and address. I mean you could pick up the phone and ring—

Ms ROXON—Or more importantly I should know.

Mr Smith—It may become obvious when—

Ms ROXON—When you tell me. Anyway that is my personal situation. It is really nothing to do with it. What I am trying to get at is where you get information from because presumably that renting example that you have used will be subject to all of these provisions in the future?

Mr Smith—Correct, yes.

Ms ROXON—And you have said in your submission that you are happy with that. You have not said, I do not think, in your submission whether you actually are subject to the direct marketing code of practice.

Mr Smith—We would be because we are a member of ADMA.

Ms ROXON—And that is automatically part of it?

Mr Smith—Yes. But these principles we have actually operated on for many years. We do not actually rent our own database but we do tell people what we use the information for. In our terms of offer we tell people that we have their name and address, we use it for marketing purposes and running a customer raffle and if they do not want to receive any—

Ms ROXON—This my problem, it is not opening a letter.

CHAIR—I was going to say I, or my wife or someone in the house in which I live, have received information from Reader's Digest and so presumably, amongst all that information, between the two car keys and the gold token and the—

Mr Smith—I see, so you have looked at it.

CHAIR—I have looked at it, that is right. Presumably in there there must be a page of terms and conditions that tell me if I bothered to read it that I could have my name taken off your list?

Mr Smith—Yes. As simple as that.

Mr CADMAN—One way to get it off the list is to say you want the prize but you do not want to pay any money for the subscription. That works—you do it three times and you are off the list.

Ms ROXON—No, but the serious question is how people get on your database to start with—where do you get that information from and we are only seeing you here giving evidence as an organisation that operates in this area and I think your evidence is you either buy it from people, buy use of it for a particular—

Mr Smith—You rent the use of it.

Ms ROXON—which is the same thing, or you get publicly available information—

Mr Smith—Or you have got existing customers.

Ms ROXON—or you have got existing customers.

CHAIR—*Reader's Digest* has traditionally been the package you get in the mail that we are all aware of. To what extent, Mr Smith, is *Reader's Digest* moving into email?

Mr Smith—Six months ago in Hong Kong we tested a new Internet mailing system. We own several financial magazines in the east. The base of one magazine has its email address component, and we have been able to do a package exactly like you say with the keys and people can go and click on all the parts, turn the pages, move the key and stick it where it has to go—what we call action devices; it takes you through a package. That has been very successful and we are looking at one now for Australia.

Globally we have a lot of strategic alliances. Reader's Digest is a fairly low key company. It has been a household name for many years, so we do not trumpet what we do, but we tell all our customers what we are doing. That is why on all our offers you will find if where we have just launched some insurance product here in Australia as a joint venture with the American Insurance Group we state that it is Digest and so on. So we are moving into some of these new fields. We also have homehandyman.com; we have RDhealth, which is a joint venture with webMD in the United States; we have gift.com—

Ms ROXON—If I can just stop you there, do you understand that the provisions of this bill, if they came into effect, would allow you to use information that you have obtained from any customer? So if I break all historical records and actually open one of my envelopes and order a magazine, you would then think you would be complying with the provisions of this bill if you sent me the information about your own insurance, about handyman.com and gift.com, because you would be only using it for your purposes?

Mr Smith—For Readers Digest products, therefore for our purposes.

Ms ROXON—Even though I as a consumer presumably think I am on your database for buying a magazine? What do you ask people to consent to by doing that and staying on your database? If you have got an opt-in and opt-out process—

Mr Smith—It is opt out.

Ms ROXON—What are people told they are signing on for, though?

Mr Smith—We tell people that we will use this information to supply them with information on goods or services that they may be interested in; if they do not want to receive them, just let us know and we mark the files accordingly.

Ms ROXON—But what I am saying is that you do not ask people to consent to a particular part of your business in any way. Presumably the strength of an organisation like yours is that, once you have someone on your database for a particular thing, you can actually market to them all your other products.

Mr Smith—Most of our products, let us say, inform and inspire their entertainment—magazines, books, music, videos and so on.

Ms ROXON—It would be stretching it to think insurance was part of entertainment.

Mr Smith—Yes, but it is just part of a natural progression into other parts of the business we are forming because our name is valued and trusted.

Ms ROXON—Or because of your access to information; it is a good marketing tool. I can understand from a business perspective—

Mr Smith—But people rely on the company as well.

Ms ROXON—What I am asking you is what privacy protection—given that is what we are inquiring into—an individual has if they sign on for a particular item that then opens them up to being on your list for absolutely everything?

Mr Smith—No, only what they are interested in. If they do not respond to a certain thing or say, 'We are not interested in that,' then we do not promote that to them. It costs a lot of money to—

Ms ROXON—You mean you do it once and if they have not responded to it you do not do it the next time?

Mr Smith—We might try a magazine. The way Digest works is that the first mailing anyone gets is to the magazine, because that is what we call the flagship product. If people subscribe to the magazine, we know they are interested in reading, so then we might try them with a book of one sort or a series book, which is condensed stories from well-known authors.

Ms ROXON—What I am trying to get at is: if someone says yes once to one magazine, are they then on your list for any new item that comes up for an indefinite amount of time? You have said no to the book, but then you get the CD which you say no to, then you get the insurance which you say no to, then you get the something else which you say no to. Basically, are you on the list?

Mr Smith—Your name could be on the list but you are not going to get promoted—maybe once a year if there is a new product similar to one you bought earlier.

Ms ROXON—I think I have got my answer.

Mr CADMAN—Let us see if I understand what you are saying: it is a waste of money for you to mail her about wine and overseas trips if she is interested in books?

Mr Smith—Correct.

Mr CADMAN—So, from a business point of view, you will hit her for books and that alone until she shows an interest in something else, and then you will target that as well?

Mr Smith—Correct.

Ms ROXON—Except I will get sent everything to find out.

Mr Smith—No, not necessarily. If you do not respond to certain promotions, then you will not be targeted again for a year, when there might be a new product and then we will send out a new promotion.

Mr CADMAN—So it is not really cost effective for you to have her targeted for everything that moves?

Mr Smith—This is why, if I can go back to the way our list is compiled, you have to have some components in there of people you know will buy, and then you put in these other names and addresses that you are prospecting to. Then the profitability is held up by the core and you bring in some of the new customers. If they do not respond, then you do not promote them. A mailing package with postage is around $1,800 for 1,000 to produce and get in the mail.

Ms ROXON—Sure, but your commercial interest dictating what my privacy interests are is not really a reassuring situation.

Mr Smith—No. Whatever you tell us, we will tell you what we are going to do with your information. You can have access to it. You can see your customer record. If you do not want to be promoted, we can mark the file 'do not promote'. We do not remove the name and address because 'do not promotes' are flagged so that if names and addresses come in from another source and are matched against our database, the flag tells us not to promote that person.

CHAIR—You are also a part of the ADMA 'do not mail, do not call' service?

Mr Smith—Yes.

CHAIR—Just out of interest, roughly how many people a year would, through that, say that they do not want to be mailed or called?

Mr Smith—I do not know the exact figures. We take the entire file and we run it against out database. What often happens is that you find that you have got some active customers in there as well. So we write to that customer and say, 'We have picked your name up off the Direct Marketing Association "do not promote" list. Is this your wish?' Often they will write back and say, 'No, I did not mean you'—

CHAIR—You meant someone else.

Mr Smith—but we run that file and we take action to accommodate.

Ms ROXON—Can I ask you about the provisions about existing databases because some of the other witnesses have said that it would be impractical, unless they had a very long lead-time, to be able to ensure that their existing databases complied with this legislation. I presume that you are confident that your existing practices comply with what is proposed in the bill in any case so that you would not actually have any lead-time problems. You would not have any objection to it applying to your existing database?

Mr Smith—You would apply it from when, say, the enactment took place. What was on the database prior to that would be very difficult to control under that regime because the data is active and every time a mailing went out and data came back it would have to comply. But if you are not mailing it then we talk about grandfathering that data. After three years that data is really non-existent because of the way the population moves.

Ms ROXON—You do not think that your existing data complies and you would not—

Mr Smith—All our data complies. Because we run New Zealand from here our databases are set up—

Ms ROXON—To be consistent?

Mr Smith—to be consistent. But for data that exists prior to the enactment, companies would really have to have an audit team come in and search every record and basically put a marker on to say, 'This is prior to 1 July. Here is data after then.' The cost of doing that would be astronomical.

Ms ROXON—You could do it with a few keystrokes, couldn't you?

Mr Smith—Is it that easy!

Ms ROXON—I seem to be able to do it on my database. I am sure it is not as large but dating things is not very difficult. You do not make any comments, I think, in your submission about existing databases. Others have objected to there being an exemption for existing databases. Some witnesses have said that they think there should not be an exemption but just a time frame for which they have to be brought into compliance. I am just trying to understand what your view is on how existing databases should be treated.

Mr Smith—I know the point you are making. There is no legislation I know of in the world that has applied privacy legislation to information gathered prior to the enactment date. I go back to my point that information to be accurate and up to date has to be used. If that information that was on the database from 1 July is never used again it is non-existent after three years.

Ms ROXON—But presumably, considering you can mark every time you mail out to someone every response you have, it would not be over time a massive burden for your organisation to ensure that they had at least at some point sent another letter to say, 'This

is what we have on the database; the privacy bill is now legislation; do you want X, Y and Z'—or whatever you might say?

Mr Smith—If we sent our promotion after 1 July, let us say—it sounds like a nice date—everything then would have to comply with the prior scheme, so that information, even though it has come out of the existing database, would then be flagged as complying with the legislation, but if you did not use the information prior—

Ms ROXON—This might be wrong, and other members can ask their questions, but I understand that there is a difference between what you would do after 1 July—if, say, that is the magic date—and that was your first contact compared with what you might do after 1 July if you are using information which is in an existing database which you want to ensure complies with the new legislation, so it would not just be a matter of having your standard opt-out provisions or whatever; it would require more than that, I think.

Mr Smith—No, you would not.

Ms ROXON—You might be able to help me here with whether that is what the legislation, the bill, says. You may not be able to, either.

Mr CADMAN—You say you comply now. What is different after the enactment date?

Mr Smith—Nothing really, but what I am saying is that that data that exists now, when you send it out after 1 July, if you use some of the existing data, then you ensure that all the opt out, the access regime and so on—

Mr CADMAN—But if you comply, surely you can get an audit note to say, 'These are the principles that applied to our existing data; we can exempt the lot now because it complies.' Is that what you mean? The whole lot of it complies even though the enactment date may be some time in the future, but you could write a note now to say it will all comply with the new provisions to be enacted on 1 July.

Mr Smith—We probably could but—

Mr CADMAN—You would not have to get these records because your principles would apply, the procedure would apply.

Mr Smith—Yes, you are quite right. It is an ongoing process, so the information would be complying. It is information that you do not use, as I say. It would grandfather and become inaccurate. You would not use it after so many years.

Ms ROXON—Let us go back. Is it not different? Say I am on your database for having bought the magazine, but I have not responded to anything for three years. Post 1 July you go to mail out something; you are mailing out a new bargain on some new magazine and you think that I am a potential buyer because I have bought a magazine in the past. All you have to do, as I understand it, to comply with this legislation for an existing record on a database is make sure that in that letter there is an option for me to say, 'No, thank you, I do not want your new magazine'?

Mr Smith—Yes.

Ms ROXON—What I am asking is, is it really impossible for you to actually undertake more than that? That is, post 1 July, you will say, 'Okay, I haven't made any contact with this person since this new legislation has come into place. What I really should do as well as offering the new bargain on the new magazine is say, "I have you marked on my database as being interested in the magazines; can you confirm you want to stay on my database for that reason or will I have you marked as not wanting anything except Y magazine"?' That is what people are going to have to do in other areas with new contacts. That is quite different to sending out something which has a standard log in as if you were a new contact. Do you get my point?

Mr Smith—Yes, I take your point. The thing that would be prohibitive is if, on 1 July, you had to write to everyone on your database and say, 'You are there; can we have permission to mail you?'

Ms ROXON—I can understand that, but that is why I was asking, as long as you know who was on your database pre 1 July, you know when your first contact is post 1 July, and when you eventually get to that, whatever a practical time frame is, would there be anything that would be that difficult to include?

Mr Smith—We are already doing it now. For a number of years we have been doing exactly what the legislation is suggesting, which is to tell people what you are doing with their information, give them the option to opt out and not receive any further information, and tell them how to access that information. We would carry on doing that.

Ms ROXON—If this process and the legislation come into place, existing databases will have to comply, but over a time frame of 12 months. That would not create any difficulty for you?

Mr Smith—No, none whatsoever.

Ms ROXON—Do you have a view on what time frame is realistic?

Mr Smith—Twelve months would probably cover that. In New Zealand it is three years. That is why I go back to this grandfathering. If you did not use the information, after three years it is useless.

CHAIR—So when the New Zealand legislation was enacted it provided a three-year sunset clause for existing information?

Mr Smith—Yes. That was mainly for direct marketing. That is one of the direct marketing exemptions.

CHAIR—Three years would seem to be such a length of time that, if you are direct mailing and in business, you would churn through your list. Even in your examples of one year, it might be tight if you have got someone who has not responded before 1 July. You say, 'We're not going to put this person back until another offer comes around that might

match what they came on for in the first place.' That could be longer than a year, I suppose.

Mr Smith—Yes. We would generally mail a person once a year if they have not responded. If they say, 'Don't send me any,' then they get flagged. It would have all the options that are really within the legislation and give them all those options to opt out.

Mr CADMAN—What is your main source of new databases? Where do you get them from? Banks?

Mr Smith—No, mainly other direct marketers.

Mr CADMAN—Do you mean there is a system there—that everybody is mailing to the same people?

Mr Smith—There is a core. The growth in direct marketing has been phenomenal over the years.

Mr CADMAN—I notice some of the big users are organisations like ANZ Bank and even Centrelink. It seems to me there could be quite a good business by BT Funds, Optus, CCH and people like that exchanging lists.

Mr Smith—We do not use financial people's lists. Ours come mainly from other direct marketers.

Mr CADMAN—Such as Fairfax and those sort of people?

Mr Smith—No. Doubleday, because they are a book club, Time and so on.

Mr CADMAN—How do Telstra trade in the market? Do they trade in the same way?

Mr Smith—I am not familiar with Telstra.

Mr CADMAN—Time Life would be another local exchange?

Mr Smith—Because they are related products, so that you know people are going to buy books. It is not a shotgun approach; it is targeted. If you rented a Telstra list, that is a shotgun approach, because you are not sure if they are going to respond to a book offer. But if they are a Time Life or Doubleday customer, or if they purchase through one of these other companies that so order, it is a matter of sticking together and having a bit of involvement. It is what we call affinity marketing.

Mr CADMAN—The major mail users would tend to trade between each other with similar commodities, would they?

Mr Smith—Yes. I do not think Telstra would be swapping their lists with Optus.

Mr CADMAN—Probably not. But they could be swapping—

CHAIR—But that is only because it is not a real marketing decision.

Mr Smith—True.

CHAIR—You are saying that the principle of marketing which you apply is that it is better to have other people in the particular market that you are in than not. A simple analogy is that one of my McDonald's franchisees told me that he would much prefer to have a Hungry Jacks next door than any other sort of store because then they were both attracting the market and people could swap between. That is what you are saying.

Mr Smith—Yes, it is affinity, there is a formula that is used.

Mr CADMAN—Let us take that principle line: I am an ANZ Bank customer, what information are they likely to swap with some of the financial people, or travel packages that they are associated with?

Mr Smith—I am not really qualified to answer that.

Mr CADMAN—No, you are not, but if you could speculate as an observer, pretty well informed one actually?

Mr Smith—Mainly the information that is exchanged is name and address and that is it. That is why you go to, let us say, Time—in our case, it is Time or Doubleday—because there is a good chance those people are book buyers or video buyers. It is an affinity thing. So taking your question, you might say that ANZ, through their direct marketing arm, are going to sell some travel, so they might—

Mr CADMAN—Investment properties, that sort of stuff?

Mr Smith—Yes. Some of these things do not have very big lists and they are high value, so the investment in finding a database is very hard.

Mr CADMAN—Are people actively building databases?

Mr Smith—I think all companies build their own database. A lot of people never look forward to, once they have got this huge database, what they are going to do with it. The world is changing, not only in direct marketing, but in making products relate to the people who come into your store. One of the greatest things with direct marketing has really been store generation. There was a campaign years ago in the United States with all the letter box stuff which is lead generation. Everyone calls it 'junk mail', but they started a campaign calling it 'jobs mail'. So it was a four-letter word for jobs, because of the industries that build up and generate and, ultimately, the lead generation ends in a store. You are starting to see that now. All of the major department stores with their credit cards and so on, are now targeting people to come in and buy. We do not have a shop-front, so that is why our packages are such. That is the evolution. The other thing is that I think you

will see a growth in the Internet, but a mailing package will still be used to get people through the front door.

Mr CADMAN—Exactly. Are there provisions that will protect privacy pressures?

Mr Smith—They are the same ones that are in there now. People will prospect: they will send an offer and give people the option of not receiving any further offers. It is just like hanging banners in a shop window.

CHAIR—Thank you for your submission and thank you for coming in and discussing with us this afternoon not only the privacy aspects but some of the more general aspects as well.

Mr Smith—Thank you.

[3.58 p.m.]

GAUDIN, Dr John Howard, Acting Legal and Policy Officer, Privacy New South Wales

CHAIR—Welcome, Dr Gaudin. Do you have anything to add to the capacity in which you are appearing?

Dr Gaudin—I am appearing on behalf of the New South Wales Privacy Commissioner Chris Puplick, who is overseas and also on behalf of Acting Deputy Commissioner Katherine Reardon, who is indisposed today.

CHAIR—I should advise you that, although the committee does not require you to give evidence under oath, the hearings today are legal proceedings of the parliament and warrant the same respect as proceedings of the houses themselves. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. Dr Gaudin, we are in receipt of the Commissioner's submission to the inquiry. I invite you to make some opening statements.

Dr Gaudin—Thank you. The submission is based on the experience of the privacy committee of New South Wales and the Privacy Commissioner's office, as its successor, in dealing with private sector complaints over a period from 1975 onwards. In dealing with private sector complaints over the period from 1975 onwards I have been a research officer with the committee since 1992 and, because we are a fairly small organisation, research officers deal with members of the public and deal with complaints at the same time as helping to develop policy including, for example, this submission.

There are a number of matters in our submission which I would like to draw particular attention to. We have some problems with the way the national privacy principles are expressed. We are concerned that the disclosure threshold for health information is lower in some ways than that for other forms of information which are not as sensitive. We feel there is a need to reinforce the definition of consent in the Privacy Act to reflect the kinds of contract relations which exist in the private sector and to avoid any blanket waiver of privacy rights by people who enter into relations with the private sector.

We felt that the public revenue exemption was unnecessary and inappropriate in the non-government sector and that if government agencies need to obtain information for the protection of public revenue they should exercise their legal rights to do so. We felt—and this is in relation to matters that were discussed by the last speaker—that the transitional principles were unrealistic. But in relation to use and disclosure we thought it was unrealistic to assume that information collected before it was possible to separate out the way you treat information collected before the commencement date as far as the use and disclosure principles are concerned.

Ms ROXON—I am sorry. Can you say that again: that it is impossible to—

Dr Gaudin—That it is unrealistic to do so in many cases. We had some concerns about enforcement: that the enforcement provisions would be complex and there would be too

much scope for organisations to bury or sidetrack a complaint. I think our view would be that a clear notification of the right to adjudication when people start dealing with an organisation or some form of alternative complaint through the Privacy Commissioner, even if there was a separate adjudication system, would be of benefit.

We also had a number of concerns over the exclusions. Overall we felt that creating so many exemptions will tend to confuse the public in relation to what their privacy rights are and to encourage avoidance practices. We felt the small business exemption was anomalous and will lead to various inconsistencies. The one that has occurred to me since is private schools. It would seem that private schools which have a large turnover will have information protected, whereas private schools which have a small turnover may well be unregulated. I do not think this is a good social position. We felt that it was very hard to define the application of the reverse exemption which applies to small businesses which collect or disclose personal information for a profit. We found it difficult to actually see what businesses would be covered by this.

In relation to state trading enterprises, the situation is slightly more complicated than was suggested in our submission. We did not take proper notice of clause 6F which allows governments to opt in their state trading enterprises when they are exempt. From the point of view of New South Wales we would prefer to bring state trading enterprises under state law rather than face unpredictable negotiations as to whether they are included in a national scheme or not or whether they come within the small business exemption or not. I guess we were thinking here in particular of organisations like small electricity or water providers which might fall into the small business category.

CHAIR—You still have them in New South Wales?

Dr Gaudin—There are some, yes, like the Cobar Water Board. With contract service providers we had some concerns about the way they ended up being in something of a vacuum, caught between the public sector provisions and the private sector provisions. Particularly we have concerns in relation to New South Wales because our act really only very indirectly covers private sector contractors and this act would exempt them. But that is something that we may have to do under our own legislation if there is no amendment.

We felt the exemption for political parties sends the wrong message and that any exemption which applies needs to be more narrowly defined. We had concerns that the media exemption was too broadly defined and we were concerned that it might exempt online subsidiaries of media organisations and that possibly even web sites which disseminate information to the public would come under it. With the recent developments over CrimeNet, that is an interesting case to see whether that would actually be covered by the media exemption.

Finally, we had concerns about the employment records exemption in relation to the difficulty of defining and restricting what were employment records, given that new technologies automatically gather data on employees. Industrial remedies, which were mentioned in the explanatory memorandum, are not really adequate when dealing with the fairly large range of employment related complaints which we receive.

Ms ROXON—I will start on one of the minor things. I am not sure if you were here this morning when we were asking some questions about the political exemption. One of the things that we were trying to explore was whether the legitimate concerns of the public about information being collected were in the area of the large scale telemarketing formation of databases or those sorts of things that occur through polling through state offices or national secretariats, or whether there was also a concern about individual members of parliament collecting information.

Kevin used an example of walking down the street with your clipboard saying hello to 10 constituents, talking to them about whatever issues they raise and marking down that information, so that the next time you make a speech on the environment, for example, you send it out to all the people who have stopped you and talked to you about the environment. We did not get that far with comments about whether there was any distinction. I would be interested in your view. You said that perhaps it needs to be narrowed. Is that to allow those processes that anyone wants to be able to go through to serve their constituents properly, but not allow others, or is it to regulate both? What is your view on that?

Dr Gaudin—I dare say that foremost in our mind, because of some of the complaints we have received over the years, are cases which more obviously appear to be misuse of information. These tend to happen at the local government level and sometimes at the state government level.

Ms ROXON—What is an example of that—not identifying people, just that type of thing?

Dr Gaudin—No, I cannot identify them. An example would be the use of information about people who have applied for rate relief to local councils in order to send direct mail to pensioners. We realise that when elections happen there are often claims and counterclaims flying about whether a particular use of information is a legitimate use. We can see the need for perhaps restricting the privacy legislation so it does not get drafted into political bunfights between people at the time at local, state or federal elections—maybe some provision which would avoid that. But, at the same time, it has to be recognised that political parties do use personal information very intensively, people do get upset about it and there should at least be some mechanism for people to make complaints and have them dealt with, even if you did it through, say, a code.

Ms ROXON—But even if you had some exemption at the time of elections, the information is being collected at all other times, so you would still need to deal with it in some way, presumably.

CHAIR—To take your point, if you are going to have information which is going to be useful when the election is called, you have got to collect it before then; it is too late waiting until the election is called.

Dr Gaudin—Part of the problem about a complaint driven privacy scheme, which this is, is that it is only when people become aware of the information being used in a way they find unacceptable that they will actually complain about it.

CHAIR—The example about the rate relief seems to me quite clearly about somebody who has gone to their local council for a particular purpose and then finds presumably information given about pensions is being used by a councillor for political propaganda or some other purposes. If local council stands in the place of the government, it would be like people providing information to the government which then individual members of parliament or political parties make use of, which tends not to happen because the government departments at the federal level at least are subject already to privacy principles. There are times when I want information because—

Ms ROXON—But, Kevin, isn't it the same if someone comes and asks you in your office about assistance getting a back payment from Centrelink which they think they should have got and your office assists in finding out? Presumably that then gets marked so that next time you send out something about Centrelink or pensions or whatever it goes to that person. I am just using you as an example.

CHAIR—No, it does not in my case.

Ms ROXON—Well, it should. What I am trying to get at is your view. Do you think it is different if the person comes to Kevin? They know that Kevin is a politician that they are talking to, so they are giving him some information. Is that different from the situation where they go to Centrelink and somehow then it gets to Kevin? Or they answer a telephone call and they do not know that it is on behalf of the Liberal Party; they give all sorts of information that then is used to ensure that Kevin is mailing out to—

Dr Gaudin—Behind your question, I think you are tending to assume it is impossible to work within the principles. The principle would be that the person tells you at the time what it is for.

Ms ROXON—No, I am not assuming that. Through your experience and office you made a comment that you think it sends the wrong message and that there needs to be better regulation of what politicians do. What I am trying to get a feel for is the things that you think are offending that. Is it the whole range and is it a particular—

Dr Gaudin—It is usually those examples of a politician appearing to get information as a result of their official role or from a government source and marketing out widely. One can say that that is a complaint which can be dealt with as a breach of the public sector principles. Indeed, I think there was a complaint at the last election about that which was made to the Privacy Commissioner and published. But I think if you simply create a total exemption for politicians, it is very hard to investigate it.

CHAIR—Would you say, for example, if there is telephone polling done by XYZ corporation which is being done on behalf of a political party, then it should be disclosed on whose behalf it is being done?

Dr Gaudin—I think that would be a reasonable privacy standard, yes.

Ms ROXON—You also said that you were concerned that you thought that the health standards were lower than the standards in other areas rather than lower than health standards in other legislation or at the state level.

Dr Gaudin—That is correct, yes.

Ms ROXON—A number of witnesses have said that their preference would be that the provisions relating to the health sector actually be removed from this bill and dealt with entirely separately. Do you have a view about that being an appropriate course? We asked the witness was if it was better to have something in place than nothing. If you could comment on that as well, it would be helpful for us.

Dr Gaudin—I think one is recognising a general need which exists in the present Privacy Act for health information to be made available for medical research and possibly for other forms of research. There are provisions obviously for the Commonwealth public sector for that. We are working on similar provisions which would apply to research records generally under the New South Wales privacy legislation. I am not sure that I would like to take it entirely out of the Privacy Act because, again, that increases the confusion of people as to why their health information is not protected by privacy when they come to look at it.

But even with something like a code made to cover research, I am not quite sure if the bill really allows that because it focuses very much on codes on sectors. You could say there is a sector, there is a research sector, or a sector on organisations which are involved in research and have a more tailored provision. I think what concerns me about the scale of the health exemption is that it uses words like 'research' and 'statistical purposes' fairly loosely and then has some provisions for ethical approval of research projects. But a lot of what would pass as research or statistical use does not fit easily within the existing framework for ethical approval of research.

CHAIR—Can I ask you about something which I do not recall seeing in the submission, and that is the treatment of information which is already on the public record.

Dr Gaudin—You are talking about publicly available publications in particular?

CHAIR—Yes, or registers. There is a whole range of things on public records ranging from marriages, deaths and births through to—

Ms ROXON—ABNs—

CHAIR—ABN and electoral rolls—

Dr Gaudin—They are covered.

CHAIR—criminal records, connections.

Dr Gaudin—Public registers are covered under the New South Wales legislation, but from the point of view of restrictions on New South Wales government agencies

disclosing public record information, in fact the provisions are quite difficult there because it becomes very difficult to define what is a legitimate use of public register information and what use there is going to be on what is legitimate. The New South Wales legislation tries to define this in terms of the function of the register, what the legislation is under which the register is there.

CHAIR—Take one. Take the register of births.

Dr Gaudin—Yes. It is not a public register in New South Wales.

CHAIR—Give me one that is.

Ms ROXON—The lands.

Dr Gaudin—Okay; the lands titles are.

CHAIR—Deaths or marriages or something like that.

Dr Gaudin—Births, deaths and marriages in New South Wales are restricted.

Ms ROXON—Business trading names?

Dr Gaudin—Okay.

Ms ROXON—Pick one example to tell us how they work.

CHAIR—It does not matter what it is, as long as it one that is available in New South Wales so that we can try and tease —

Dr Gaudin—One that causes a lot of attention for people is council rate rolls. Councils receive notices of sales of property and the prices paid for them and councils at the moment are fairly divided on how to provide that information. Lots of councils will sell that information. It will be used by people interested in prospect sales to people, and it causes a great deal of distress among a fairly definable section of the population.

Ms ROXON—So what is the legislation that covers it at the moment?

Dr Gaudin—At the moment all council information is made available under the Local Government Act as a sort of open council regime. Under the New South Wales privacy legislation which comes into force on 1 July, councils are required to satisfy themselves that the information is to be used for a purpose that is consistent with the purposes of the register. One could say that, because the rating information the councils have is made available to allow people to check rates for sale and purchase of properties, that people involved in the sale and purchase of properties have a legitimate need to look at that information. So you could say, for instance, that real estate agents should have access to that information.

Mr CADMAN—The same as the lady next door.

Dr Gaudin—Yes. There are a whole lot of reasons why people would want it—prospective purchasers, people who want to have disputes over dividing fences, people who want to object to developments and things. There are lots of reasons why that information should be publicly available. That is what we are struggling to define.

Ms ROXON—Is that a standard sort of guiding principle that is used in other areas, that the access should be restricted to purposes consistent with the purpose for which the information was originally collected?

Dr Gaudin—I think privacy legislators in different countries are struggling for a way of controlling public registers. In the past there was a feeling that if you went to the council and took the trouble to look you were entitled to use the information. But because it is so easy to electronically capture it now, there have been discussions in Europe and at the last privacy commissioners conference about their attempts to deal with it. I am not in a position to say whether the way that we have chosen to tackle it in New South Wales is the best.

Ms ROXON—What I was trying to say is that the example you used was for the council lots. Is that one that applies—

Dr Gaudin—It applies to all public registers under New South Wales, but it comes into force only after 1 July this year.

Ms ROXON—So, for example, you would use the electoral roll, which we have been talking about before, for electoral purposes but not necessarily for any other purpose?

Dr Gaudin—The electoral roll is different because it becomes a publicly available publication. It is impossible for government agencies to try to control how people use publicly available publications under public sector privacy law.

CHAIR—If it is published it is in a different category from information which is public and available but not physically published?

Dr Gaudin—Yes, that is a distinction made in our legislation.

Mr CADMAN—So an electoral roll is a published document, so it is different. We will call it ‘records’.

CHAIR—Would that be one that is available but not published?

Mr CADMAN—Presumably you can go to the local magistrates court or district court and inspect the records.

Dr Gaudin—Not everyone can. You have got to have an interest—for instance, to look at local court records in New South Wales.

Mr CADMAN—Have you?

CHAIR—What about civil courts? New South Wales is different. You can go into the prothonotary's office in the Supreme Court in Melbourne and, as long as you are prepared to sit there—

Ms ROXON—Spend a very boring day.

CHAIR—and spend a boring day, you can look at all the matters that have been filed that day if you want to. In fact, there is a journalist from the *Melbourne Age* who regularly does so.

Dr Gaudin—I think that would be so with Supreme Court records here in New South Wales.

CHAIR—My question then is: are they published? There is a published list of cases. There is the court calendar, which has the cases that have been filed and set down for trial, et cetera. Does that qualify as having been published?

Dr Gaudin—I presume so but I would also note that in New South Wales it is not kept permanently. There is a copy in the *Sydney Morning Herald* and a copy put on the Internet page for about a week.

Ms ROXON—Of the list—but the file?

CHAIR—But presumably there is also a physical court calendar which is issued every month, or every so often, and which you could collect and put on your bookshelf.

Ms ROXON—To give you an understanding, some of the questions we asked at previous hearings were to do with CrimeNet where the information that is being collated and put on that site is publicly available information but it is not necessarily readily available—in some circumstances it is publicly available—not in some published form. But is there any breach of privacy—

Mr CADMAN—It is not consolidated in one place, is it—the information that goes on the CrimeNet?

Dr Gaudin—I think it is a bit like the point Mr Smith was discussing previously—that once you actually take the information and put it in your own system it is enhanced in some way. There is nothing to stop you collecting information which is publicly available in that way, but once you compile it you are adding something to it. You are putting it all together in one place. It becomes personal information that you have collected, are holding, are processing and that you are using or disclosing for other purposes. At that point, I think it needs to be covered by whatever privacy legislation is around. A lot of people are very sensitive about their date of birth. In most cases your date of birth is published in the newspaper at the time you are born. If you said that that information meant that your date of birth had never had privacy rights attached to it, people would object to that. There is nothing to stop somebody going through the *Sydney Morning*

Herald and collating dates of birth and getting names and dates of birth of a lot of people. It probably would not be much use to them.

Ms ROXON—You would not have to go to so much trouble once some states get public registers.

CHAIR—That is a good example because it would be in the interests of a lot of commercial companies to know about dates of birth. Presumably at the time of the birth you can look in the *Sydney Morning Herald* or in Victoria you can go to the registry and get it. If you were in the business of marketing baby equipment or prams—affinity marketing, I think Mr Smith called it—then the market you are going to be directing yourself to presumably is more likely to be buying prams. The people who are most likely to be buying prams are those who have just had babies, so you could make use of that information. Equally, if you knew all the people who were turning 50—to grab a figure out of the air—on a regular basis and you thought that a particular product would be attractive to 50-year-olds, then it seems to me that that would potentially have considerable commercial value.

Mr CADMAN—Or you could store the birth dates for 12 years and then say, 'Here is a skateboard market.' There are a lot of uses you could put that information to.

Dr Gaudin—Yes, you are collecting publicly available information, but once you actually store it and sort of work out how you are going to use that—

Ms ROXON—Presumably when you send that first letter to them, this still requires you to then comply with the opt-out standards?

Mr CADMAN—You hit them once and then they say, 'I don't want this anymore.' They have opted out, but you have had the chance of hitting them once, haven't you?

CHAIR—Let me complicate it a little bit more because I am trying to look at the CrimeNet. I go into business of collecting dates of birth and I do not market anything else except lists of dates of birth. I am not interested in selling prams, but I know a lot of people are interested in selling prams and skateboards and all of that. My business is using publicly available information, compiling that in a way and then providing it as a source to those who want to market whatever the goods are. Then they can come to me and they can say, 'I want birth dates of people born this year, or that year, or a list of people who are this age, or whatever.'

Mr CADMAN—You would even be able to have the gender of them.

Dr Gaudin—That is right.

CHAIR—Therefore, in terms of the privacy principles, this is publicly available information. Leaving aside any peculiarity of the law about, say, births in New South Wales, let us assume it is publicly available information on public records. My question is: how should legislation apply to that, given that I have really just compiled information that is there anyway? Any of these companies could have put the effort into going and

doing it; presumably they would not because it would not be in their commercial interest to do it. It is only in mine, because I can sell it to a thousand companies rather than use it for my own interests.

Dr Gaudin—I would still say that once you have incorporated it into a database yourself and are using that database, what you are using is not publicly available information. It is a little bit like the attempt to provide legal security for databases.

Ms ROXON—So the individual entry might be publicly available, but once you turn it into a—

Dr Gaudin—I presume that the exemption under the existing Privacy Act for publicly available sources and in New South Wales for publicly available publications was put there to make it clear that you do not have to collect that with the consent of the individual and so forth, that anybody is free to collect information from a public source. Going back to the birth date example, you make a joke of any attempt at privacy regulation if you say that that public availability continues as long as you hold the same information. Probably all of us have got some information about us which has been in the public source, but one of the things that people do not like and in which they expect to be protected by privacy legislation, is the possibility of pulling everything that is in a public source together in another source. So it is the electronic dossier that people are concerned about.

CHAIR—If a company is big enough to do it themselves—Hallmark Cards or someone like that, a big multinational corporation—presumably they can compile that list themselves and then the first time that they would have to say to people, 'You can have access to or be removed from our mailing list,' is when they post something to them.

Dr Gaudin—Yes. But the other principles about disclosure of the fact they hold information on people and their disclosure of it to other people for purposes other than that for which they brought it or assembled it might still kick in.

Ms ROXON—I have a question on an unrelated matter. How is small business treated under the New South Wales legislation?

Dr Gaudin—The Privacy Commissioner has the power to investigate complaints about small business. The mandatory provisions of the privacy legislation which begin in July will only apply to the public sector, so all this does is basically continue what the privacy committee has done for about 25 years, which is to allow us to investigate complaints about businesses, schools and non-government organisations, with no restriction on size, but with no real power to enforce anything on them. If there is a pattern of behaviour by small businesses we might recommend legislation and this might result in something like the commercial agents legislation which licenses commercial agents and private investigators.

Ms ROXON—Do you have a view, from the breadth of complaints that you deal with, about whether it is small business or large business that is the more regular offender? We have had lots of submissions about whether this exemption is appropriate or not.

Dr Gaudin—We discussed this in the office before I came here and generally agreed that we probably get more complaints from small business, that the friction is there. There is the perception that people ask for too much information in order to provide a service. It is very difficult, because of the threshold question of what a small business is, to know in all cases whether you are dealing with people that would be small businesses under the act. Certainly there is more friction there from small businesses because I think the large businesses, the large organisations like Readers Digest, have probably got their act together.

Ms ROXON—Do you go the step further and say—I am not sure if this is in your submission, but I think not—that the exemption should not be there for small business?

Dr Gaudin—Yes. But, equally, it may be necessary for the Privacy Commissioner to develop some sort of code for certain kinds of small businesses as a more convenient way of freeing them from some of the more onerous provisions which might otherwise apply.

CHAIR—Dr Gaudin, thank you very much for the submission and also for coming and discussing it with us this afternoon. We really appreciate it. I thank you all for your attendance today and I thank those recording the evidence.

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

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

Committee adjourned at 4.35 p.m.